

Policing in the Digital Society  
Network Yearbook 2025

# Legal and Ethical Issues in Digital Policing

Wouter Stol

Lene Wachter Lentz

Markus Naarttijärvi

Inger Marie Sunde

Adam Jackson

Litska Strikwerda

Jurjen Jansen

(eds.)

**Boom**

Digital developments have a significant impact on crime and therefore on law enforcement practices. One of the profound issues is that the police have to deal with challenges in balancing new technological possibilities for law enforcement agencies in the investigation of crimes, and the implications that these developments have for fundamental human rights. There are no clear-cut solutions or answers. Step by step, the police have to find answers to several legal and ethical issues that go together with the digitalisation of society. The aim of the PDS-network and of this volume is to address and discuss critical policing issues. This volume is the result of the 2023 Policing in the Digital Society Network conference at the Police Academy in Apeldoorn, the Netherlands. This volume provides the police, as well as institutions for academic and police education, with insights into the latest developments and legal and ethical issues in modern policing.



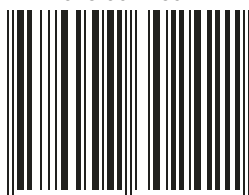
POLITIEACADEMIE



Open Universiteit  
[www.ou.nl](http://www.ou.nl)



ISBN 978-90-4730-242-1



9 789047 302421 >



[www.boom.nl/criminologie](http://www.boom.nl/criminologie)

## Legal and Ethical Issues in Digital Policing



# LEGAL AND ETHICAL ISSUES IN DIGITAL POLICING

*POLICING IN THE DIGITAL SOCIETY*  
*NETWORK YEARBOOK 2025*

WOUTER STOL  
LENE WACHER LENTZ  
MARKUS NAARTTIJÄRVI  
INGER MARIE SUNDE  
ADAM JACKSON  
LITSKA STRIKWERDA  
JURJEN JANSEN  
(EDS.)

**Boom**

Cover design and typesetting: Textcetera, Den Haag

*This book is published in open access under licence CC-BY-NC-SA. Without prejudice to the agreements on reproduction rights and the reader regulation, this license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.*

*This publication is protected by international copyright law.*

*All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher.*

ISBN 978-90-4730-242-1

NUR 741

[www.boom.nl](http://www.boom.nl)

[www.boom.nl/criminologie](http://www.boom.nl/criminologie)

# TABLE OF CONTENTS

<b>1</b>	<b>Preface</b>	<b>13</b>
	<i>Lene Wachter Lentz and Markus Naarttijärvi</i>	
1.1	Dilemmas in new technologies for combating crime	13
1.2	A brief history of the Policing in the Digital Society Network	16
1.3	The wide scope of digital policing	17
1.4	The contributions in this volume	18
1.5	The future	21
<b>2</b>	<b>Local police, digitalisation and implementation</b>	<b>23</b>
	<i>Jan Terpstra</i>	
2.1	Introduction	23
2.2	Context and methods	24
2.3	Theoretical framework	25
2.4	Dominating logics and normative orders	27
2.5	Four types of digitalisation	29
2.5.1	Searching and processing of information	29
2.5.2	Social media	31
2.5.3	Real-time intelligence and mobile applications	33
2.5.4	New visibility	34
2.6	Conclusion	36
	References	37
<b>3</b>	<b>Disentangling the interaction between professional intuition and technologies in policing</b>	<b>43</b>
	<i>Nienke de Groes, Vlad Niculescu-Dinca and Pieter Tops</i>	
3.1	Introduction	43
3.2	Methodology	45
3.3	Conceptualising the impact of digital technologies on the police practice	45
3.4	Technologies and the discretionary power of policing professionals	46
3.5	Digital technologies and professional intuition: mutually exclusive or interacting?	47
3.6	Theoretical framework	48
3.6.1	Conceptualisation of digital technologies in policing	48
3.6.2	Technological Mediation Theory	49
3.6.3	Dual Process Theory	49
3.7	Proposing the initial steps in a taxonomy of intuition-technology interaction	51
3.7.1	How professional intuition and digital technologies interact	51

## TABLE OF CONTENTS

3.7.2	The need for ethnographic research to examine intuition-technology interactions in policing	53
3.8	Conclusion	54
	References	55
<b>4</b>	<b>The digitalisation of the police</b>	<b>59</b>
	<i>Kevin Emplit, Maxime Mauquoy and Lies Vande Meulebroucke</i> <i>With the collaboration of Sarah Van Praet</i>	
4.1	Introduction	59
4.2	Exploring three key technologies in policing	60
4.3	Systematic reviewing method	63
4.4	Digital device implementation in police organisations	64
4.4.1	The genesis of digital device implementation	64
4.4.2	The implementation process of digital devices	65
4.5	The transformations of work and working conditions of frontline police officers	66
4.5.1	Impact on work content and organisation	66
4.5.2	Impact on well-being and work environment	67
4.5.3	Impact on relations with hierarchy	67
4.6	The transformations of 'policing' and police-public relations	68
4.6.1	Body-worn cameras (BWCs)	68
4.6.2	Crime analysis software (CAS)	69
4.6.3	Multi-tenant platforms (MTPs)	70
4.7	Conclusion	71
	References	73
<b>5</b>	<b>Advancing the potential of VR in policing</b>	<b>83</b>
	<i>Meret Asara Paululat, Bas Böing, Vlad Niculescu-Dinca and Peter W. de Vries</i>	
5.1	Introduction	83
5.2	The issues of ethnic profiling and racist stereotypes	84
5.3	The potential and issues of deepfakes in VR	85
5.4	The deepfake study	88
5.5	Methods	89
5.5.1	Participants	89
5.5.2	Procedure	90
5.5.2.1	Before VR-environment phase	90
5.5.2.2	360° VR Environment	90
5.5.2.3	Post-VR environment phase	91
5.6	Measures	92
5.6.1	Stop-and-search behaviour	92

## TABLE OF CONTENTS

5.6.2	User experience	93
5.6.3	Stereotype threat	93
5.6.4	Open questions	93
5.7	Results	94
5.7.1	Main analysis	94
5.7.2	Thematic analysis	95
5.8	Discussion	98
5.8.1	Participant behaviour	99
5.8.2	Reflection on VR and deepfake	101
5.9	Limitations and future directions	103
5.10	Conclusion	104
	Acknowledgements	104
	References	104
<b>6</b>	<b>From code to courtroom</b>	<b>109</b>
	<i>Saskia Westers, Maike Berkenpas, Jurjen Jansen, Wendy Schreurs, Greg Alpar and Kimberly Bluhm</i>	
6.1	Introduction	109
6.2	Methods	110
6.3	Results	111
6.3.1	What is the nature of encryption in criminal cases?	111
6.3.1.1	Types of encryption	111
6.3.1.2	Presence of encryption in criminal cases	113
6.3.2	What is the role of encryption in evidence gathering in criminal cases?	114
6.3.2.1	Obtaining decrypted data	115
6.3.2.2	Role of encryption in how an investigation proceeds of an investigation	117
6.3.3	What is the role of encryption in the criminal prosecution and judicial resolution of these cases?	118
6.3.3.1	Criminal prosecution	119
6.3.3.2	Judicial role	123
6.3.3.3	Judicial resolution	124
6.4	Conclusion	125
6.5	Limitations	126
	References	128
<b>7</b>	<b>When does police processing of personal data fall within the material scope of the Law Enforcement Directive?</b>	<b>133</b>
	<i>Tanja Kammergaard Christensen</i>	
7.1	Introduction	133
7.2	Methodology	135
7.3	The scope of the LED	136

## TABLE OF CONTENTS

7.3.1	Criminal offence	139
7.3.2	Public security	140
7.3.3	Summarising the scope of application	142
7.4	The role of the police in Denmark	143
7.4.1	The role of the police within the criminal justice system in Denmark	145
7.4.2	The role of the police outside the criminal justice system	148
7.5	Conclusion	149
	References	150
	ECTHR case law	152
	CJEU case law	152
	Law and orders	152
<b>8</b>	<b>'Fishing' in large data lakes</b>	<b>155</b>
	<i>Inger Marie Sunde, Tanja Kammergaard Christensen and Lene Wacher Lentz</i>	
8.1	Introduction	155
8.2	Method, theoretical background and research question	157
8.3	The Law Enforcement Directive	160
8.3.1	Introduction	160
8.3.2	Subsequent processing of personal data: Article 4(2) LED	160
8.3.3	Deletion: Article 5 LED	164
8.3.4	Summary on the LED	165
8.4	National law in Denmark and Norway	165
8.4.1	Introduction	165
8.4.2	Denmark	166
8.4.2.1	Law Enforcement Act	166
8.4.2.2	Danish Procedural Code	167
8.4.3	Norway	169
8.4.3.1	Introduction	169
8.4.3.2	Purpose limitation	170
8.4.3.3	Data collected in real time	171
8.4.3.4	Historical (stored) data (collected by search, seizure and production order)	173
8.4.3.5	Scenario 1: Purpose specificity	173
8.5	Comparative conclusion	175
8.6	Summary and future challenges	176
<b>9</b>	<b>Assessing interference</b>	<b>177</b>
	<i>Carlos José Calleja</i>	
9.1	Introduction	177
9.2	Methods of disrupting computer-enabled crime	180

9.2.1	The narrative around the methods of disrupting computer-enabled crime	180
9.2.2	Conceptualising the methods – degrading, disrupting and disabling	181
9.2.3	Conceptualising the infrastructure targeted	182
9.2.4	Disrupting computer-enabled crime at a cognitive level	183
9.3	Aims of disrupting computer-enabled crime	184
9.3.1	Increasing costs and mitigating harm caused to victims	184
9.3.2	The rationale that underpins disrupting computer-enabled crime	185
9.4	Interference with the right to receive and impart information in Article 10(1) of the Convention	186
9.4.1	The Court’s case law on the right to receive and impart information in Article 10 of the Convention – blocking means of disseminating and receiving information	186
9.4.2	Disrupting computer-enabled crime as an interference with the right to receive and impart information in Article 10(1) of the Convention	187
9.5	Interference with the right to respect for private life and correspondence in Article 8(1) of the Convention	189
9.5.1	The Court’s case law on the right to receive and impart information in Article 8(1) of the Convention – reasonable expectation of privacy	189
9.5.2	The Court’s case law on the point at which an interference with the rights in Article 8(1) takes place	190
9.5.3	Disrupting computer-enabled crime as an interference with the right to respect for private life and correspondence in Article 8(1) of the Convention	191
9.6	The particular case of cognitive forms of disrupting computer-enabled crime	193
9.6.1	The Court’s case law on the protection that Article 8(1) affords to establish relations and personality development	193
9.6.2	Restrictions to the protection of Article 8(1)	194
9.6.3	Cognitive disruption – an interference with Article 8(1)?	195
9.7	Conclusions	196
	References	196
	Academic writings, commentaries and media reports	196
	Case law	199
	Reports, guidelines and national strategies	200
	Treaties and legislation	201
<b>10</b>	<b>Digitalisation and the police function</b>	<b>203</b>
	<i>Wouter Stol, Jurjen Jansen and Wouter Landman</i>	
10.1	Introduction	203
10.2	Social control as a theoretical perspective	204
10.3	Study design and methods	204

## TABLE OF CONTENTS

10.4	Digitalisation and crime	205
10.4.1	Digitalisation and offending behaviour	205
10.4.2	Digitalisation and participation in crime control	207
10.4.3	Digitalisation, police and crime-fighting	208
10.5	Digitalisation and public order	209
10.5.1	Digitalisation and public order disturbances	210
10.5.2	Digitalisation and participation in order maintenance	210
10.5.3	Digitalisation, police and order maintenance	211
10.6	Conclusions: changed positions and the police function	212
10.6.1	Digitalisation and organisational capacity	212
10.6.2	Digitalisation and information capacity	213
10.6.3	Digitalisation and normative capacity	214
10.6.4	Digitalisation: altered social relations	215
10.7	Discussion: task for the police in the changed landscape of the police function	216
10.7.1	New power blocs in a changed landscape	216
10.7.2	Collaboration	217
10.7.3	Integrated approach	218
10.7.4	Safeguarding legal protection	219
	References	220
<b>11</b>	<b>Efficacy of the Dutch General Municipal Bylaw in combating online troublemakers</b>	<b>225</b>
	<i>Willem Bantema</i>	
11.1	Introduction	225
11.2	Legal background	226
11.3	Societal and administrative background	227
11.3.1	Examples of online-incited disturbances	227
11.3.2	Research and administrative developments	228
11.4	Methods	229
11.5	Description of the administrative General Bylaw experiment in the city of Utrecht	230
11.5.1	Case study description	230
11.5.2	Basis of the measure	231
11.5.3	Case law and literature	231
11.5.3.1	Limitations on Article 7 by central government legislation	231
11.5.3.2	Specificity of Utrecht's General Municipal Bylaw article	232
11.5.3.3	Extent of disorder	233
11.5.3.4	Conflicting views of the municipality and legal experts	233
11.5.3.5	Reflection from the focus group and expert meeting	234
11.5.3.6	Reflection of the Court	235

## TABLE OF CONTENTS

11.6	Description of Brussels General Police Regulations (Belgium)	235
11.6.1	Description of the Belgian case study	235
11.6.2	Reflection on the Belgian case study	236
11.7	Articles of the General Municipal Bylaw that explicitly focus (more) on the online domain	237
11.7.1	Expanding the definition of public space	237
11.7.2	Adaptation of the General Municipal Bylaw in Almelo	238
11.7.3	Reflection on current events	239
11.8	Discussion and conclusion	241
11.8.1	Discussion	241
11.8.2	Conclusion	242
	References	243
<b>12</b>	<b>Partners in crime-fighting?</b>	<b>247</b>
	<i>Rianne Dekker</i>	
12.1	Introduction	247
12.2	Methodology	249
12.2.1	Collection of relevant literature	249
12.2.2	Meta-synthesis	250
12.3	Findings	251
12.3.1	The focus of online citizen-led policing	252
12.3.2	The activity of online citizen-led policing	254
12.3.3	Perceptions of government law enforcement	256
12.4	Conclusions	258
	References	260
	<b>About the authors</b>	<b>265</b>



# 1 PREFACE

*Lene Wachter Lentz and Markus Naarttijärvi*

## 1.1 DILEMMAS IN NEW TECHNOLOGIES FOR COMBATING CRIME

Law enforcement agencies, privacy organisations and many others had their eyes set on the EU Council meeting on 20 June 2024, where a controversial proposal was meant to be discussed: the Child Sexual Abuse (CSA) Regulation. The aim of the proposal, presented two years earlier on 11 May 2022 by the European Commission, was to make it mandatory for communication service providers to scan private communications for child sexual abuse material and make the information available to law enforcement authorities.<sup>1</sup>

The proposal, also referred to as the EU ‘Chat Control’, was presented with the aim of combating crimes related to sexual violence against children.<sup>2</sup> However, the proposal has been heavily criticised, for example by privacy organisations, for subjecting EU citizens to mass surveillance, thus jeopardising the fundamental right to private communication.<sup>3</sup> As the obligation would also extend to providers of end-to-end encryption, an intense technical debate emerged, specifically on how the providers could ‘moderate the upload’ without breaking the end-to-end encryption.<sup>4</sup>

Shortly before the EU Council meeting on 20 June 2024, the proposal was taken off the agenda, apparently because no agreement on it had been reached.<sup>5</sup> There is so far no date for a new discussion of the proposal.

The initiative illustrates a profound challenge in balancing the new technological possibilities for law enforcement agencies in the investigation of crimes, and the implications for fundamental human rights. It also demonstrates an important challenge regarding how much power must be handed to law enforcement agencies for preventive measures, meaning before anyone has committed a crime, rather than

---

1 2022/0155(COD).

2 2022/0155(COD), Explanatory Memorandum, Section 1, Context of the Proposal.

3 EDRI and 47 civil society organisations: ‘Joint statement on the future of the CSA Regulation’, 1 July 2024, calling for the proposal to be withdrawn, <https://edri.org/our-work/joint-statement-on-the-future-of-the-csa-regulation/>.

4 E.g. statement from Meredith Walker, President of the communication network Signal: ‘New Branding, Same Scanning: “Upload Moderation” Undermines End-to-End Encryption’, 17 June 2024, <https://signal.org/blog/pdfs/upload-moderation.pdf>.

5 Clothilde Goujard, Politico: ‘EU cancels vote on child sexual abuse law amid encryption concerns’, 20 June 2024, <https://www.politico.eu/article/eu-council-cancels-vote-on-encryption-breaking-child-sexual-abuse-law/>.

reacting to crimes already committed. Naturally, law enforcement agencies have an interest in gaining as much knowledge as possible, thus enabling them to intervene as early as possible, before or when a crime is committed. From a citizen's perspective, the state's surveillance and interference are only justified if one actually does something wrong; only a reasonable suspicion can justify interference.

From a privacy perspective, it has been argued that tools for scanning communication would make all communication liable to interference, and for example catch teenagers consensually sending nudes to each other.<sup>6</sup> It has also been pointed out that the fight against child sexual abuse material is only the beginning for these tools; once the technology for messaging and chat control has been established, it becomes very easy to use them for other purposes.<sup>7</sup>

From a legislative point of view, crucial implications are at stake when EU law is used to combat crimes. Considering the law enforcement perspective, crimes against children involving abusive material are often found online and have cross-border aspects. The EU countries would benefit from cooperation on these matters. The harmonisation would ensure that all communication service providers in the EU are subject to the same obligation, although it has been argued that a mandatory scan would not effectively combat these crimes, as the perpetrators organise in self-run forums and the law enforcement agencies would be flooded with automatically generated information, most of which will be irrelevant.<sup>8</sup> It is also important to note that the CSA initiative is a proposal for an EU regulation, which would be directly applicable in each Member State. The legislative tool is therefore particularly strong, since it cannot vary from member state to member state.

While the proposal was presented by the EU Commission, the EU Court of Justice has elsewhere made a particularly strong stand on privacy in relation to data retention of call data records. The EU Data Retention Directive of 2006<sup>9</sup> aimed to harmonise data retention across the EU countries, for the benefit of law enforcement agencies in combating serious crimes, but it was annulled by the EU Court of Justice with the judgment in the joint cases of *Digital Rights Ireland* and *Kärntner Landesregierung* in

---

6 Electronic Frontier Foundation: 'Now The EU Council Should Finally Understand: No One Wants "Chat Control"', 1 July 2024, <https://www.eff.org/deeplinks/2024/06/now-eu-council-should-finally-understand-no-one-wants-chat-control>.

7 Patrick Breyer, German Member of the European Parliament: 'Chat Control: The EU's CSEM scanner proposal', blogpost (last visited 13 July 2024), <https://www.patrick-breyer.de/en/posts/chat-control/#how-does-this-affect-you>

8 Patrick Breyer, blogpost, <https://www.patrick-breyer.de/en/posts/chat-control/#how-does-this-affect-you>.

9 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

2014.<sup>10</sup> The CJEU's case law over the years on these matters has always related to the traffic data of the communication, not the content of the communication. The court noted in the *Tele2 Sweden* judgment that the Swedish legislation provided for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.<sup>11</sup> Furthermore, the Court stated:

That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.<sup>12</sup>

If – or when – the proposal for a CSA Regulation emerges for consideration in the EU Council, it will face strong debate again, as fundamental considerations are at stake. Ultimately, such a regulation would also have to deal with the CJEU's strong stance on privacy in communication.

The EU proposal for the service providers to scan communications for CSA illustrates some of the fundamental considerations at stake: the investigation of crime versus privacy; the never-ending drive of new technology; whether the role of the police is to react or prevent; how to design new technology to take into consideration privacy and avoid mass surveillance; and the role of national law, the EU and international organisations, such as the Council of Europe and the European Human Rights Convention. Continuous research on these matters is needed to ensure the right balance; it must also be interdisciplinary, so that the legal framework intended matches the technology and aligns with the ethical boundaries.

These topics are core interests of the dedicated researchers within the Policing in the Digital Society Network.

---

10 CJEU, 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof.

11 CJEU, 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, para. 97.

12 *Tele2*, para. 99. The CJEU's approach on these matters has been developed in subsequent judgments, e.g. in 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*.

## 1.2 A BRIEF HISTORY OF THE POLICING IN THE DIGITAL SOCIETY NETWORK

The Policing in the Digital Society Network and its associated conference emerged from the merger of two groups: the Nordic Cybercrime Conference and the PDTor research project. Both groups consisted of researchers in the fields of policing and criminal law, focusing on new technologies and the possibilities and challenges they present. In 2023, on the initiative of Wouter Stol and Inger Marie Sunde, initial meetings were held to discuss setting up a European network and annual conference. We saw the benefit of enhancing collaboration and reaching out to a broader community, thereby adding new perspectives to our research and fostering new relationships.

The Nordic Cybercrime Conference, initiated by the Law Department at Aalborg University, was first held in 2017. This gathering of researchers and practitioners from law enforcement authorities proved very promising, with participants expressing a strong desire to continue the event and the associated cooperation and network. Since then, the conference has also been hosted by the Norwegian Police University College and Umeå University. It has expanded its focus from specific provisions related to cybercrime and criminal procedure to broader topics like policing, big data, surveillance and related legal issues.

The PDTor research project (2017-2022) was formed by researchers from the Netherlands, the United Kingdom, Sweden and Norway, supported by a NordForsk research grant. The project explored the tension between citizens' privacy (Tor users) and state power (police on the Tor network) in crime prevention and investigation. The project's core idea was to compare daily police work with the demands of forensic correctness and legal fairness. The results aim to assist police in modern crime-fighting and provide accountability and fresh insights to the academic community on technology-based policing, human rights and enforcing laws on anonymous communication networks.

The new network that was formed on the basis of the two above-mentioned networks held its first European conference on 15-17 November 2023, at the Dutch Police Academy in Apeldoorn. The three-day event featured inspiring keynotes and a packed programme of exciting presentations divided into four tracks: (1) Our Digital Society and Its Police; (2) Everyday Policing and Digital Technologies; (3) Predictive Policing and AI; and (4) Digital Evidence. With up to 100 participants, the conference facilitated fruitful discussions and networking, leading to important new contacts and promising future collaborations. We received very enthusiastic feedback, reinforcing our desire to continue this network and cooperation. The network is currently organising the next European Conference on Policing in the Digital Society, scheduled for January 2025 in Newcastle.

Based on abstracts from distinguished researchers in the field of digital policing, this volume was created through a writing and review process conducted in 2024. With this

edited volume, our network's website ([www.policinginthedigital.org](http://www.policinginthedigital.org)), the additional newsletter and the conference, we are very pleased with the network's achievements and progress thus far.

### 1.3 THE WIDE SCOPE OF DIGITAL POLICING

The development of the network we have described so far illustrates an important point about digital policing. It is an area that has long existed at the intersection of different academic disciplines. Even within a single discipline, such as legal science, digital policing can intersect intradisciplinary boundaries between constitutional law, criminal law, procedural law, administrative law, data protection law, etc. Research questions relating to digital policing routinely flow between and through these different areas. In a similar vein, our conferences have illustrated how a commonly discussed topic, such as the use of algorithms for predictions or recommendations in policing, can bring together researchers from sociology, policing studies, management, law, political science and more – each with their own unique insights and perspectives, and each contributing to a fruitful exchange where everyone leaves the conference a little wiser and a little more mindful of the complexities we face.

These disciplinary exchanges and accompanying insights are valuable in their own right. As legal researchers – traditionally less empirically driven – we can, through these exchanges, identify fresh issues ripe for legal analysis that might have remained invisible to us otherwise. As researchers of policing practices, we can recognise the impact of those practices on victims, or on legal procedures, fundamental rights, the efficiency or effectiveness of policing, or wider societal values. Listening to practitioners, we can learn where the frontlines of digital policing are, what problems they face and the solutions they have found. Meanwhile the practitioners can draw from a wellspring of research-based insights into what works, what does not, and where the possible red lines are.

While these exchanges are important in their own right, they also speak to the vast potential for interdisciplinary and transdisciplinary approaches to digital policing. We have over the years been able to see the important insights such approaches can bring, through presentations of interdisciplinary projects at our yearly conference. But we can also see the seeds of new collaborations grow in the intense discussions and conversations taking place during the coffee breaks and conference dinners, discussions where interdisciplinary exchanges happen organically and spontaneously, and have led to articles, research applications, seminars and more, that might never have happened otherwise.

As a network organised not around a discipline, or a method, but around a societal issue and a practice, the PDS Network is not only a place where such collaborations can begin. The network is in itself a pool of diverse competences and experiences, insights

*LENE WACHER LENTZ AND MARKUS NAARTTIJÄRVI*

and personalities, professional and research-based knowledge, that collaborations can draw upon. The value of these connections can sometimes be obscured by their more practical expression in the shape of the conference itself, but should not be ignored. We would like to encourage our network to nourish these connections, build on them, and recognise that they may bring unexpected and positive things in the long run. After all, what began as a small criminal-law-oriented conference on cybercrime has grown into a European network on digital policing that continues to expand, and which has already (through the ever-important coffee breaks) spawned many new projects and collaborations.

Nowhere is the diversity and depth of the competences within the network more clearly illustrated than in this volume, the first official book produced by the network and appropriately the result of its first European-wide conference. As we can see, the contributions span the practical and the theoretical, cross disciplinary boundaries, and illustrate the very forefront of research into policing in the digital society.

#### **1.4 THE CONTRIBUTIONS IN THIS VOLUME**

Following this introduction, Terpstra begins our exploration. He considers the question of how local police units in the Netherlands are digitalised, to reveal how traditional and digital ways of policing are combined and/or come into conflict within this large and important part of the police service. Based on interviews with 60 officers from different positions in local policing, combined with observations across 134 hours of local policing, Terpstra identifies four different types of digitalisation impacting local policing: the search for and processing of information; the use of social media; real-time intelligence and mobile applications; and how policing becomes more visible through mobile phone cameras and online video sharing. The findings show that digitalisation is a process fraught with frictions, tensions, resistance and delay, where digital tools can be perceived as conflicting with practical knowledge and personal relations with citizens.

The dynamic between street-level police and digital tools continues in the contribution by de Groes, Niculescu-Dinca and Tops, who write about the relationship between intuition and data-driven approaches to policing, illustrating that they are not mutually exclusive. They highlight how intuition can drive the use of technology, and technology can confirm intuitive presumptions. Moreover, intuition can call into question the output of technology and vice versa. The chapter highlights how the discretion characterising street-level bureaucrats, such as the police, is still present, but has now become technologically mediated. The chapter proposes a taxonomy of intuition-technology interactions and calls for ethnographic research to enrich our understanding of this relationship.

Emplit, Mauquoy, Vande Meulebroucke and van Praet also take on digitalisation through a different lens, namely the Belgian local police's use of body-worn cameras,

multi-tenant platforms for drafting reports and communicating, and crime analysis software. Like de Groes et al., they stress the mediating effect of technology, but also the possible tangible impacts of technology in terms of a decreased quality of police-citizen interactions and prediction error rates reinforcing bias and over-policing. The authors point to the importance of training and performance measures and the ramifications of non-technological factors.

The importance of training also shines through in the contribution by Paululat, Böing, Niculescu-Dinca and De Vries. This chapter contributes to our understanding of how virtual-reality (VR) and deepfake technology can be utilised in police training programmes. By testing the response of police officers to a stop-and-search VR scenario and a preceding video clip, the authors underscore the transformative potential of this technology in highlighting, for example, police behaviour influenced by biases, while calling for a nuanced investigation of the implementation of VR technology and the need to revisit our understanding of technological mediation.

Shifting theme to investigation and evidence, Westers, Berkenpas, Jansen, Schreurs, Alpar and Bluhm explore the challenges and opportunities that encryption presents for law enforcement and the justice system, revealing that current laws are insufficient to address the rapid evolution of encryption technology. Police authorities have adopted innovative methods, such as accessing Google backups to retrieve encrypted WhatsApp messages, which, once decrypted, provide reliable evidence. However, these practices have also sparked international legal challenges concerning the legality of data collection methods. The chapter also discusses the Dutch Innovation Criminal Procedure Act, a pilot programme aiming to modernise legal procedures to better address the complexities of encryption, emphasising the need for enhanced knowledge and expertise within the judiciary and prosecution services. The findings contribute to the ongoing public debate on encryption's impact on the legal landscape.

The balance between fundamental rights and investigatory methods is continued in the chapter by Kammersgaard Christensen, who in her chapter explores the scope of the EU Law Enforcement Directive, which is the EU's initiative to ensure the consideration of privacy in police work, with requirements of collecting personal data for specific purposes, minimisation of data, etc. This is crucial given the new technological capabilities for collecting vast amounts of data.

The dynamic of European law impacting national policing continues in the chapter by Sunde, Kammersgaard Christensen and Wachter Lentz, discussing how the EU Law Enforcement Directive sets boundaries for police when collecting personal data as part of an investigation. The Directive mandates that data should only be collected for a specific purpose, with provisions for data deletion, etc. This is particularly relevant in the digital age, where large amounts of data ('data lakes') can be gathered. Despite the Directive's purpose, a significant scope is left for national implementation, as illustrated by Danish and Norwegian legislation. Traditionally, these two countries have had similar approaches to criminal law and procedure, but their implementation

*LENE WACHER LENTZ AND MARKUS NAARTTIJÄRVI*

of the Directive shows significant differences. Notably, Danish law presents a risk of collecting large amounts of data that could be reused for other purposes.

The chapter by Calleja develops an important understanding of the emerging tactic of disrupting computer-enabled crime in relation to the concept of interference as outlined in Articles 8 and 10 of the European Convention on Human Rights. These tactics include disruption of internet access and influencing cognitive processes. The chapter addresses the issue of how the interpretations of what constitutes an interference are evolving, whereby different conditions apply, including legality and proportionality, and highlights important fundamental rights considerations to consider when implementing disruption tactics.

The next chapter of the book, by Stol, Jansen and Landman, explores the impact of digitalisation on the police function, highlighting how it has changed the landscape by providing new opportunities for external actors to influence the rule of law. These changes relate to shifts in organisational, informational and normative capacities. The chapter examines how digitisation affects crime and public order, prompting the police to reconsider their role.

Shifting theme, our last two contributions look at how social media can be used to incite people to commit disturbances, but also to urge them into actions rivalling police functions. Bantema begins by looking at how local bylaws have been used in the Netherlands to counter disturbances caused by social media posts. It raises the question of whether, similar to banning individuals from physical areas in a city, it would be possible to ban individuals from digital areas on social media platforms. This inquiry touches on the fundamental issue of whether digital spaces can be equated with physical ones. The chapter also discusses whether local bylaws are the appropriate legal tool for addressing such issues, particularly when restrictions on the fundamental right to freedom of expression are involved.

The somewhat contrasting use of social media is explored in the final chapter by Rianne Dekker, who analyses the new technological possibilities for citizens to investigate, form collective movements in search of individuals, surveil areas, solve crimes or confront perpetrators. It explores how online citizen-led policing relates to government law enforcement. One driving factor for online citizen-led policing could be considered to be current government inaction in certain crime areas, alongside rising expectations for higher security levels in society.

We are happy to see that the chapters in this book capture the pervasive and multidimensional way digital technologies impact policing, and represents a cross-section of topics that have emerged from our conferences.

## 1.5 THE FUTURE

The contributions in this book stand as testaments to the increased importance of *the digital* in modern policing. They also illustrate how a plurality of methodologies, disciplines and geographies can contribute to our understanding of policing in the digital society. As such, this book provides a clear reminder of the importance of academic exchanges and networks daring to take steps beyond one's comfortable home turf. In this, we owe a great debt of thanks to Wouter Stol, who both encouraged and practically enabled the growth of our network to the European level and who continues to be a kind yet relentless force in strengthening the network. Any academic endeavour is only as strong, and as enjoyable, as the people involved in it. Wouter has built on the pioneering steps taken in our earlier Nordic network to bring us to a point where we not only gather a wide array of interesting perspectives and insights into policing in the digital society, but also where we find ourselves surrounded by friends, who brighten our bleak winters by participating in our yearly conferences.

The PDS Network organising committee is happy with what has been achieved so far and at the same time believes that we have not yet reached the end of the network's development. The network could be strengthened, for example, by starting (multidisciplinary) working communities focusing on specific fields of interest, such as police patrols and new technologies or the tension between digitised police surveillance and privacy. Since the role of the police is an important part of the social structure of our society, we need people – professionals as well as scholars from different disciplines – who study and discuss the developments in policing in our digital era, people searching for answers to practical issues as well as to the legal and ethical dilemmas that go along with modern policing. Join the PDS Network!



## 2 LOCAL POLICE, DIGITALISATION AND IMPLEMENTATION

*Normative order, institutional logics and street-level coping strategies\**

Jan Terpstra

### **Abstract**

*In this chapter a theoretical framework is presented to understand how local police operational police officers use digital instruments and tools. This framework consists of elements derived from both institutional theory and the street-level bureaucracy approach. Four different forms of digitalisation of the Dutch local police are investigated: the processing of information, the use of social media, the use of real-time intelligence and of mobile applications, and the new visibility of the police. Three concepts prove to be especially relevant for understanding how operational police officers use and adapt digital instruments and tools: their normative order, their institutional logic, and the strategies these police officers as street-level bureaucrats use to cope with the constraints related to digitalisation.*

### 2.1 INTRODUCTION

Over the past decades, the far-reaching process of digitalisation has created both new opportunities and new challenges for the police. Views and expectations about the implications of digitalisation for police practice and police organisations have diverged considerably, from on the one hand the suggestion that the police will fundamentally change into a ‘knowledge profession’ (Ericson & Haggerty, 1997) or the belief that digitalisation will ‘hollow out’ the traditional police role (McGuire, 2021), and on the other hand the more sceptical view that the traditional style of policing will continue to dominate (Chan, 2003; Manning, 2008).

Especially the more radical views on the impact of police technology (either utopian or more dystopian) often tend to overlook a central issue: how digital tools and instruments are used in practice in daily police work. According to for instance Ariel (2019, p. 502), ‘the most common concern with technology in policing is its implementation failures.’ For that reason, in this chapter we will try to understand how the local police use digital tools in their everyday work and what processes and

---

\* This chapter is partially based on Terpstra (2024).

JAN TERPSTRA

factors may be involved. A theoretical framework is presented to understand the use of digital means and instruments by the local police. In this framework, elements will be incorporated that derive from both institutional theory (Scott, 2014) and street-level bureaucracy theory (Lipsky, 1980). These two approaches are generally not seen as related, but in this chapter they will be treated as complementary, with each perspective highlighting specific backgrounds of the use of digital instruments by the police.

Findings of empirical studies on the digitalisation of the Dutch local police are used to illustrate the relevance of this theoretical approach. These relate to four different types of digitalisation in the Dutch local police: searching of online information; the use of social media; mobile applications; and the new visibility of the police. The combination of these four cases makes it possible to study police digitalisation from different perspectives.

## 2.2 CONTEXT AND METHODS

This chapter concentrates on digitalisation in the local teams of the Dutch police. The main reasons why it concentrates on the local police are that this is by far the largest part of the police service, and that it enables us to see how 'traditional' and 'digital' ways of policing are combined and/or conflict in practice.

Since 2013, the Netherlands has had a national police force with 168 local teams. Their main tasks are patrolling the local area (including emergency response), community policing, criminal investigation of high-volume crime, and 'service and intake'. The number of officers in these teams varies between 60 and 200, with an average of about 150. In the Netherlands more specialised tasks, such as intelligence, investigation of organised crime, undercover work or the (regional) control room, are not tasks of the local police. For these specialised tasks, the local teams are dependent on other organisational units, often at a higher organisational level.

In many respects the Dutch local police teams have to follow national rules and procedures, and are dependent on formats, instruments and decisions made at higher organisational levels. For other issues, however, especially in relation to community policing, the local teams have a great deal of discretion to make their own decisions and to develop strategies that are tailored to local circumstances (Terpstra, 2021).

Most empirical data in this chapter are from a study on the digitalisation of the Dutch local police. It was conducted in three different local teams of the National Police between June 2019 and March 2020 (Terpstra et al., 2021). These teams are from both urban and rural settings and from different regions in the country.

In each team, documents were studied, interviews were conducted and daily police work was observed. Open interviews lasting an average of one hour were conducted with 60 individual police officers at different positions in local policing, divided across the three teams. The open, qualitative and non-standardised observations (Van Maanen,

1981; Ciesielska et al., 2018) of daily police work took 134 hours (about 17 complete shifts).

The empirical data of this study were supplemented with findings from several other studies on the use of digital tools and instruments by the Dutch local police. If presented data are from other studies, this will be mentioned explicitly.

### 2.3 THEORETICAL FRAMEWORK

The role of police technology and its practical impact are dependent on how technology is used, incorporated in and adapted to police practices, and on how at street level officers deal with its different enabling and constraining aspects (Orlikowski, 2000; Manning, 2001; Buffat, 2015; Høybye-Mortensen, 2019). These elements are also important for understanding why the use of digital tools in the police may fail to meet expectations and ambitions (Byrne & Marx, 2011).

The problems in the implementation and use of digital technology by the police are often seen as resulting from a lack of skills, knowledge and acceptance on the part of police officers, from a lack of perceived usefulness, and from a conservative culture that treats (technological) innovation as threatening the valued traditions of the police. Although these notions have a certain validity, this explanation has significant shortcomings (Manning, 2001). Lack of skills, knowledge, acceptance and perceived urgency, as well as anti-technology cultures, can better be seen as elements that should be looked at as part of what we try to understand. What is more, this explanation raises new questions of why this knowledge, skills, perceived urgency, etc. are so low. Therefore another approach is followed, combining institutional aspects and a street-level perspective that concentrates on how police officers try to cope with practical problems in relation to digitalisation.

To understand how the police use digital technology, it is important to notice that this is not only a matter of material resources and technical instruments, but also of social practices and their institutional setting (Reckwitz, 2002). Following Scott's (2014) notion of the three pillars of institutionalisation (the regulative, cultural-cognitive and normative pillars), a distinction can be made between three factors that police officers can draw upon in their recurrent practices when they use digital technology: resources, interpretive schemes, and normative rules.

These elements correspond to what Giddens (1979; 1984), in his theory of structuration, called structural modalities. These are both mediums and outcomes of social practices. These elements were also used by Orlikowski (2000) in her studies of the use of technology in organisations.

*Resources* can be defined as the institutional means that can constrain and regulate organisational behaviour, such as rule setting, monitoring and sanctioning. Resources

JAN TERPSTRA

may also be found in diffuse, informal ways of regulating and sanctioning (Scott, 2014, pp. 59-64).

*Interpretive schemes* consist of 'standardized elements of stocks of knowledge' that are applied by actors in their social practices (Giddens, 1979, p. 83). An important element of this knowledge, which may be tacit or explicit, is the *institutional logics*. According to Thornton, Ocasio and Lounsbury (2012, p. 2), these institutional logics 'represent frames of reference that condition actors' choices for sense-making, the vocabulary they use to motivate action, and their sense of self and identity.' In this context, the notion of *technoframe* is also important, guiding police officers in how they define and perceive technology and the use of it (Orlikowski & Gash, 1994). Police organisations may have long-term conflicts between different institutional logics (Terpstra & Salet, 2019; Gundhus, Skjevraak & Wathne, 2023).

In line with the third institutional pillar is what Goetz (2017) called the '*normative order*' in organisations such as the police. Goetz defined normative order as the interplay between bureaucratic structures and procedures, and agency subcultures. Where interpretive schemes give meaning to police officers, for instance about 'what is going on here', the normative order of the police, with its taken-for-granted norms, moral rules, expectations and workplace scripts, prescribes 'how (good) policing should be done' (Goetz, 2017, pp. 32-37).

Given this institutional perspective, it may be expected that how the police use digital technology depends on available resources, institutional logics and the normative order. Technological means will not be used or their use will be brought into line with the institutional circumstances if the necessary resources are not available or if their use is in conflict with the institutional logics and normative order that dominate the (local) police at that place and time (see also Koper et al., 2015, pp. 240-243).

In addition to these institutional aspects, practical issues in daily operational police work are also important in understanding how digital technology is used in police organisations. The street-level bureaucracy theory of Lipsky (1980) may be helpful to understand these processes of implementation. 'Street-level bureaucrats' is an umbrella term for public service workers who interact directly with citizens and who have a great deal of discretion in making decisions. Street-level bureaucrats are confronted with several forms of stress. A main source of strain is that the demand for street-level bureaucracy's services is chronically high and the resources insufficient to meet all needs. The police also have two other sources of stress. Police officers are confronted with stress resulting from perceived risks, uncertainty and danger in working the streets and in interacting with citizens. They may also be confronted with stress resulting from the relations with their supervisors (Terril, Paoline & Manning, 2003; Terpstra & Schaap, 2013). Street-level bureaucrats use several strategies to cope with the stress in their work, such as creating (more) autonomy, routinising, creaming, avoidance or bending the rules (Lipsky, 1980; Tummers et al., 2015).

It has often been suggested that digitalisation has radically changed street-level bureaucracy. Among the suggested changes are reduction of officer discretion, more control over frontline work, a shift to system-level bureaucracy, and replacement of street-level decision-making with automated decisions and of direct interaction with citizens with digital communication (Bovens & Zouridis, 2002; Ben & Schuppan, 2016; Busch & Henriksen, 2018; Høybye-Mortensen, 2019; Zouridis, Van Eck & Bovens, 2020). Zacka (2017, p. 27), however, has noted that it is important ‘not to overstate the speed, reach, and inevitability of technological change. [...] [S]treet-level bureaucrats still make plenty of significant decisions in the course of face-to-face encounters.’ Zacka’s reservation is even more relevant in the case of the local police. Even with all the digitalisation going on, the local police are still predominantly a street-level bureaucracy, a long way from a system-level bureaucracy with its automated processes of decision-making (Zouridis, Van Eck & Bovens, 2020). In the local police, direct relations between police officers and citizens are still the core of their frontline work. It also implies that much of the local policing still depends on how local police officers use their discretion. Even if local street-level police work has had its processes of digitalisation, the usual coping strategies of street-level bureaucrats can often still be found. This may be for example because digitalisation and traditional face-to-face encounters are combined (Hansen, Lundberg & Syltevik, 2018).

In this context it is also relevant that digital technology may have not only ‘enabling’ but also ‘constraining’ elements (Buffat, 2015) for operational police officers. As a result, technology may create (new) forms of stress at street level (Meijer, Lorenz & Wessels, 2012), for instance because it disturbs established routines or creates more (digital) red tape (Koper et al., 2015). Stress may also arise because technological tools are felt to be too complex, outdated or time-consuming (Terpstra & Kort, 2017). In such cases, police officers may decide to ‘decouple’ their tools, such as their mobile phone or app, and follow their own common sense or intuition (Sørensen & Pica, 2005; Sandhu & Fussey, 2021). They may use discretionary solutions to technological failures, such as shortcuts, workarounds or foot-dragging (Tanner & Meijer, 2015; Høybye-Mortensen, 2019; Brayne & Christin, 2021). Coping strategies can also be used if digitalisation is mainly perceived as managerial control or as one of the distrusted surrogate performance measures (Lipsky, 1980). In other cases, police officers may avoid the guidelines based on big data analyses, because they are sceptical about their validity (Drenth & Van Steden, 2020).

## 2.4 DOMINATING LOGICS AND NORMATIVE ORDERS

Although digitalisation has become an important element of contemporary society, our study showed that traditional styles of policing still dominate the local teams of the Dutch police (Terpstra et al., 2021). In one of the teams, about half of the citizens’ reports

JAN TERPSTRA

concerned cases with clear digital dimensions. However, the observations showed that, at the time of our fieldwork, digital cases receive hardly any attention, neither in everyday policing, nor in the daily briefing or other meetings. The main focus is on traditional policing of the streets. For most operational officers, what happens in the digital world falls largely outside their scope.

What is relevant is that in the Dutch police complex forms of cybercrime are transferred to specialised organisational units. Most of the problems that the local police act in relation to do not differ much from local policing issues in the past (see also Johnson et al., 2020). The main difference is that now many of these problems have a 'virtual dimension'. This means that now they generally develop faster, are less place-bound, and may easily escalate, including at other locations.

To understand the continued dominance of traditional policing, two sets of prevailing institutional logics and normative order in the local teams should be mentioned. The first is related to patrol work, including emergency response. The main focus here is on the reactive policing of generally unpredictable incidents. Despite the policy rhetoric in the Dutch police of problem-orientedness, information-led policing and context-driven work, in practice a fatalistic disbelief prevails about the possibility to steer police work. Patrol officers often describe their work as 'sticking plasters'; after each incident they leave quickly the scene for the next incident. Building up long-standing relations with citizens is not seen as realistic.

The related normative order is a combination of the action of policing, the thrill of unpredictability and the moral value of doing visible police work in public, either as first aid and support to citizens in need, or as a practical authority in the enforcement of rules and public order. Although patrol officers often complain about time pressures and staff shortages, it is the combination of pressure, unpredictability and the moral values of first aid and of authority in public places that often motivates and fascinates them (Terpstra, 2002; Terpstra et al., 2016).

The second set of institutional logics and normative order is mainly associated with community policing. Several elements can be distinguished. First, there is the need to 'know and be known', a practical but also moral requirement. Community officers should be informed in detail about what is going on in their neighbourhood to be able to contribute to problem-solving and to promote citizens' trust. Local residents should also know them in person. Second, the building up of trust requires informal and personal relationships. Building up relationships, creating trust, becoming 'known' and collaboration with citizens require a lot of time, something that may conflict with the time pressures and short-term perspectives of daily policing, especially in patrol and emergency work. An important moral aspect in the views and logic of Dutch community officers can be found in their need for involvement with the problems of their neighbourhood and its residents.

In most local teams, the first institutional (patrol work) logic predominates. Although the two sets of institutional logics and normative order may conflict, they

share a reactive approach. Even if prevention is often defined as a key task of community policing, in practice this is hardly the reality in the Dutch police (Terpstra, 2010).

These institutional logics/normative orders have consequences for how digital tools and instruments are used in local policing. Street work, personal contact with citizens and practical experience are valued as more important than the use of abstract data or the use of social media (Egbert & Leese, 2021). These are seen as risks for traditional routines in policing. Many local police officers fear that digitalisation will divert the attention from 'real police work' (Tanner & Meijer, 2015). They feel uncomfortable about digital instruments replacing personal relationships and personal knowledge:

Yes, warm contact is better. That is our power. [...] Human relationship is important, putting a hand on a shoulder. If a youngster is fearful, for instance about sharing information with us, in face-to-face contact I can try to tackle it. I think that social media can make a contribution [...] and that it can help us, but only in addition to warm contacts.

## 2.5 FOUR TYPES OF DIGITALISATION

The institutional and coping approach presented in this chapter can be illustrated with four different forms of digitalisation in the local police. These forms of digitalisation are: searching and processing of information, the use of social media, real-time intelligence and mobile applications, and the new visibility of the police. These were selected because they were often mentioned by local officers in the Dutch police as important examples of digitalisation in their work.

### 2.5.1 *Searching and processing of information*

Both digitalisation and the increasing importance of intelligence-led policing have resulted in a growth of desk and computer work. Community and patrol officers often spend more time on making reports at their computer than on street work and on their visibility in the neighbourhood (Terpstra, 2008). Especially when officers feel that digital instruments are slow, outdated or too complex, computer work is felt to be a burden that distracts from 'real' police work (see also Koper et al., 2015).

In relation to digitalisation, one of the policy expectations is that the local police should be informed about relevant problems and situations not only in the 'physical' but also in the 'virtual neighbourhood'. For that reason, members of local teams should collect relevant information on the internet and social media in a proactive way. To collect this information, they can use OSINT (open-source intelligence), a technique to search open sources. In practice, the local police rarely use this tool (Landman &

JAN TERPSTRA

Groothuis, 2022). Most local police officers do not have the skills for open internet searches. What is more, this proactive work does not fit their view of 'real police work': incident-driven street work, and not preventive-oriented work at the computer or desk (Manning, 2008). In some local teams, this internet searching is only done by a special officer, the so-called digital community officer (see below).

Although some local officers avoid the use of the internet to collect information as far as possible, others are more active in this respect. They use several, mainly reactive methods to collect online information about neighbourhood problems. The first method is quite traditional: they are informed by residents about certain incidents on social media, for instance that a person living in the neighbourhood has been threatened because of rumours that he is a 'paedo' (Terpstra, 2019).

To collect information, some community officers become a members of a closed social media group. Sometimes they use a fake account, so as not to be recognised as a police officer. Other community officers use a personal account, for the same reason. Both practices are now forbidden by the National Police. As a consequence, in one of the teams studied the digital community officer had to put an end to his activities on Facebook. In another team, the digital surveillance on the web raised legal problems in relation to the distinction between surveillance and criminal investigation and the limits of systematic observation.

Local teams may also get information from specialised intelligence units. This information may refer to specific problems that the local police should act upon. In other cases, this information transfer is part of predictive policing. Many Dutch local teams use a CAS (Crime Anticipation System), focused on the prevention of residential burglary via the use of algorithmic analysis and crime mapping. This system is used to decide when and where local police officers should patrol. This form of predictive policing may restrict the traditional discretion of local police officers (Landman, 2023). Although police officers are generally quite positive about predictive policing, its impact on daily policing is somewhat limited (Mali et al., 2017). Street-level officers often prefer practical knowledge and feel that this is more suitable than abstract data (Egbert & Leese, 2021). Drenth and Van Steden (2020, p. 497) showed that even with CAS information, members of a special local police squad mostly use their discretion to follow their own routines, informal knowledge and experience. They question the effectiveness of CAS, emphasise contextual information, have their own priorities and stress that policing is more than crime-fighting.

To compensate for the lack of digital skills, expertise and motivation in local police teams, special organisational positions and units have been created, such as the aforementioned digital community officers. Their tasks include proactive digital surveillance of open online sources, collecting information about social media groups in the work area of the team, prevention activities (such as lessons at schools), giving digital support to criminal investigation of the local team and promoting digital expertise and skills of colleagues in their local team. Digital community officers do not

have their own (physical) community or neighbourhood. Contrary to what this job title suggests, the role is more a local intelligence officer than a community officer.

Specialised units, such as the regional information unit or the public order intelligence team, may also be relevant. These units have to provide information to local police teams, both in relation to specific problems and as an element of predictive policing.

This organisational differentiation and specialisation may raise new tensions and conflicts (Giacomantonio, 2015). Community officers often feel that the information they receive from the intelligence department is superficial, does not bring something new and is not helpful in their work. In their view, their practical knowledge, expertise and discretion, but also their moral skills (McGuire, 2021) are ignored. These tensions and conflicts are not just a matter of inadequate communication, coordination or transfer of information (although these may be part of it). More important is the clash of perspectives, logics and normative rules between local teams and intelligence departments: incident-driven versus data-driven, reactive versus proactive, practice-based knowledge versus context-free abstract knowledge, personal, idiosyncratic and informal knowledge versus formalisation. In other words, a lack of fit between street-level practical knowledge and more technical and abstract forms of knowledge or data (also Drenth & Van Steden, 2020; Brayne & Christin, 2021; Egbert & Leese, 2021; Gundhus et al., 2023). Local police officers use different strategies to respond to these tensions. Some of them try to maintain their 'intuition-led style of policing' as far as possible, even against the current (Sandhu & Fussey, 2021, p. 78).

The introduction of special officers and units seems to assume that the digitalisation of local police can be managed by specialists, isolated from the (rest of the) local police team. This raises the question of whether this strategy of differentiation and specialisation will leave much of traditional policing intact, including in the long run.

### 2.5.2 *Social media*

Staff and supervisors in the local teams often have high expectations about the use of social media by the police. They expect that social media will make it easier to send messages to large audiences, will promote open dialogue and citizens' trust in the police, and improve the police's image and citizen engagement (see also Broekman et al., 2017; Walsh & O'Connor, 2019). Several studies have shown that these expectations are often too optimistic (Crump, 2011; Brewster et al., 2018; Bullock, 2018; Czapska & Struzinska, 2018).

Despite these ambitions, only a small number of police officers in the local teams are regular users of social media. Most of them say that they are 'not interested' in social media. In addition to open searches for information, the use of social media by the local police is mainly a one-way form of communication, meant to disseminate

JAN TERPSTRA

police-relevant information. This is generally not focused on the promotion of open dialogue or on improving citizen participation (also Crump, 2011; Bullock, 2018). The most promising initiatives are so-called WhatsApp neighbourhood groups, a nationwide phenomenon. However, the local police have a very limited role here, only at the start-up phase of these groups, leaving them to the responsibility of the municipality (Terpstra & Salet, 2022). In a similar way the local police try to shift the responsibility for preventive use of social media to the municipality, because this would not fit the traditional view of policing as street work:

That is a task of the municipality, and not our task. [...] I think it is better that the municipality will provide this information and that our officers will be out on the streets to make it more secure there.

In the early days of police use of social media, some officers got in trouble because afterwards the information they had posted on social media was seen as an infringement of privacy rules, as sensitive information, or as damaging the police's image. Some of these officers were sanctioned for this. Stories about these incidents continue to circulate, and are one of the reasons why significant numbers of police officers decide not to use social media.

In some local teams, conflicts and tensions have arisen about the use of social media. To control the use of social media and communication with the general public, it was decided that citizens should no longer be able to report crime and other problems via Facebook, for instance. In several teams, community officers were no longer allowed to have their own Facebook account. Since then, each team has had only one central Facebook account (see also Dekker et al., 2020). Community officers are not happy about this because they lost an opportunity to tailor their communication via Facebook to the specific situation of their neighbourhood (Terpstra, 2019).

These examples illustrate how the use of social media is often adapted to fit into the traditional, reactive logic of police work (Crump, 2011). Prevention, open dialogue with citizens or the promotion of citizen engagement fall outside this logic and normative order of 'real police work'. The use of social media is generally ignored if it is perceived as risky and stressful.

There are exceptions to the generally limited use of social media. In our study, as well as in other studies (Terpstra et al., 2016; Terpstra, 2019), we observed community officers who were very active on social media. In their view, social media makes it possible to collect information about what is going on in their neighbourhood and to provide relevant information to residents. They also felt that mainly young people expect the police to be visible and approachable on social media. For these officers, the enabling aspects of this type of digitalisation outweigh the constraining aspects.

### 2.5.3 *Real-time intelligence and mobile applications*

Since 2014, each of the 10 regional units of the Dutch police has had a Real Time Intelligence Centre (RTIC). In case of urgent calls or incidents, officers of the RTIC have to collect relevant information, both from police systems and other sources, that may be relevant for patrol officers who are driving to an incident. This information has to be communicated within five minutes. The information is generally not sent directly to the patrol officers in the car, but via the control room, where it is decided whether the information will be communicated to the street officers.

Scholtens et al. (2016) found that most of the information collected by RTIC officers never reaches the officers on the street. Several factors contribute to this failed implementation of RTICs, some of which are related to the norms, logic and strategies of patrol officers. Except in urgent situations, patrol officers prefer to search for information on their own, for example on their mobile phone. This makes them less dependent on the RTIC and can make their work much easier to do. The combination of driving very fast to an emergency and the reading of information delivered by the RTIC is often problematic. When officers are driving fast and using blue lights and sirens, the co-driver is also more concentrated on preventing dangerous traffic situations than on reading incoming information on their screen or mobile phone. After arriving at the scene, police officers do not take the time first to read RTIC information, but leave the car to hurry to the incident. This is even more the case because patrol officers often believe that RTIC information is generally not very useful.

In some regions, every time new RTIC information is sent by the control room, a red light starts flashing on the dashboard in the patrol car. Patrol officers can use a button to let the control room know that they have read the information. This stops the flashing light. However, patrol officers may feel that the flashing is irritating and disturbs safe driving, which is why they may use the button to stop the flashing without having read the RTIC information.

In 2016, the Dutch National Police introduced an application that operational police officers can use on their mobile phone when they are on the street or in the car. This app, called MEOS (More Effective On the Streets), can be used to establish the identity of a person by scanning their ID documents, to scan a fingerprint, or to check information from several files and from registration documents about, for instance, a person's driver's licence or whether they are the subject of administrative measures such as restraining orders. The app can also be used to issue a digital ticket.

In 2018, an app called Proco was added to MEOS. This app was introduced because of debates about ethnic profiling by the Dutch police. By using Proco, police officers are able to see if an individual citizen was stopped before, in which case they could refrain from a new stop. Proco automatically counts how often police officers consult the system and stop citizens. This information is reported to chief officers of the local

JAN TERPSTRA

police team. The aim of this app is to prevent ‘unnecessary stops’ and to make police-stop practice more transparent and accountable.

MEOS has both enabling and constraining effects (Buffat, 2015) on the daily work of street-level police officers. In general, MEOS means that operational police officers have more autonomy and are less dependent on the back office for information. By using MEOS, they can do their work faster and take care of administrative work when they are on the street or in the car. However, many officers do only a small part of their administrative work on their mobile phone, because they feel that typing on a mobile phone is inconvenient. They return to the police station to do the rest of their administrative work there. Often this means twice the work and a loss of information (Molenaar et al., 2020).

Street-level police officers use the Proco app less often than was assumed. The main reason is that the introduction of this app was felt to create more hierarchical control over their work. At first, Proco received much resistance from among local police officers, because it was perceived as an accusation that they discriminated against members of ethnic minorities. Doubts about the effectiveness of Proco and the reliability of the information about former stops contributed to the resistance and non-use. Officers often refuse to use the app on the street, because working on their mobile phone there might have a negative impact on their interaction with citizens (Molenaar et al., 2020).

In practice, the use of these apps may be contrary to the original intentions. Some officers use information from MEOS to ‘hunt’ for certain cars (Terpstra et al., 2021), as a sort of human Automated Number Plate Recognition (ANPR). About a third of the officers in the study by Molenaar et al. (2020) used information from Proco about former stops by the police not as a warning not to stop an innocent person again, but in the opposite way: if a person had been stopped so often by the police, it was assumed that there must have been a good reason for it, and as a consequence, they stopped the person again. This illustrates how police officers adapt the use of digital instruments so that they fit into their existing practices, routines, normative order and institutional logic. If the digital instrument is too complex, contributes to activities that are defined as not real police work or is considered to represent more managerial control, police officers may ignore these digital tools, enhance their autonomy or use them only selectively.

#### 2.5.4 *New visibility*

The increasing use of mobile phone cameras, social media and video-sharing platforms has contributed to a ‘new visibility’ of the police (Thompson, 2005; Brown, 2016). It has become more difficult for the police to control information about police conduct (Goldsmith, 2010; 2015; Haggerty & Sandhu, 2014). The reasons why citizens record

police conduct vary from counter-surveillance to citizen journalism (Sandhu, 2016; Walsh & O'Connor, 2019) or a form of 'fun'.

Police officers are generally aware of the fact that at any moment on the street they can be filmed, and that videos may simply be posted on social media and have a wider impact, including outside the context of their conduct. One of their complaints is that the videos do not give accurate information about the context of police action and result in a biased image of what really happened:

You often see only the violence that was used. But not what happened before. These are often videos without any context.

In the Netherlands, citizens are formally allowed to film police officers working in public, as long as they do not disturb 'necessary' police work. Unless this is the case, police officers are not allowed to stop the recording or to confiscate a mobile phone.

Still, this new visibility of the police is often perceived by police officers as a source of stress and tension in their work. Although many of them say that the risk of being filmed on the street does not change their behaviour, they notice that this issue often bothers their colleagues and has an impact on their behaviour. This is not only a matter of strain in police street work. Videos made by citizens can also be used for formal complaints against the police, which may be a source of tension in their relations with higher-level supervisors.

Police officers use several strategies to cope with this new visibility. Sandu (2016) found that police officers try to avoid certain situations so that they can minimise the 'risk' of being filmed. In our study it was found that police officers may try to stop the anonymity of the video-maker by asking for their ID and then calling their name many times, supposing that it will then become uninteresting to continue the video-making and post it on social media.

Some police officers decide to use their own body-worn camera and to start to record the situation from their own perspective. According to police officers this will often stop the video-making by members of the public:

As soon as there is a colleague with a bodycam, you often see that their behaviour changes: shit, now we are recorded. [...] Somehow that has an impact. They cannot hide anymore behind their screen. [...] As soon as that the bodycam is working, the aggression will become less. It seems as if at that moment people become aware of what they are doing.

## 2.6 CONCLUSION

This chapter has focused on how local police use digital tools and instruments. Although the four types of digitalisation that were analysed show considerable differences, the findings are in line with the theoretical framework presented. In their use of digital tools, police officers draw upon their normative order and institutional logic. They try to fit the use of digital instruments into their traditional, reactive, personalised and practice-oriented normative and cognitive framework of policing and police work. In addition, operational police officers use strategies to cope with the constraining aspects of digitalisation. The resulting internal and external strain can range from the irritation of a flashing light on the dashboard of the patrol car or the fear of a loss of autonomy, to the feeling of unjust treatment because of citizens' videos of police conduct posted on social media.

This theoretical framework consists of two perspectives, the institutional approach and the street-level coping theory. These two approaches are generally seen as unrelated. The analysis in this chapter, however, shows that combining them is useful because each perspective highlights specific, complementary elements and factors. If the analysis were limited to one of these approaches, either the cultural-institutional aspects or the use of coping strategies in response to the practical constraints and stress created by digital instruments would be left out.

This theoretical perspective is not only relevant for understanding how local police officers use and negotiate digital instruments and tools. It also shows why the digitalisation of the local police is often a process with frictions, tensions, resistance and delay. Even if local police officers use digital instruments, they are often ambivalent and sceptical about digitalisation. This is an important reason why digitalisation, despite its potential for radical change, generally does not result in fundamental changes to local policing (Manning, 2001; 2008; Chan, 2003). Digital innovations may be perceived by local police officers as threatening not only their work routines, but also how they define and perceive of police work and their role and identity (Tanner & Meijer, 2015; Brayne & Christin, 2021; McGuire, 2021).

Practical knowledge, personal relations and direct contact with citizens are often seen by local police officers as more important and valuable than abstract data or decisions by digital systems. Viewed from this perspective, many of the adaptations and strategies used by local operational police officers in relation to digitalisation are linked to conflicts about the emerging abstract nature of police organisations (Terpstra, Fyfe & Salet, 2019; Terpstra & Salet, 2022).

The analysis in this chapter shows the relevance of two of the three pillars of institutionalisation as distinguished by Scott (2014) in understanding how local police use digital instruments: the cultural-cognitive pillar with its institutional logic, and the normative pillar with its normative order of local police officers. Contrary to what was hypothesised, this study could not confirm the relevance of the third, regulative,

pillar. It was assumed that the digitalisation of the local police would (also) be regulated and controlled by top-down guidelines and potential sanctions. However, evidence for the importance of this third pillar could not be found. This may be a consequence of the decision of the Dutch National Police to have what was called an ‘incremental’, ‘bottom-up’ policy on the digitalisation of the local police, leaving much scope for the local teams to decide how to deal with new technologies. This third institutional element of regulation and resources may still be relevant in other processes or settings of police digitalisation. Other studies, in other (national) contexts, are needed to see what the relevance is of this theoretical perspective, including the importance of the regulative pillar, for understanding processes of digitalisation of police and police work.

The theoretical approach presented here can also have practical implications. For digital innovation in policing, it is important not to look only at the material and technological aspects. The promotion of skills, expertise and perceived acceptability is not enough for successful implementation. It is important that before a certain digital innovation is introduced in practice, there is an investigation to see how it will relate to the existing cultural-institutional setting of the local police and whether it will create additional constraints and stress for police officers (Adang et al., 2023). If this is omitted, the problem is not so much an ‘implementation failure’ (Ariel, 2019) caused by local police officers, but rather a failure to adapt the development of the technological instrument to the institutional and practical setting of the local police.

## REFERENCES

- Adang, O.M., Mali, B., & Vermeulen, K. (2023). A prospective Police Technology Assessment of the use of non-penetrating projectiles for public order maintenance and riot control. *Policing: A Journal of Policy and Practice*, 17, paad076.
- Ariel, B. (2019). Technology in policing. In D. Weisburd & A.A. Braga (Eds.), *Police Innovation. Contrasting Perspectives* (pp. 485-516) (2nd ed.). Cambridge University Press.
- Ben, E.R., & Schuppan, T. (2016). E-Government and the Transformation of Professionalism: The Case of the Police. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 2667-2676). IEEE.
- Bovens, M., & Zouridis, S. (2002). From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control. *Public Administration Review*, 62(2), 174-184.
- Brayne, S., & Christin, A. (2021). Technologies of crime prediction: the reception of algorithms in policing and criminal courts. *Social Problems*, 68(3), 608-624.
- Brewster, B., Gibson, H., & Gunning, M. (2018). Policing the community together: the impact of technology on citizen engagement. In G. Leventakis & M.R. Haberfeldt

JAN TERPSTRA

- (Eds.), *Societal Implications of Community-oriented Policing and Technology* (pp. 91-102). Springer.
- Broekman, C.C.M.T., et al. (2017). Social Media: facilitator and stimulator of community policing. In P.S. Bayerl et al. (Eds.), *Community policing: a European perspective* (pp. 167-191). Springer.
- Brown, G.R. (2016). The blue line on thin ice: police use of force modifications in the era of cameraphones and YouTube. *The British Journal of Criminology*, 56(2), 293-312.
- Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing: a review of the research on implementation and impact. *Journal of Police Studies*, (3), 17-40.
- Bullock, K. (2018). The police use of social media: Transformation or normalization? *Social Policy & Society*, 17(2), 245-258.
- Buffat, A. (2015). Street-level bureaucracy and e-government. *Public Management Review*, 17(1), 149-161.
- Busch, P.A., & Henriksen, H.Z. (2018). Digital discretion: A systematic literature review of ICT and street-level discretion. *Information Polity*, 23(1), 3-28.
- Chan, J.B.L. (2003). Police and new technologies. In T. Newburn (Ed.), *Handbook of Policing* (pp. 655-679). Willan.
- Ciesielska, M., Bostrom, K.W., & Ohlander (2018). Observation methods. In M. Ciesielska & D. Jemielniak (Eds.), *Qualitative methods in Organization Studies* (pp. 33-52). Palgrave MacMillan.
- Crump, J. (2011). What are the police doing on Twitter? Social media, the police and the public. *Policy & Internet*, 3(4), 1-27.
- Czapska, J., & Struzinska, K. (2018). Social media and community policing implementation in South Eastern Europe: a question of trust. In G. Leventakis & M.R. Haberfeldt (Eds.), *Societal Implications of Community-oriented Policing and Technology* (pp. 47-54). Springer.
- Dekker, R., van den Brink, P., & Meijer, A. (2020). Social media adoption in the police: Barriers and strategies. *Government Information Quarterly*, 37(2), 101441.
- Drenth, A.R., & van Steden, R. (2020). Everyday patrol work for a data-driven flying squad: advancing theoretical thinking on police craftsmanship in interacting with civilians. *Journal of Crime and Justice*, 43(4), 486-501.
- Egbert, S., & Leese, M. (2021). *Criminal Futures. Predictive policing and everyday police work*. Routledge.
- Ericson, R.V., & Haggerty, K.D. (1997). *Policing the risk society*. Clarendon Press.
- Giacomantonio, C. (2015). *Policing integration: The sociology of police coordination work*. Palgrave.
- Giddens, A. (1979). *Central Problems in Social Theory. Action, structure and contradiction in social analysis*. MacMillan.
- Giddens, A. (1984). *The Constitution of Society: Outline of the theory of structuration*. Polity Press.

- Goetz, B. (2017). *On the Frontlines of the Welfare State. How the fire service and police shape social problems*. Routledge.
- Goldsmith, A.J. (2010). Policing's new visibility. *The British Journal of Criminology*, 50(5), 914-934.
- Goldsmith, A.J. (2015). Disgracebook policing: social media and the rise of police indiscretion. *Policing & Society*, 25(3), 249-267.
- Gundhus, H.O.I., Skjevraak, 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.
- Haggerty, K.D., & Sandhu, A. (2014). The police crisis of visibility. *IEEE Technology and Society Magazine*, 33(2), 9-12.
- Hansen, H.T., Lundberg, K., & Syltevik, L.J. (2018). Digitalization, street-level bureaucracy and welfare users' experiences. *Social Policy & Administration*, 52(1), 67-90.
- Høybye-Mortensen, M. (2019). Street-level bureaucracy research and the impact of digital office technologies. In P. Hupe (Ed.), *Research handbook on street-level bureaucracy* (pp. 157-171). Edward Elgar Publishing.
- Johnson, D., Faulkner, E., Meredith, G., & Wilson, T.J. (2020). Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, 84(5), 427-450.
- Koper, C.S., Lum, C., Willis, J.J., Woods, D.J., & Hibdon, J. (2015). *Realizing the potential of technology in policing*. George Mason University.
- Landman, W., & Groothuis, S. (2022). *Politiewerk op het Web. Een verkennend onderzoek naar online gegevensvergaring door de politie*. P&W.
- Landman, W. (2023). *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk*. P&W.
- Lipsky, M. (1980). *Street-level bureaucracy: Dilemmas of the individual in public service*. Russell Sage Foundation.
- Mali, B., Bronkhorst-Giesen, C., & den Hengst, M. (2017). *Predictive Policing: Lessen voor de toekomst. Een evaluatie van de landelijke pilot*. Politieacademie.
- Manning, P.K. (2001). Technology's ways: information technology, crime analysis and the rationality of policing. *Criminal Justice*, 1(1), 83-103.
- Manning, P.K. (2008). *The Technology of Policing. Crime mapping, information technology, and the rationality of crime control*. New York University Press.
- McGuire, M.R. (2021). The laughing policebot: automation and the end of policing. *Policing & Society*, 31(1), 20-36.
- Meijer, A., Lorenz, L., & Wessels, M. (2021). Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems. *Public Administration Review*, 81(5), 837-846.
- Molenaar, J., et al. (2020). *Professioneel Controleren. Een onderzoek naar de pilot Proactief controleren*. Politieacademie.

JAN TERPSTRA

- Orlikowski, W.J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science*, 11(4), 404-428.
- Orlikowski, W.J., & Gash, D.C. (1994). Technological Frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, 12(2), 174-207.
- Reckwitz, A. (2002). Toward a theory of social practices. A development in culturalist theorizing. *European Journal of Social Theory*, 5(2), 243-263.
- Sandhu, A. (2016). Camera-friendly policing: how the police respond to cameras and photographers. *Surveillance & Society*, 14(1), 78-89.
- Sandhu, A., & Fussey, P. (2021). The 'uberization of policing'? How police negotiate and operationalise predictive policing technology. *Policing & Society*, 31(1), 66-81.
- Scholten, A., den Hengst M., & Waterreus, R. (2016). *Het Real-time Informeren van Noodhulpeenheden*. P&W.
- Scott, R.A. (2014). *Institutions and Organizations. Ideas, interests, and identities* (4th ed.). Sage.
- Sørensen, C., & Pica, D. (2005). Tales from the police: Rhythms of interaction with mobile technologies. *Information and Organization*, 15(2), 125-149.
- Tanner, S., & Meyer, M. (2015). Police work and new 'security devices': A tale from the beat. *Security Dialogue*, 46(4), 384-400.
- Terpstra, J. (2002). *Sturing van politie en politiewerk. Een verkennend onderzoek tegen de achtergrond van een veranderende sturingscontext en sturingsstijl*. IPIT/P&W.
- Terpstra, J. (2008). *Wijkagenten en hun dagelijks werk. Een onderzoek naar de uitvoering van gebiedsgebonden politiewerk*. Reed Business/P&W.
- Terpstra, J. (2010). Community policing in practice: Ambitions and realization. *Policing: A Journal of Policy & Practice*, 4(1), 64-72.
- Terpstra, J. (2019). *Wijkagenten en veranderingen in hun dagelijks werk. Verslag van een onderzoek*. P&W.
- Terpstra, J. (2021). Local policing in a nationalized police force: a study on the local teams of the Netherlands' national police. *Policing: A Journal of Policy and Practice*, 15(1), 251-262.
- Terpstra, J. (2024). Digitalization and local policing: normative order, institutional logics and street-level bureaucrats' strategies. *European Journal of Policing Studies*, 7(1-2), 36-58.
- Terpstra, J., & Kort, J. (2017). Rigmarole and red tape: background to a common police officers' complaint. *Policing: A Journal of Policy and Practice*, 11(4), 437-447.
- Terpstra, J., & Salet, R. (2019). The contested community police officer: An ongoing conflict between different institutional logics. *International Journal of Police Science & Management*, 21(4), 244-253.
- Terpstra, J., & Salet, R. (2022). Community policing in the age of the abstract police. In J. Terpstra, R. Salet & N.R. Fyfe (Eds.), *The Abstract Police. Critical reflections on contemporary change in police organisations* (pp. 81-101). Eleven.

- Terpstra, J., & Schaap, D. (2013). Police culture, stress conditions and working styles. *European Journal of Criminology*, 10(1), 59-73.
- Terpstra, J., Fyfe, N.R., & Salet, R. (2019). The Abstract Police: A conceptual exploration of unintended changes of police organisations. *The Police Journal*, 92(4), 339-359.
- Terpstra, J., Salet, R., van Duijneveldt, I., & Havinga, T. (2021). *Gebiedsgebonden Politiewerk in Ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Sdu/P&W.
- Terpstra, J., van Duijneveldt, I., Eikenaar, T., Havinga, T., & van Stokkom, B. (2016). *Basisteams in de Nationale Politie. Organisatie, taakuitvoering en gebiedsgebonden werk*. P&W.
- Terrill, W., Paoline, E.A., & Manning, P.K. (2003). Police culture and coercion. *Criminology*, 41(4), 1003-1034.
- Thompson, J.B. (2005). The new visibility. *Theory, Culture & Society*, 22(6), 31-51.
- Thornton, P.H., Ocasio, W., & Lounsbury, M. (2012). *The Institutional Logics Perspective: A new approach to culture, structure and process*. Oxford University Press.
- Tummers, L.G., Bekkers, V., Vink, E., & Musheno, M. (2015). Coping during public service delivery: A conceptualization and systematic review of the literature. *Journal of Public Administration Research and Theory*, 25(4), 1099-1126.
- Van Maanen, J. (1981). The informant game. Selected aspects of ethnographic research in police organizations. *Urban Life*, 9(4), 469-494.
- Walsh, J.P., & O'Connor, C. (2019). Social Media and Policing: A review of recent research. *Sociology Compass*, 13(1), e12648.
- Zacka, B. (2017). *When the State meets the Street. Public service and moral agency*. Harvard University Press.
- Zouridis, S., Van Eck, M., & Bovens, M. (2020). Automated discretion. In T. Evans & P.L. Hupe (Eds.), *Discretion and the Quest for Controlled Freedom* (pp. 313-329). Palgrave MacMillan.



### 3      DISENTANGLING THE INTERACTION BETWEEN PROFESSIONAL INTUITION AND TECHNOLOGIES IN POLICING

*Nienke de Groes, Vlad Niculescu-Dinca and Pieter Tops*

#### **Abstract**

*Police professionals often emphasise the value of their ‘sixth sense’ or intuition when making decisions at work. At the same time, there is a strong emphasis within data-driven policing on the role of ‘objective, hard data’, positioning data-driven technologies as a replacement for intuition. However, different forms of interactions can be observed where intuitive and data-driven decision-making processes are not necessarily mutually exclusive. For instance, intuition can incite the use of technology and technology can be used to confirm intuitive presumptions. Also, intuition could question the output of technology, and vice versa: technological output could cause one to doubt one’s own intuition. Research on these interactions is limited and more in-depth research is needed. This contribution focuses on the question of how professional intuition and technologies in policing interact. The chapter first presents an overview of a qualitative literature review on the effects of technologies on policing, after which a theoretical framework is discussed on how to conceptualise and study the interactions between professional intuition and technologies.*

#### 3.1 INTRODUCTION

What are the relations between professional intuition and digital technologies in policing? This is not a new question in policing studies but there have been new twists with the growing focus on data-driven practices. More and more technologies are making their entrance into the world of policing, for example in the domain of the fight against organised crime and so-called undermining in the Netherlands. Whereas ‘organised crime’ deals with hard and violent forms of crime, the term ‘undermining’ aims to cover their often invisible social ramifications. Undermining deals with the harmful social effects of organised crime, for example the lure of money and status that attracts people to criminal paths (Tops & Van der Torre, 2024; Tops et al., 2023). In the fight against organised crime and undermining there is a strong emphasis on ‘making the invisible visible’, which translates into a strong and growing focus on the potential of digital technologies. Data-driven technologies are introduced to better detect signs of organised crime and undermining (e.g. dashboards). Data-driven technologies are also

used in other policing domains, for example in daily police work to inform decisions about the deployment and distribution of police teams (e.g. the Crime Anticipation System (CAS) of the Dutch police).

The relations between technologies and police work are often problematised in broad conceptual strokes. On the one hand, digital technologies are presented as 'objective, hard data' and 'distinct entities' that can replace and outperform intuitive decision-making by police practitioners (Mastrofski & Ritti, 2000; Byrne & Marx, 2011; Ferguson, 2017; Dresser, 2019; Kennedy et al., 2021; among others). On the other hand, police professionals often emphasise the value of their 'sixth sense' or 'street smarts' when making decisions at work (Quinton et al., 2000). This tension can often lead to frictions, for instance in the process of introducing new technologies, or in practice, when police officers reject a prescriptive technological system if they perceive it as disregarding their agency and skills (Rattcliffe et al., 2019). This results in missed opportunities, problematic outcomes or a failure to meet the potential of both technologies and police organisations. Several studies show that new technologies within police organisations are mainly used to perform already existing tasks and do not involve innovations in the objectives or performance of the work (Manning, 1992;2008; Braga et al., 2011; Byrne & Marx, 2011; Miranda, 2015; Sanders & Condon, 2017, in Ernst et al., 2019). For example, information and analytical technology is mainly used to achieve short-term goals and is often heavily reactive to incidents rather than strategic goals and planning (Byrne & Hummer, 2017) and police officers prefer to follow their own judgement rather than have a technological system dictate to them where to patrol (Koper et al., 2015).

So, with a growing focus on data in policing practices, and the key role for technologies that is being stressed in approaches to crime and security issues, it is important to study how to best achieve the potential of technologies as well as of professional intuition in policing practices. How does professional intuition, the so-called 'sixth sense', of police practitioners interact and balance with digital technologies? We will need to engage more with this question if we are to make the most of the power of new technologies and the wealth of professional intuition. Therefore, the central research question of this chapter is as follows: *how can we conceptualise and study the interaction between digital technologies and professional intuition during policing practices?*

This chapter aims to outline a conceptual and methodological framework that is able to give us a better handle on the complex interactions between professional intuition and new technologies. The chapter first discusses the literature on data-driven policing, with an emphasis on the decision-making of police practitioners. Next, the chapter offers an argument for a theoretical framework on how to conceptualise and study the interactions between professional intuition and technologies. Then, the chapter presents a first taxonomy of intuition-technology interactions and proposes the concept of 'technologically mediated intuition' to enrich the understanding of intuition-technology interactions. Lastly, this chapter outlines the contours of an empirical case study to illustrate these conceptual advances.

### 3.2 **METHODOLOGY**

A qualitative literature review was performed to analyse perspectives in the literature on the effects of technologies on policing practices. The choice of articles for the qualitative review took place using qualification criteria and a selection process. First of all, the article should engage in the discussion of the effects of digital technologies on policing practices. Several search terms (in both English and Dutch) were used to come to a preliminary selection of articles:

- 1 terms related to policing: ‘police’, ‘policing’, ‘security’, ‘safety professionals’;
- 2 terms related to the use of technologies in policing: ‘big data’, ‘artificial intelligence’, ‘data-driven policing’; and
- 3 terms related to the practical meaning of the technologies in police work: ‘decision-making’, ‘discretionary power’, ‘task execution’.

Several databases were used for the literature search based on the compiled list of search terms: Web of Science, Scopus and Google Scholar. Next, a manual scan of the titles and abstracts of the articles found was performed. This scan focused on articles discussing the effects of technologies on policing practices. This resulted in a final selection of 69 articles. Of course, the set of articles discussing technologies in policing is much bigger. However, a larger selection was not necessary for a theoretical chapter aiming to discuss conceptualisations and establish a typology. The articles were read to analyse the ways in which the effects of data-driven policing on policing practices are conceptualised and studied, which will be outlined in the next sections (3.3-3.5).

### 3.3 **CONCEPTUALISING THE IMPACT OF DIGITAL TECHNOLOGIES ON THE POLICE PRACTICE**

One classification of the literature can be done according to the underlying attitude it has towards the impacts of technologies on policing practices. We noticed that the literature tended to fall into two broad categories: the more positive and the more critical view. According to the more positive studies, the use of digital technologies is expected to make policing more cost-effective and productive (see e.g. the theoretical contributions of Joh, 2015; Kubler, 2017; Ridgeway, 2018), support more efficient criminal justice decisions (Joh, 2015; the empirical contribution of Brayne, 2017), and lead to the reduction of crime rates (see e.g. the literature review by Pramanik et al., 2017). Digital technologies are often introduced with the promise of greater efficiency in the practice of policing, as well as more accurate and reliable decision-making compared to decisions based on intuition and personal expertise (see e.g. the systematic literature review by Busch & Henriksen, 2018). On the other hand, more critical studies underscore concerns about the potential impacts of big data on ethical issues like human rights and privacy (see e.g. the empirical

contribution of Richardson et al., 2019 based on the analysis of jurisdictions; and the theoretical contribution of Rowe & Muir, 2021) or point out that the introduction of digital technologies in policing has not provided the expected benefits in terms of more efficient policing (see the theoretical contributions of Chan et al., 2020; Browning & Arrigo, 2021). Although these studies on the impact of digital technologies on police practice might take conflicting views on whether impacts are positive or negative, there is a consensus that the introduction of digital technologies are changing the way in which policing activities are designed and implemented (Brayne, 2017): shifting from reactive action to preventive actions and proactive management styles (see amongst others the work of Van der Vijver & Terpstra, 2007; Van Brakel, 2016; Brayne, 2017; and the argumentative essays written by Schuilenburg, 2016; Sheehey, 2019). However, few studies concentrate on the impact of those technologies on the individual practices and experiences of police officers (see amongst others Stol, 1996; Bovens & Zouridis, 2002). When they do, the predominant perspective has been that of the impact of technologies on the discretionary power of police practitioners.

### 3.4 TECHNOLOGIES AND THE DISCRETIONARY POWER OF POLICING PROFESSIONALS

A large set of the analysed literature takes a view of policing practitioners as *street-level bureaucrats* (a term coined by Lipsky, 1980). As public service employees in direct contact with citizens in the performance of their duties, they have *discretionary power*: the ability to deviate from standard rules and to have a degree of autonomy about how to act within policy and organisational frameworks (Lipsky, 1980). The policing professional constantly makes decisions about how to apply rules, and which rules apply in which situation (for practical examples of this ‘room for action’, see Jansen et al., 2009). Police professionals make use of their professional intuition and case-specific experience to give meaning to this discretionary space, often referring to the importance of their ‘sixth sense’ or ‘street smarts’ when making decisions at work (see amongst others the empirical study of Quinton et al., 2000; a study based on storytelling on street-level bureaucracy by Maynard-Moody & Musheno, 2003; and the theoretical contribution of Tummers & Bekkers, 2014). This human nature of decision-making forms the basis of the discretion of street-level bureaucrats according to Lipsky (1980), as ‘[t]he nature of service provision [of street-level bureaucrats] calls for human judgement that cannot be programmed and for which machines cannot substitute’ (Lipsky, 1980, p. 161).

However, in recent decades digital technologies have made their entrance into police practice and the discretionary power of the policing professional. According to Bovens and Zouridis (2002), the nature of bureaucracy in public agencies (like the police) has changed due to technologies, from a *street-level bureaucracy*, via a *screen-level bureaucracy*, to a *system-level bureaucracy*. In this view, the bureaucrats

on the streets, characterised by face-to-face contact, have been gradually replaced by computers and lead to a screen-level bureaucracy where computerised routines influence their discretionary practices. In screen-level bureaucracy, public servants can no longer freely take to the streets, but are always connected to the organisation via the computer. Decision-making is no longer happening at street level, but has been accounted for in the design of the software. This screen-level bureaucracy evolves to system-level bureaucracy when fully automated technologies are in place in public agencies to make decisions based on collected data and predefined algorithms (Bovens & Zouridis, 2002). This can be seen, for example, in the application of surveillance technologies, and technological applications in crowd control.

This view can also be seen in the work of Mitrou et al. (2021). In their analysis of the degree of discretion and human control needed in AI-driven decision-making in governments, they conclude that the introduction of technologies in the practice of bureaucracy has diminished the role for human decision-making. Busch and Henriksen (2018) describe this as the concept of digital discretion, where the street-level bureaucrats' intellectual process of decision-making is shifting to a situation where ICT replaces some or all of the intellectual discretionary process.

However, in this view, in which technological decision-making is seen as taking over human decision-making, there is little conceptual space to still analyse the role of professional intuition other than in terms of diminished discretion. There is often a strong emphasis on the role of 'objective, hard data', positioning data-driven technologies as a replacement for intuition (see Byrne & Marx, 2011; Ferguson, 2017; Dresser, 2019; Kennedy et al., 2021, among others). Although the introduction of digital technologies is often framed as incompatible with intuition, different forms of interactions are still taking place where intuitive and data-driven decision-making processes are not necessarily mutually exclusive, which will be discussed in the next section.

### **3.5 DIGITAL TECHNOLOGIES AND PROFESSIONAL INTUITION: MUTUALLY EXCLUSIVE OR INTERACTING?**

How do digital technologies and professional intuition interact in policing practices? A study by Stol (1996) showed that police using information technologies might encounter situations in which the input by the technology and their own assessment of the situation do not align. This may incite several reactions; intuition could question the output of technology, and vice versa: technological output could cause one to doubt one's own intuition. Furthermore, evaluation studies on information technologies in police organisations indicate that the intuition of police officers might conflict with the acceptance and use of technologies within a data-driven working environment. Koper et al. (2015) conducted a multi-method evaluation study, consisting of surveys,

observations and interviews, on the effects of technologies in policing. One of the findings of this study was that some police officers would rather rely on their experience and intuition instead of leaning on new technologies that tell them what to do.

These examples illustrate that several interactions between digital technologies and professional intuition are present, but that there is a gap in the literature on how they interact during decision-making in policing and what the practical implications of those interactions might be. In order to understand the effects of data-driven technologies in police practice, it is important to unpack this interaction beyond diminished discretion: when does the technology or the professional intuition take the floor and how do they interact? How do police officers experience technologies? In the next section we suggest a theoretical framework that could help enrich our understanding of those questions.

### 3.6 THEORETICAL FRAMEWORK

#### 3.6.1 *Conceptualisation of digital technologies in policing*

We have seen that a ‘mutually exclusive’ conception offers a limited understanding of the interactions between human intuitive decision-making and technologically driven decision-making in policing. In an earlier section (section 3.4), we outlined the conceptualisation of the transformation of the street-level bureaucrat, via a screen-level bureaucrat, into a system-level bureaucrat. However, the concept of digital discretion tends to be underlined by a dualistic and deterministic view on technology that does not cover adequately the richness and complexity of human-technology interactions. This is because a dominant conception of technology in organisation theory is that of ‘means for converting raw materials or organisational inputs into outputs’ (Perrow, 1970; Scott, 1987, in Koen et al., 2019). And in this view, people are conceptualised as a ‘raw material’ to ‘which technology is applied to produce a service or product’ (Mastrofski & Ritti, 2000, p. 185). In this conception, technologies tend to be analysed as ‘distinct entities’, ‘well developed technically’ and helping an organisation realise its ‘predetermined and precisely defined’ goals (Koen et al., 2019). Therefore, such conceptions of technology are less able to pay attention to the dynamic interpretations that practitioners give to technologies beyond these goals. That is, in a highly digitalised working environment a practitioner could still give their own meaning to the technology, influencing if, when and how to use it or how to ‘read’ technological cues. In this ‘room for choice’, the role of intuition is apparent. For example, in the experimental study of Selten et al. (2022) AI recommendations were only trusted if they were in line with the professional’s intuition. At the same time, these conceptions of technologies as ‘distinct’ and ‘well developed’ pay less attention to the context of design of technologies when technologies are less defined, and to the role of designers in shaping police technologies. The study of Niculescu-Dinca (2021) shows how the designers of police algorithms implemented various dynamic

software-enabled entities in police technologies with various affordances for police professionals.

To understand the role of professional intuition and its interactions with technologies, a more dynamic approach to conceptualising intuition and data-driven policing is needed. Therefore, we propose a theoretical framework that can enrich our understanding of their co-existence and interaction, drawing on theories from philosophy of technology (Technological Mediation Theory) and psychology (Dual Process Theory).

### 3.6.2 *Technological Mediation Theory*

The theory of technological mediation offers a framework to analyse the roles that technologies play in human existence. Its central idea is that technologies are not adequately conceptualised as mere neutral tools, but as active actants helping to shape the relations between human beings and the world. Rather than approaching technologies as passive material objects, it sees them as active mediators of human-world relations (Ihde, 1990). Similarly, in the policing domain, they fundamentally mediate what is a suspect, a new criminal trend or suspicious behaviour (Niculescu-Dinca, 2018). Information infrastructures are far from neutral intermediaries that produce objective interpretations of reality; rather, they play an active role by mediating the practitioners' perceptions, decisions and actions. This does not imply a deterministic view. Technological mediation means that the user gives meaning to the technologies and their suggestions. A user can change, ignore or give a new meaning and interpretation to the intention of the developer, which is included in the design of the technologies (Niculescu-Dinca, 2021). At the same time, in seeing technologies as active mediators, Technological Mediation Theory also allows room to conceptualise the role and responsibility of technology developers. Databases and data infrastructures can not only be seen as neutral, technical means of collecting, processing and displaying data, but are more adequately conceptualised as complex socio-technical systems that do not simply reflect the world, but actively produce it (Lauriault, 2012; Kitchin, 2014). Therefore, this framework allows us to understand the processes in which developers *inscribe* values and their views into the design of technologies (Akrich & Latour, 1992).

### 3.6.3 *Dual Process Theory*

Dual Process Theory offers a framework to understand how human decision-making occurs (Kahneman, 2011). This theory introduces two different thinking processes that precede decision-making, referred to as system 1 and system 2. System 1 processing is characterised as an intuitive, automatic and unconscious process for 'everyday decisions'.

System 2 processing, on the other hand, requires much more effort as this process consists of logical judgement and a mental search for additional information gained through past learning and experience (Tay et al., 2016). An example of a situation where system 1 processing is used is tying one's shoelaces or dodging a bump in the street when walking. An example where system 2 processing is used is finding someone in a crowd, parking a car or doing maths.

According to this theory, system 1 processing is intuitive, automatic and emotional, and is based on simple rules of thumb (called heuristics). These heuristics help system 1 processing to come up with a quick solution with little mental effort. However, the use of heuristics could lead to biases in decision-making, for example confirmation bias, which describes people's tendency to process information in a way that is consistent with their prior beliefs (Nickerson, 1998, in Selten et al., 2022). In cognitive psychology there is an ongoing discussion on whether those two systems are exclusive or actually interact, and whether (the interaction of) the two decision-making processes are prone to biased decision-making (Da Silva, 2023).

In policing, intuition is often the area where biases (e.g. discriminatory decision-making) have been pointed out, while data-driven technologies are introduced as ways to mitigate those risks. However, several authors have shown that both types of decision-making processes are prone to biases and errors. For example, people may be more alert to information that supports their existing beliefs and intuitions (Kahneman, 2011). At the same time, however, they may also use analytical processing to analyse new information to justify their existing beliefs and intuitions, resulting from confirmation bias. The same fallacy can be seen in research findings on police intuition and data-driven technologies. For example, a study by Selten et al. (2022) seems to suggest that police officers only trust AI recommendations (aimed at improving the analytical process) if they confirm their professional judgement (the automatic and intuitive process).

However, how those two systems interact and are interrelated is currently under-researched, let alone in the context of decision-making in policing. The studies that are available on those two systems in decision-making in policing are inconsistent in their findings. A study by Wright (2013) suggests that police detectives utilise both intuitive and analytic thought processes and that each of these thought processes can result in accurate decision-making. A study by Rassin (2018) on the use of analytic thought processes by police investigators showed that analytic thought processes were superior to intuitive thought processes in decision-making. In contrast, Sahn and Von Weizsäcker (2015) came to the conclusion that intuitive thought processes outperformed analytic thought processes in policing.

These findings suggest that there is indeed some form of interaction, but that more and deeper research needs to take place on the form of this interaction(s). Do professionals use technology to confirm their intuition or to complement or reinforce it? What does this technologically mediated intuition look like in data-driven policing?

And what do these interactions mean for justifying and reasoning decisions in police practice?

The combination of Technological Mediation Theory and Dual Process Theory provides a framework to enrich our understanding of these interactions. Technological Mediation Theory illustrates how human-technology interactions could be approached in a more dynamic instead of a static or dualistic way, recognising the active and mutual influence of the technology, the practitioner and the designer. This framework helps to make the translation to practical implications; the focus is not on how technologies *should* be used (by reading policies and instruction guide), but first on how technologies *are* being used. Insight into the latter could provide input for policies on technology designs. Furthermore, Dual Process Theory demonstrates that it is important to go beyond a deterministic point of view when studying potential risks in decision-making in policing. Often biases are assigned to system 1, intuitive decision-making, whilst digital technologies are introduced as solutions to promote system 2 processing and to mitigate system 1's risks and biases. However, biases might arise in system 1 as well as in system 2 processing and also in the interactions of those two. Is this also the case for intuitive decision-making and digital technologies? The theoretical framework of this chapter provides guidance to capture more facets of professional intuition and digital technologies in decision-making.

### 3.7 PROPOSING THE INITIAL STEPS IN A TAXONOMY OF INTUITION-TECHNOLOGY INTERACTION

This section provides a typology of these interactions based on a qualitative literature review and proposes a new conceptual advancement. In addition, it argues for the methodological approaches best placed to offer data that is able to help in understanding these concepts. As human-technology interactions in policing are best studied (and understood) in a real-life setting, we outline the contours of an empirical study to examine these interactions.

#### 3.7.1 *How professional intuition and digital technologies interact*

Limited research has been conducted on the interactions between professional intuition and technologies in policing (Koper et al., 2015; Kennedy et al., 2021; Selten et al., 2022). Based on the work of those authors we can distil three interactions, taking place in the context of design and the context of use.

*Interaction in the context of design:* When a new technology is introduced, interaction can be seen in *conditional acceptance*. If (the design of) technology leaves little room for professional expertise, it affects the acceptance and use of the technology. Evaluation

studies on information technologies in police organisations indicate that the intuition of police officers might conflict with the acceptance and use of technologies within a data-driven working environment; some police officers prefer to stick with their ‘gut feeling’ rather than lean on new technologies that tell them what to do (e.g. Koper et al., 2015).

*Interaction in the context of use:* Technology and intuition might also interact in a *confirmative way*, whereby technological recommendations are only trusted when they confirm the professional intuition of the police officer (Selten et al., 2022). An experimental study by Selten et al. (2022) suggests that police professionals are prone to confirmation bias, as they only use algorithmic recommendations if these are congruent with their prior beliefs. On the one hand, confirmation bias in this context could lead to the preservation of professional intuition during their interaction with (AI) technologies. On the other hand, this bias also implies that police practitioners will not be capable of correcting prejudicial or biased algorithmic advice when it matches their prior beliefs (Kassin et al., 2013; Alon-Barkat & Busuioc, 2021, in Selten et al., 2022).

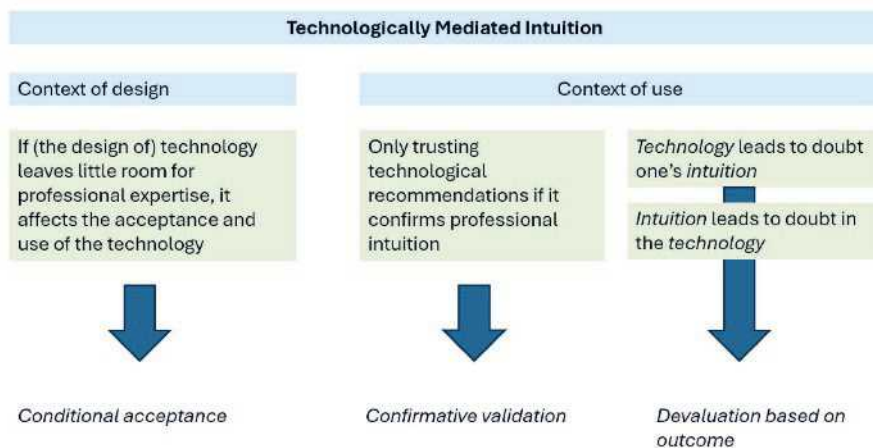
The interaction of intuition and technology can also lead to a process of *devaluation*. When technology and the intuition of the police practitioner contradict each other, this could lead to a devaluation of one or the other. As Kennedy et al. (2021, p. 1) states:

The outcomes of data analysis can be highly abstract and go counter to the intuition or experiences of police officers. This can leave analysts struggling to find common ground between the evidence that is presented through their analysis and the beliefs of members.

Besides these three examples of interactions, the authors of this chapter propose to add a theoretical lens to this taxonomy to be able to study the dynamics of the interactions: *technologically mediated intuition*. The concept of technologically mediated intuition is shaped in the highly digitalised work environment of police officers. Where traditional policing is characterised by interactions with citizens on the street, policing nowadays is more characterised as abstract policing where the police are more dependent on digitalised data systems and operate at a greater distance from citizens (Terpstra et al., 2022). In exploratory conversations with police practitioners on professional intuition, the practitioners explained that this intuition is built by spending hours on the street and gaining street smarts, for example on how criminals think and act. This professional intuition still plays a vital role in their daily practice, even in the interactions with data-driven technologies. The police practitioners underscore the importance of their intuition and skillset to *understand* technological cues, and to know *how* and *when* to follow up on those technological indicators. The concept of technologically mediated intuition invites the idea that the intuition of the professional in a data-driven policing environment is not going ‘extinct’, but is taking on a new shape. Due to their interaction with technologically mediated data collection and

-visualisation, the professional develops a new intuition. For example, a combination of plotted data mediates the perceptions of the professional who may interpret a deviation as suspicious. In combination with prior knowledge of the criminal phenomenon, the professional's decision becomes informed by a technologically mediated intuition as indicative of organised crime. This theoretical perspective allows room for both professional intuition and the active role of technologies, instead of simply considering them as objective tools.

**Figure 3.1** Intuition-technology interactions based on the literature review



### 3.7.2 *The need for ethnographic research to examine intuition-technology interactions in policing*

According to the conceptualisation of bureaucracy by Bovens and Zouridis (2002), the street-level bureaucrat is transforming, via the screen-level, to a system-level bureaucrat. Working in a highly digitalised environment, the role for human decision-making and discretion is considered to be diminished or even no longer present (Mitrou et al., 2021). However, the argument outlined in this chapter offers a new perspective on this: the nature of the street-level bureaucrat (discretion, human interference in decision-making) is still present, but now they are technologically mediated.

To adequately understand these technologically mediated forms of street-level bureaucracy we argue that more studies need to return to the street and engage in studying these technologically mediated practices. We propose that an ethnographic study could provide more in-depth insights in the interactions of intuition and technologies in policing. Ethnography through fieldwork is the 'close-up study of culture and how meaning [is] produced, distributed and understood' (Manning, 2014).

Research that is close to practice will not only increase the practical significance of the research, but also its theoretical significance (Tops, 2022).

To study the interaction of professional intuition and technologies in more depth, we have initiated an ethnographic study on the use of ANPR (Automated Number Plate Recognition).<sup>1</sup> ANPR systems use cameras on patrol cars or at fixed locations and data analysis to identify licence plates. ANPR technologies are also used to flag organised crime in transport flows (e.g. drug shipments on the highway). Several questions, derived from the theoretical framework, are addressed in this study: how does a professional's intuition interact with the technology in the decision-making process? How is the perception of the practitioner mediated by the (design of the) technology? Is the interaction between the practitioner and technology happening in more active (e.g. confirming intuition) or more subtle ways? How do technology developers inscribe their views of the criminal phenomenon into the design of an ANPR profile? A case study on ANPR could provide insights into those questions for three main reasons. First, ANPR is used by street-level bureaucrats (police patrols in mobile units). Second, the users have discretionary power whether to follow up on a technological cue or their intuition. Observation could provide insight into how police professionals' intuition interacts with ANPR when making decisions on the street. Third, this study includes the design aspect of ANPR. By also involving designers of ANPR in this study, we can explore how design affects and mediates police practice – and how police practice might also affect the design of the technology. Being able to simultaneously study the design of ANPR as well as police practice in the use of ANPR could deliver valuable insights.

### 3.8 CONCLUSION

With the increasing digitalisation of police work, more theoretical insights are needed to adequately understand the relation between intuition and digital technologies. How does this influence the perceptions, behaviour and actions of police professionals, beyond just a change in the nature or reduction of discretionary powers? This chapter has presented a conceptual and methodological framework to aim for a better understanding of the complex interactions between professional intuition and new technologies. The combination of Technological Mediation Theory and Dual Process Theory results in a more dynamic approach to understanding the various ways in which professional intuition and technology might interact and shows that they are not mutually exclusive. This chapter has presented a first attempt to arrive at a taxonomy of intuition-technology interactions. Furthermore, we have introduced the concept of technologically mediated intuition, to understand how digital technologies in police work do not in fact lead

---

<sup>1</sup> This ethnographic study is still in progress at the time of writing this contribution.

to the demise of intuition or discretionary powers of the police practitioner, but that the intuition and discretionary powers of the police professional are nowadays being technologically mediated.

We have proposed in this chapter to combine those theoretical insights with ethnographic research, to study the interaction between intuition and technologies close to the police practice. We propose that an empirical case study on ANPR is a good fit since it involves street-level bureaucrats interacting with technologies whilst trying to flag organised crime in transport flows. The combination of theoretical and practical insights could enrich our understanding of how to best realise the potential of both professional intuition and technology (and their interactions) in policing practices. Although there are various user manuals and policies to understand technologies in policing, we first must understand how technologies *are* used in reality and not merely how they *should be* used. After we understand this practice, we could go back to policies and design and outline the practical implications.

## REFERENCES

- Akrich, M., & Latour, B. (1992). A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 259-264). MIT Press.
- Bovens, M., & Zouridis, S. (2002). From Street-Level to System-Level Bureaucracies: How Information and Communication Technology Is Transforming Administrative Discretion and Constitutional Control. *Public Administration Review*, 62(2), 174-184. <https://doi.org/10.1111/0033-3352.00168>.
- Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82(5), 977-1008. <https://doi.org/10.1177/0003122417725865>.
- Browning, M., & Arrigo, B. (2021). Stop and Risk: Policing, Data, and the Digital Age of Discrimination. *American Journal of Criminal Justice*, 46(2), 298-316. <https://doi.org/10.1007/s12103-020-09557-x>.
- Busch, P.A., & Henriksen, H.Z. (2018b). Digital discretion: A systematic literature review of ICT and street-level discretion. *Information Polity*, 23(1), 3-28. <https://doi.org/10.3233/IP-170050>
- Byrne, J., & Hummer, D. (2017). Technology, Innovation and Twenty-First Century Policing. In M.R. McGuire & T. Holt (Eds.), *The Routledge Handbook of Technology, Crime and Justice* (pp. 375-389). Taylor and Francis.
- Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Journal of Police Studies*, 3, 17-40.

- Chan, J., Logan, S., & Moses, L. (2020). Rules in information sharing for security. *Criminology & Criminal Justice*, 22(2), 304-322. <https://doi.org/10.1177/1748895820960199>
- Da Silva, S. (2023). System 1 vs. System 2 Thinking. *Psychology*, 5(4), 1057-1076. <https://doi.org/10.3390/psych5040071>
- Dresser, P. (2019). 'Trust Your Instincts – Act!' PREVENT Police Officers' Perspectives of Counter-Radicalisation Reporting Thresholds'. *Critical Studies on Terrorism*, 12(4), 605-628. <https://doi.org/10.1080/17539153.2019.1595344>.
- Ernst, S., Ter Veen, H., Lam, J., & Kop, N. (2019). *Leren van technologisch innoveren: 'De techniek is niet zo spannend'*. Politieacademie.
- Ferguson, A.G. (2017). *The Rise of Big Data Policing*. New York University Press.
- Ihde, D. (1990). *Technology and the lifeworld*. Indiana University Press.
- Jansen, T., Van den Brink, G., & Kole, J. (2009). *Beroepstrots. Een ongekende kracht*. Boom.
- Joh, E. (2015). The new surveillance discretion: automated suspicion, big data, and policing. *Harvard Law and Policy Review*, 10, 15-42.
- Kahneman, D. (2011). *Thinking Fast and Slow*. Penguin Books Limited.
- Kennedy, L., Caplan, J., Garnier, S., Lersch, K., Miró-Llinares, F., Gibbs Van Brunschot, E., & Lopez, D. (2021). Using Evidence Based Analytics to Create Narratives for Police Decision Making. *Frontiers in Psychology*, 12. <https://doi:10.3389/fpsyg.2021.791605>.
- Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), 1-14.
- Koen, M., Willis, J., & Mastrofski, S. (2019). The Effects of Body-Worn Cameras on Police Organization and Practice: A Theory-Based Analysis. *Policing and Society*, 29(8), 968-964. <https://doi.org/10.1080/10439463.2018.1467907>.
- Koper, C., Lum, C., Willis, J., Woods, D., & Hibdon, J. (2015). *Realizing the Potential of Technology in Policing: A Multi-Site Study of the Social, Organizational, and Behavioral Aspects of Policing Technologies*. National Institute of Justice.
- Kubler, K. (2017). State of urgency: Surveillance, power, and algorithms in France's state of emergency. *Big Data & Society*, 4(2) 1-10. <https://doi.org/10.1177/205395171773>.
- Lauriault, T.P. (2012). *Data, Infrastructures and Geographical Imaginations*. PhD thesis, Carleton University, Ottawa.
- Lipsky, M. (1980). *Street Level Bureaucracy: Dilemmas of the Individual in Public Services*. Russell Sage Foundation.
- Manning, P. (2014). *Ethnographies of the police*. In M. Reising & R. Kane (Eds.), *The Oxford Handbook of Police and Policing*. Oxford University Press.
- Mastrofski, S.D., & Ritti, R.R. (2000). Making sense of community policing: A theoretical perspective. *Police Practice and Research Journal*, 1, 183-210.
- Maynard-Moody, S., & Musheno, M. (2003). *Cops, teachers, counselors: Stories from the Front Lines of Public Service*. The University of Michigan Press.

- Mitrou, L., Janssen, M., & Loukis, E. (2021). Human Control and Discretion in AI-driven Decision-making in Government. *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance ICEGOV 2021*, 10-16. <https://doi.org/10.1145/3494193.3494195>.
- Niculescu-Dinca, V. (2018). Towards a Sedimentology of Information Infrastructures: A Geological Approach for Understanding the City. *Philosophy & Technology*, 31(3), 455-472. <https://doi.org/doi:10.1007/s13347-017-0298-7>.
- Niculescu-Dinca, V. (2021). Theorizing technologically mediated policing in smart cities. An ethnographic approach to sensing infrastructures in policing practices. In M. Nagenborg, T. Stone, M. González Woge & P.E. Vermaas (Eds.), *Technology and the City: Towards a Philosophy of Urban Technologies* (pp. 75-100). Springer.
- Pramanik, M., Lau, R., Yue, W., Ye, Y., & Li, C. (2017). Big Data analytics for security and criminal investigations. *WIREs: Data Mining and Knowledge Discovery*, 7(4). <https://doi.org/10.1002/widm.1208>.
- Quinton, P., Bland, N., & Miller, J. (2000). *Police Stops, Decision-Making and Practice*. Home Office, Policing and Reducing Crime Unit.
- Rassin, E. (2018). Fundamental failure to think logically about scientific questions: an illustration of tunnel vision with the application of Wason's Card Selection Test to criminal evidence. *Applied Cognitive Psychology*, 32(4), 506-511. <https://psycnet.apa.org/doi/10.1002/acp.3417>.
- Rattcliffe, J., Taylor, R., & Fisher, R. (2019). Conflicts and congruencies between predictive policing and the patrol officer's craft. *Policing and Society*, 30(6), 1-17. <https://doi.org/10.1080/10439463.2019.1577844>.
- Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review*, 94(2), 192-233.
- Ridgeway, G. (2018). Policing in the era of Big Data. *Annual Review of Criminology*, 1(1), 401-419. <https://doi.org/10.1146/annurev-criminol-062217-114209>
- Rowe, M., & Muir, R. (2021). Big Data policing: governing the machines? In J. McDaniel & K. Pease (Eds.), *Predictive Policing and Artificial Intelligence* (pp. 254-268). Routledge.
- Sahm, M., & Von Weizsäcker, R.K. (2015). Reason, Intuition and Time. *Managerial and Decision Economics*, 37(3), 195-207. <https://dx.doi.org/10.2139/ssrn.2550130>.
- Schuilenburg, M. (2016). Predictive policing: De opkomst van een gedachtenpolitie? *Ars Aequi*, 65(12), 931-936.
- Selten, F., Robeer, M., & Grimmelikhuijsen, S. (2022). 'Just like I thought': Street-level bureaucrats trust AI recommendations if they confirm their professional judgment. *Public Administration Review*, 83(2), 263-278. <https://doi.org/10.1111/puar.13602>.
- Sheehy, B. (2019). Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics and Information Technology*, 21(5), 49-58. <https://doi.org/10.1007/s10676-018-9489-x>.

NIENKE DE GROES, VLAD NICULESCU-DINCA AND PIETER TOPS

- Stol, W. (1996). *Politieoptreden en informatietechnologie*. Koninklijke Vermande.
- Tay S.W., Ryan, P., & Ryan, C.A. (2016). Systems 1 and 2 thinking processes and cognitive reflection testing in medical students. *Canadian Medical Education Journal*, 7(2), 97-103. <http://dx.doi.org/10.36834/cmej.36777>.
- Terpstra, J., Salet, R., & Fyfe, N.R. (2022). *The Abstract Police*. Boom Criminologie.
- Tops, P. (2022). *Undermining and Data Science: what's it all about?* Lectoral Speech, Jheronimus Academy of Data Science.
- Tops, P., van der Torre, E., & Muller, E. (2023). Georganiseerde misdaad en ondermijning in Nederland vanuit een bestuurskundige invalshoek. In T. Overmans, M. Honingh & M. Noordegraaf (Eds.), *Maatschappelijke bestuurskunde, hoe verbindende bestuurskundigen (kunnen) inspelen op maatschappelijke vraagstukken* (pp. 149-169). Boom bestuurskunde.
- Tops, P., & van der Torre, E. (2024). *Ondermijning. Over de praktische betekenis van een analytisch begrip*. Boom bestuurskunde.
- Tummers, L., & Bekker, V. (2014). Policy Implementation, Street-level Bureaucracy, and the Importance of Discretion. *Public Management Review*, 16(4), 527-547. <https://doi.org/10.1080/14719037.2013.841978>.
- Van Brakel, R. (2016). Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing. In B. van der Sloot (Eds.), *Exploring the Boundaries of Big Data* (pp. 117-141). Amsterdam University Press.
- Van der Vijver, C.D., & Terpstra, J.B. (2007). Organisatie en sturing van politiewerk. In C.J.C.F. Fijnaut, E.R. Muller, U. Rosenthal & E.J. van der Torre (Eds.), *Politie: Studies over haar werking en organisatie*. Kluwer.
- Wright, M. (2013). Homicide Detectives' Intuition. *Journal of Investigative Psychology and Offender Profiling*, 10(2), 182-199. <https://doi.org/10.1002/jip.1383>.

## 4 THE DIGITALISATION OF THE POLICE

### *A state of the art on body-worn cameras, multi-tenant platforms and crime analysis software*

*Kevin Emplit, Maxime Mauquoy and Lies Vande Meulebroucke*

*With the collaboration of Sarah Van Praet*

#### **Abstract**

*This chapter explores the growing role of digital technologies in modern policing, specifically focusing on body-worn cameras (BWCs), multi-tenant platforms (MTPs) and crime analysis software (CAS). These technologies have been increasingly adopted by police forces worldwide, including in Belgium, as part of efforts to enhance efficiency, accountability, and public trust. Through a systematic review of international literature, the chapter explores the implementation, use, and impact of these technologies on police practices and organisational dynamics. It examines how digitalisation is reshaping both internal police operations – such as officer discretion, accountability, and workload – and external interactions with the public. The study also highlights the ethical and legal concerns surrounding these technologies, including privacy, surveillance, and the potential for biased decision-making. Ultimately, the chapter addresses how digital tools are transforming modern policing, while raising important questions about their role in reinforcing police legitimacy and procedural justice.*

#### **4.1 INTRODUCTION**

Policing has always relied heavily on the timely collection of relevant data. In so-called 'reactive' or traditional policing, this data and information were primarily related to offenders and the crimes they committed (Moore, 1992). Now, the modern policing era demands a shift to 'proactive' policing, implying a refocusing of attention on problems that need to be discovered and solved in partnership with the community. This imperative requires devices for ever-increasing data collection, as well as software adapted to their analysis (Santos, 2014). These tools must contribute to the increased efficiency and legitimacy of the police. This shift is reinforced by technological advancements. This technological shift is commonly called the process of digitalisation.

Digitalisation can be seen as the process of changing analogue formats to a digital format, which can be processed by a computer. This process has an impact on the way the organisation works and on the technologies the organisation uses during service provisioning (e.g. big data and AI) (Redlein & Höhenberger, 2020). Most research on

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

policing and technology typically discusses the effectiveness of specific technologies, tools, or devices in crime control, or explores tensions regarding police discretion, autonomy, accountability, transparency, or privacy issues. However, we were interested in constructing a systematic review of literature on how these technologies are experienced in the field and how they influence the role, function, and daily work of the police. We are particularly interested in transformations in the daily operations of the police, which could potentially alter, on the one hand, the interaction between the police and the public (external) and, on the other hand, the interaction between police officers and superiors (internal).

Our interest in this topic stems from the Digipol research project that unites us. The project's research question is: what impact does digitalisation have on the daily work of the Belgian local police? Not much is known about how Belgian police forces integrate digital devices into day-to-day policing. Funded by Belspo, Digipol investigates the impact of digitalisation on the daily work of the Belgian local police by focusing on three technologies: body-worn cameras (BWCs), multi-tenant platforms (MTPs), and crime analysis software (CAS). By studying the expectations, implementation, use and interactions with these devices, the study examines how technology can influence police legitimacy and organisational justice.

This chapter focuses on the analysis of international literature on three technologies within policing. We start with the description of the three devices on which we focus in this project (section 4.2), followed by situating the systematic review methodology (section 4.3). Thereafter, we present the findings of the review according to three perspectives: implementation (section 4.4), the transformations of police work as a working condition (section 4.5), and the transformations of policing and interactions with the public (section 4.6), before concluding.

## 4.2 EXPLORING THREE KEY TECHNOLOGIES IN POLICING

Numerous technologies are employed by the police, including BWCs, drones, radios, computers, software, etc. For this project, Digipol focuses its analytical efforts on three specific types of technologies: MTPs, BWCs and CAS. These technologies differ in terms of their purpose and the context in which they are used. Moreover, they have been recently implemented or considered by Belgian local police forces. BWCs, for example, are not universally used across all police zones or by all officers. Recently, 'Focus' has been operationalised in Belgium, serving as an example of an MTP. Lastly, CAS is used by the back office, while the other two technologies are used by the front office. Research into these technologies enhances our understanding of their use and impact in Belgian local police forces. The empirical part of the research will take place in six police zones that differ in terms of geography, capacity, allocated budget, and language. This allows us

to establish a comprehensive picture of their use of these technologies within the Belgian local police.

The first technology is the multi-tenant platform (MTP). Mobile computing technology has been one of the most central innovative technologies introduced into policing over the last few decades (Koper, Lum & Hibdon, 2015). Platform policing involves the movement of police data to the cloud, where it can be used in police operations. Relevant data, transmitted, analysed, and processed through cloud infrastructures, is communicated to police in the field in real time to inform and shape interactions (Završnik & Badalic, 2021). The concept of 'platform policing' is an organisational process in which many datasets and data banks, particularly from sources external to the police, are linked together, creating research and information production networks designed to improve police work on many levels by facilitating access to information and training (Wilson, 2019). Technologies that continuously capture and exploit this data within the platform include visual data, sensor data, content analysis, information recording and real-time dispatching activities (Rani et al., 2022).

Advances in information technology have been reported to improve the way police forces collect, use, and disseminate data and information (Nunn, 2001). The relevance of mobile technologies to policing lies, according to some literature, in access to accurate information, reducing administrative work for police officers, improving communication, and quickly retrieving and transmitting relevant information (Singh & Hackney, 2011). However, the development of these MTPs as apps for mobile devices is also justified by the desire to virtualise processes by allowing police officers to share information and communication outside fixed geographical locations, leading to improved performance, reduced costs, transparency, teamwork, and rapid, informed decision-making (Singh, 2017). They can be seen as devices of information processing (Dupont, 2004, p. 114).

The second technology is the bodycam, also known as a body-worn camera (BWC) or body-worn device. This is a small camera worn by police officers that 'allows officers to record what they see and hear' (Hayes & Ericson, 2012, p. 5) during police-citizen encounters (Demir, 2018; Sousa et al., 2015). They are worn on police officers' uniforms, mostly on the chest, shoulder, or collar (Sousa et al., 2015). Activation occurs, among other situations, during arrests, general police-public interactions and public order policing (Lee et al., 2018). The goal of BWCs is to record the actions and behaviour of law enforcement officers, members of the public who interact with them and situations in which they are involved (Hyatt et al., 2017).

Numerous studies indicate that BWCs affect the way police officers operate on the street (Ariel, Farrar & Sutherland, 2015; Ariel et al., 2017; Demir et al., 2020; Hedberg et al., 2017). BWCs are therefore expected by some scholars to offer several notable benefits (Smith, 2019) and to have a 'civilising effect' on both police and citizens, calming both parties, leading to friendly interactions, and reducing resistance in coercive situations

(White, 2014). Other authors add that the aims of BWCs are manifold: in addition to providing additional data for prosecutions and offering concrete examples of training, they should, according to proponents, increase public trust, police accountability and transparency, and reduce instances of the use of force by and against the police by influencing the behaviour of those who are aware of the recording in progress (Saulnier et al., 2021). Others argue that this is not the case because officers have the autonomy to not turn the camera on, for instance to avoid recording misconduct (Taylor, 2016). According to Boivin and D'Elia (2020), the current review of literature lacks a thorough study of how police officers incorporate BWCs into their daily work and how BWCs are (deliberately) used or not used in specific situations.

Lastly, crime analysis software (CAS) is more of an 'organisational technology', developed from problem-oriented policing: its goal is to find out problems and their solutions and assess the results (Daglar & Argun, 2016). It involves the use of big data and modern technology and a set of systematic methods and techniques. Its intent is to identify patterns and relationships between crime data and other relevant information sources to support decision-making that informs the design, allocation and priorities of police activity and crime prevention responses (Chainey & Ratcliffe, 2005), to assist police in criminal apprehension, crime and disorder reduction, crime prevention, and evaluation (Koper et al., 2015).

Through CAS, criminal events registered in the police records are monitored to generate daily factual reports or mappings as well as useful overviews. They can also assist police management in decision-making at multiple levels of responsibility (Dupont, 2004, p. 116; Didier, 2015; Tange, 2020). The use of these increasingly automated devices, relying on algorithms while leaving less and less room for human interpretation, brings us closer to what can be described as forms of artificial intelligence and raises crucial questions regarding its efficiency and the ethical and legal questions it poses (Dupont et al., 2018; Gonzalez-Fuster, 2020).

The emergence of CAS is part of the concept of 'predictive' policing. This policing strategy is based on the idea that police can use digital technologies and sophisticated data-mining systems to generate actionable predictions about the sources and spatiotemporal conditions of future crime (Egbert, 2019). From the outset, this concept of predictive policing has been controversial because of the enormous ethical implications of using data to power algorithms that would be clearly biased in terms of ethnicity and/or gender but also due to the unrealistic expectations of predicting where and when crime might occur and thus preventing it (Miró Llinares, 2020). Such software is intended to provide decision support and initiate a process aimed at achieving complete 'datafication' – seen as the process by which subjects, objects and practices are transformed into digital data – of police work, creating a continuous movement of data collection and, consequently, analysis (Egbert, 2019).

### 4.3 SYSTEMATIC REVIEWING METHOD

We conducted a systematic review, using an integrated method, procedure, and technique to locate, identify, retrieve, and analyse literature for its relevance, significance and meaning (Altheide et al., 2008). Data were examined and interpreted to derive meaning, gain understanding, and develop empirical knowledge. Literature serves to provide context, suggest questions and concepts for further research, and verify findings from other data sources (Bowen, 2009).

This systematic review focuses on three possible angles through which technology can transform policing. These angles are central in the further Digipol research:

- 1 Understanding the process of digitalisation, including how technology is implemented in police organisations and their strategies and work processes.
- 2 Understanding the changing nature of the day-to-day work of frontline police officers, including their working conditions and internal hierarchical relations.
- 3 Understanding the use of technology in the day-to-day activities of frontline police officers and how this affects frontline ‘policing’ and police-public relations.

To structure the review, we input keywords into various bibliographical databases such as Scopus, Google Scholar, ResearchGate and Science Direct, varying the terms related to our three selected devices. For body-worn cameras, results related to the keywords ‘body-worn camera’ and ‘portable camera police’ or ‘*caméras portatives*’ proved to be relevant, yielding a wealth of sources. In contrast, multi-tenant platforms presented a challenge as researchers do not often use this term. The keyword ‘multi-tenant platform’ (MTPs) did not yield relevant sources. Alternative keywords were assessed, such as ‘platform policing’, ‘mobile data police’ and ‘mobile devices police’. However, as the Belgian police use an application called Focus, an example of an MTP, the keyword ‘Focus app’ was also used to search for sources in Dutch. Finally, keywords for crime analysis software were defined, including ‘predictive police tools OR implementation OR deployment’, ‘LPR’ (licence-plate reader), ‘ANPR’ (Automatic Number Plate Recognition), ‘hot spot policing’, ‘crime analysis’, ‘*police prédictive*’ and ‘crime mapping’. Due to limited hits on MTP and crime analysis software, we decided to broaden the research to encompass more general technological innovation within police organisations using keywords like ‘police innovation’ and ‘*innovation policière*’. Snowballing was also employed to find relevant sources by using the reference lists or citations within a publication to identify additional papers (Wohlin, 2014). We did not limit our research by time, but no literature published before 2004 was identified, with most literature published since 2014. This is likely due to the relative novelty of the implementation of these technologies in the police force.

Relevance of a publication was determined based on the abstract. Scientific sources, such as peer-reviewed articles, books or book chapters, the content of which was related to the research questions and sources written in English, French or Dutch from European

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

and Anglo-Saxon countries were included. Technical and descriptive resources have been excluded in this chapter, as the focus is not on the technical underpinnings or effectiveness of digital devices. The relevant sources obtained were thoroughly read and analysed, and NVivo was used to analyse and code the relevant articles.<sup>1</sup>

#### 4.4 DIGITAL DEVICE IMPLEMENTATION IN POLICE ORGANISATIONS

##### 4.4.1 *The genesis of digital device implementation*

According to studies from Switzerland, the United Kingdom, Canada and the United States, technological innovation in police organisations often appears to be linked to crisis situations (citizen deaths involving the police, financial crises) where the legitimacy of the police is questioned, and an increased need for security is demanded by the public (Simmler et al., 2023; Laufs & Borrion, 2022; Poirier, 2021; Lum et al., 2019). This implies that police organisations are subject to external constraints, with community, media and political pressures pushing them to propose a ‘technological solution’ to the problem(s). Indeed, several American studies mention that decision-makers see BWCs as a means of maintaining confidence between police and the community, responding to the need for security, and improving police legitimacy through greater transparency and accountability (Koen et al., 2023; Pyo, 2022; Willis, 2022; Poirier, 2021; Koen et al., 2021; Pelfrey & Keener, 2018; Gaub et al., 2016). According to studies from Germany, Switzerland and France, CAS is also perceived as facilitating better management of police resources and the rationalisation of actions (Simmler et al., 2023; Egbert & Leese, 2020; Benbouzid, 2018).

However, some American studies show that the actual acquisition of these digital devices cannot be explained entirely by the need to respond to these events (Andreescu & Kim, 2022; Laming, 2019; Pyo, 2020). According to a British study, other benefits are also expected from these technical tools, and the crisis can function as a lever justifying innovation (Norris & L’Hoiry, 2017). For example, BWCs can, according to American and European studies, aim to protect police officers by countering the phenomenon of ‘under-surveillance’ (Koen et al., 2023; Goyvaerts et al., 2021; Koen et al., 2021; Laming et al., 2021; Mrozla & Marin Hellwege, 2020; Smykla et al., 2016) and provide recordings for training (Willis, 2022; Koen & Willis, 2020; Pelfrey & Keener, 2018; Coudert et al., 2015).

---

1 Here we mention that there is a lot of literature about technologies in general. In the text, where possible, we discuss which technology we specifically mean.

According to studies from Switzerland and Germany, some digital tools are implemented because they are supposed to create greater efficiency in crime prevention, by making police activities more proactive, notably by using algorithms that process already recorded police data to predict crime patterns and direct patrols accordingly (Simmler et al., 2023; Egbert & Leese, 2020; Vepřek et al., 2020). This strategic objective behind technological innovation is, however, called into question by Hendrix et al. (2019), who have shown that the adoption of technology within the police was in fact little linked to strategic models (e.g. community policing, problem-oriented policing, intelligence-led policing, etc.). Devices are still perceived as a means of changing practices and increasing the organisation's level of specialisation (Egbert & Leese, 2020; Delpuech, 2016).

Quantitative studies have focused on the organisational and contextual factors influencing the effective acquisition of digital devices. While the influence of the organisation's size, budget and level of complexity gives ambiguous results in the consulted literature, several American studies mention that the presence of strong union strength, technological affinity and the organisation's level of control are said to play a significant role (Andreescu & Kim, 2022; Lawshe, 2022; Pyo, 2022; Mrozla & Marin Hellwege, 2020; Hendrix et al., 2019; Nowacki & Willits, 2018; Randol, 2014). Although little studied, the technical characteristics of the devices themselves (e.g. data storage modalities) also seem to influence the acquisition of technologies (Koen et al., 2023). Furthermore, the acquisition would be linked to the possibilities for technical exploration, depending on the level of centralisation of services and the national and organisational culture (Lum et al., 2019; Saskia Bayerl et al., 2013). Finally, the broader political context (type of government, security policies) must be considered (Pyo, 2020; 2022).

#### 4.4.2 *The implementation process of digital devices*

Regarding the implementation process, it is interesting to note that, according to studies from Switzerland, Belgium, the Netherlands, and the United Kingdom, it often takes place prior to the establishment of a clearly defined legal framework (Simmler et al., 2023; Goyvaerts et al., 2021; Houwing & Ritsema Van Eck, 2020; Norris & L'Hoiry, 2017). This could be explained by the desire to respond quickly to crisis situations. As a result, studies from Switzerland, Belgium, Canada, and the United States mention that different interpretations exist on the legal norms underpinning the use of these tools by the police (Meyer, 2020), which are based on more general laws such as data protection laws or laws governing police procedures (Goyvaerts et al., 2021; Poirier, 2021; Sousa et al., 2016).

Several American and European studies indicate that, while an adequate legal framework is discussed by decision-makers, a multitude of actors participate in the implementation process. Firstly, government bodies set up development plans by

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

organising expert meetings, proposing guidelines, and granting funding to police organisations (Willis, 2022; Egbert & Leese, 2020; White et al., 2018). Secondly, the private companies that sell these technologies influence decision-makers' choices according to the resources and needs available to them (Laming, 2019; Koen et al., 2021). Academia also plays a role by conducting evaluative studies and participating in the dissemination of these devices (Goyvaerts et al., 2021; Koen et al., 2021; White et al., 2018; Delpeuch, 2016). Finally, frontline police officers, the main users of these tools, are particularly decisive, according to the consulted body of literature (Laufs & Borrion, 2022; Saulnier et al., 2019; Snyder et al., 2019). The resistance they demonstrate will lead to them being integrated into development projects and influencing the adoption of digital devices (Koen et al., 2023; ter Veen & Kop, 2021; Snyder et al., 2019).

The acquisition of new digital tools raises questions regarding the process of decision-making and organisational justice. American literature and a Belgian study describe a discrepancy between the benefits imagined by decision-makers and those perceived by police officers. The latter may perceive a risk of control over their behaviour, a reduction in their discretionary power and an increase in the complexity of tasks (Willis, 2022; Goyvaerts et al., 2021; Koen et al., 2021; Koen & Willis, 2020; Snyder et al., 2019; Gaub et al., 2016).

#### 4.5 THE TRANSFORMATIONS OF WORK AND WORKING CONDITIONS OF FRONTLINE POLICE OFFICERS

##### 4.5.1 *Impact on work content and organisation*

According to some American studies, there is evidence that the use of bodycams could severely restrict police discretion (Koen et al., 2019). They may prompt some police officers to reduce the number of breaks, issue warnings instead of citations or increase ticketing activity (Ready & Young, 2015). In general, they may feel they have less room for manoeuvre and will be more cautious in their decisions (White et al., 2018).

A Serbian study stated that crime analysis software also imposes new demands on police officers (Ilijazi et al., 2019) and some American studies have described that fact: they are forced to think analytically and to generate hypotheses about the cause of the problem and its perpetrators (Boba & Crank, 2008); however, to a considerable extent, police officers' field activities are guided by the knowledge they have accumulated through experience, and they are unlikely to recognise the need to verify or update it using software (Ilijazi et al., 2019). Predictive technology may also, according to an American study from Ratcliffe et al. (2020), impact police work by exacerbating potential conflicts between specific normative orders within a department's subculture.

According to some American studies, information technology (MTP) may also not correspond to the realities of police work (Manning, 1992), and its use may increase

productivity without leading to efficiency gains (Ioimo & Aronson, 2004). Furthermore, investment in information technology is doomed to failure if the information does not reach or is not used by those who are supposed to use it: frontline police officers (Ilijazi et al., 2019). Finally, according to a British study, the nature of technology could expose police officers to a range of health and safety risks, problems associated with the use of small mobile devices, and laptop portability issues (Norman & Allen, 2005).

#### 4.5.2 *Impact on well-being and work environment*

Research shows that the main stressors in police work are caused by the organisational (as opposed to operational) characteristics of the job. In other words, an Australian study shows that administrative practices, procedures, and cultures may be more related to police stress and anxiety than involvement in critical incidents while on duty (Christodoulou et al., 2019). From this organisational perspective, according to an American study, the consequences for the organisation become significant in terms of increased mental-health-related sick leave and burnout due to a loss of trust between officers and their management, and in terms of potentially counterproductive professional behaviours such as the avoidance of proactive activities in favour of safer police-initiated activities (Groff et al., 2020).

In addition, studies in the United Kingdom, Australia and the United States indicate that the use of bodycams can have negative consequences for police work and safety (Hansen Löffstrand & Backman, 2021). It has also been shown that wearing them can increase police burnout and decrease their perception of organisational support (Adams & Mastracci, 2019a). Thus, while police officers may be supportive of the use of bodycams (Jennings et al., 2014), further research is needed to better understand police organisational stress and ways to mitigate it. Conversely, mobile information technology is more often perceived as improving staff's ability to do their jobs (Carter & Grommon, 2017).

When it comes to crime prediction technology, officers on patrol express concerns about the technology's potential to marginalise their expertise, painstakingly acquired over years and decades of experience and careful observation, and to interfere with peer-based standards of responsiveness (Ratcliffe et al., 2020). Moreover, this 'datafication' of the police officer's body enables its precise management in real time and, therefore, reduces the officer's flexibility.

#### 4.5.3 *Impact on relations with hierarchy*

The implementation and use of bodycams are underpinned by two surveillance logics (Hansen Löffstrand & Backman, 2021): the control and discipline objective and the

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

protection objective. An American study suggests that bodycam-induced surveillance is often conceptualised as a means of maintaining or increasing productivity and protecting organisational interests, while the protective function of employee surveillance is rare (Ravid et al., 2020). The possibility of sanctions linked to the controlling aspect of monitoring reduces the sense of support and trust in the hierarchy and increases the level of burnout (Adams & Mastracci, 2019b).

This loss of confidence is also evident in the case of analysis software. Indeed, criminal acts can occur in a specific area (referred to as hotspots by analysts or police supervisors) but may not be reported to the police (dark figure of crime). Frontline police officers are aware of this because they know their patrol area well, but crime analysts and police supervisors do not. As a result, they may interpret police officers' perceptions as inaccurate, damaging the officer-supervisor relationships (Ilijazi et al., 2019).

Regarding the implementation of mobile information technologies, a British study indicates that most agents felt that their introduction was unlikely to change their relationship of trust with their direct superiors (Norman & Allen, 2005). Nevertheless, another British study from Green (2002) also notes the problem of resentment linked to being monitored at a distance. In addition, an American study mentions that testimonies from patrol officers report that they are aware that the integration of GPS data into technologies that make up platform policing structures strengthens the ability of their superiors to track their location and thus diminishes their flexibility (Wilson, 2019).

#### 4.6 THE TRANSFORMATIONS OF 'POLICING' AND POLICE-PUBLIC RELATIONS

##### 4.6.1 *Body-worn cameras (BWCs)*

An American study shows that BWCs are utilised in the field and are visibly worn on police officers' uniforms (Demir, 2018). According to Demir (2018), they are used to prevent discriminatory police behaviour and violent encounters, promote the quality of interactions between police and citizens, and enhance citizens' trust in the police. BWCs can improve police legitimacy, as they are considered important tools to significantly enhance citizen perceptions of police legitimacy and procedural justice by increasing police transparency and accountability (Demir, 2018).

Moreover, there are mixed results regarding the impact of BWCs on police-public relations. An American study has shown that the use of BWCs can improve the behaviour of both police officers and citizens during encounters (Jennings et al., 2015). This is related to the self-awareness theory. The self-awareness theory suggests that individual's self-awareness will increase and, when they are being aware that they

are being watched, they become conscious of their actions. This makes them behave conform to the rules. Due to the BWCs, individuals' self-awareness will increase. Both police and citizens become conscious of their actions, leading to improved behaviour during encounters by being more respectful and compliant (White, 2014). Furthermore, the deterrence theory states that individuals are more likely to conform to rules if they know that the consequences of wrongdoing (costs) outweigh the desired outcomes of their actions (benefits). BWC recordings provide objective and effective video evidence that can be used against both police and citizens. These recordings increase the certainty of punishment if either party acts in an inappropriate way and breaks the rules. Consequently, both parties are likely to behave better towards each other and comply (Demir & Kule, 2022; White, 2014). Nevertheless, according to some British studies, the activation of the camera can also aggravate a situation (Ariel et al., 2016; Taylor & Lee, 2019). Finally, another British study from Grossmith et al. (2015) discovered that officer interactions with citizens were not impacted by BWCs.

#### 4.6.2 *Crime analysis software (CAS)*

Second, according to a Dutch study, CAS is used at the police station and is broadly deployed for traditional street enforcement, investigation, and intelligence (Schuilenberg & Soudijn, 2021). However, according to some British studies, this routinisation of shifts is not positively received by everyone, and it can remove officers' discretion and initiative, which may impact self-legitimacy (Verhage et al., 2022; Wain et al., 2017). In addition, an American study mentions that officers state that crime analysis tells them what they already know (Koper et al., 2015).

Nonetheless, the use of CAS is not visible to the public. As the focus of research on police legitimacy is most on citizen perceptions of police legitimacy, little is known about the impact of CAS on police legitimacy, as the public do not have direct contact with the technologies, but they do experience the consequences of them. However, the public may not be aware of the use of this software by the police, and they may not know that the technology is the underlying phenomenon that leads to those consequences. Analysis software's potential to affect police legitimacy is substantial, yet its impact may not be readily apparent due to the difficulty of measurement.

An example of a consequence, given by an American study, is the increased engagement of police in a predicted area and their increased involvement in investigating individuals in those areas (Ferguson, 2017). However, according to some American studies, the data used by CAS can be limited, incomplete, inaccurate, or biased due to discriminatory policing practices, which can reinforce disparate treatments for already marginalised communities and create unwanted police-citizen contact or unwanted surveillance in certain areas, diverting police resources by sending officers to the wrong places (Ferguson, 2017; Shapiro, 2019). The citizens of these places will be

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

subject to undue police control, and there is an imbalanced and unfair distribution of police presence. A collective work from Slovenia informs us that this reinforces over-policing of already targeted areas, which can have negative consequences for targeted communities as they could become stigmatised (Završnik & Badalic, 2021).

In addition, there is an increased risk that an individual will be judged based on the socioeconomic characteristics of the neighbourhood rather than the individual's behaviour. Relying on CAS holds the risk, according to an American study, that police-community relations will weaken, as the community can feel like targets (Rosenbaum, 2019). Therefore, there is an increased chance, due to the software predictions, that interactions will arise that would not otherwise exist. However, the Dutch research from Schuilenberg and Soudijn (2021) found that only relatively simple big data applications are used, which means that the impact on citizens, such as risks of discrimination and ethnic profiling, appears to be limited.

#### 4.6.3 *Multi-tenant platforms (MTPs)*

Lastly, MTPs are mainly used in the field to draft reports and communicate, check automobile licence plates, and run checks on people encountered during activities (Koper et al., 2015). However, British, and Belgian studies found that police officers still use alternatives that existed before the introduction of MTPs (Abbas & Policek, 2021; Rooseleers, 2023).

Once more, not much is known about the impact of MTPs on police legitimacy. A British study indicates that they do provide legitimacy for officers by symbolising the institution, and they make officers accountable through documentation and control of actions (Sørensen & Pica, 2005). However, developments in automation in policing connect with a Dutch study from Terpstra et al. (2019). The authors state that policing is becoming less personal, less direct, and more dependent on police information systems. This devalues professional knowledge, police work and discretion in handling situations and problems, which can have, according to a British study, a negative impact on officers' sense of organisational justice and self-legitimacy (Verhage et al., 2022).

In addition, MTPs can influence the nature of police-citizen interactions in the field. Some officers find the use distracting from face-to-face interactions, while others state that it enhances the ability of police to respond to citizens' requests for information and assistance (Koper et al., 2015). Moreover, some Belgian studies show that citizens can experience an interaction mediated by a screen as an 'absent presence' of the police officer, leading to an interaction with a lack of communication and eye contact (Rooseleers, 2023; Verhage et al., 2022).

However, officers are more present in the field because of MTPs as they do not have to return to the office as often. This increase in presence on the field is associated with more visibility and accessibility to the public, allowing more proactive policing. In

addition, the possibility of interaction increases because of the increased possibility to look up information. According to a Belgian study, these searches could result in an interaction that would not otherwise take place (Rooseleers, 2023). Nonetheless, another Belgian study shows that the MTP is often used before the encounter with the citizen, resulting in a minor impact on the police-citizen interaction (Verhage et al., 2022). Other studies even show that officers try to avoid MTP use when they are in interaction with people and use the radio instead (Pica, 2006; Rooseleers, 2023).

#### 4.7 CONCLUSION

In conclusion, our review of the literature shows that the process of adopting police technologies needs to consider not only the organisational and macro-context (economic, political, social) in which they appear, but also their technical properties. While crisis situations drive or legitimise the willingness to adopt these devices, police services differ in ways that either favour or restrict the possibilities of their effective acquisition. In addition, there are other motivations than strengthening police legitimacy. Through BWCs and CAS, decision-makers may see an interest in protecting police officers, specialising the organisation, adopting a continuous preventive approach, or better managing police resources. Regarding the implementation process, the consulted body of literature generally observes a rapid introduction of devices within police departments, without a clear normative framework. Moreover, many different actors engage in their implementation. In this context, the role of frontline police officers is particularly important, given that they hold a degree of negotiating power and are the main users of these tools. This has to do with the issues regarding decision-making and the organisational justice regarding the purchase of these technologies.

On the level of the individual police officer, the literature review suggests that the implementation and the use of technology affect, on the one hand, the working conditions and, by doing so, the perceptions and the (defensive) attitudes of police officers, and on the other hand, police-citizen interactions. Still, there are differences in the impact between the three technologies as they have different goals and are used in different contexts.

Working conditions, organisational changes – structures, programmes, policies, and technologies – often generate resistance from the targets of these change efforts. This highlights the significant role of organisational justice, which includes the perception that positive and negative outcomes are fairly distributed (distributive justice), employees have a voice in decision-making (procedural justice), and supervisors treat employees with dignity and respect (interactive justice). This is a promising approach to reducing negative attitudes and organisational change more generally. In police departments, promoting organisational justice can be particularly challenging, as turnover and paradigm shifts are frequent, and supervision is high. Nevertheless, the

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

research suggests that organisations would do well to make efforts to increase officers' perceptions of organisational justice because they are linked to greater job satisfaction, a sense of trust and support from the organisation, and ensuring the use of fair and transparent processes.

Concerning police-citizen interactions, BWCs are mobile and visible on the uniform of the police officers and can change police and citizen behaviour because of a civilising effect (self-awareness theory and deterrence theory). MTPs are mobile and sometimes visibly used in front of the public. However, they are often used before the encounter with the citizen, which results in a minor impact on police-citizen interactions. Nonetheless, because of MTPs, officers can be more present in the field as they do not have to return to the office as often, allowing proactive policing. They can, however, be distracting from face-to-face interactions, which can lead to less communication and eye contact. In addition, the chance of interaction increases because of the increased visibility and accessibility to the public and because of the increased possibility to look up information. These searches could result in an interaction that would not otherwise take place. Crime analysis software is used at the police station, but the public is not directly in contact with the software. However, they do encounter the consequences. The use of CAS can indirectly decrease the quality of police-citizen interactions. Moreover, the data the software uses to make predictions can have error rates. These biases may contribute to the misallocation of police resources, which reinforces over-policing of already targeted areas, which can have negative consequences for targeted communities. There is also the possibility that an individual will be judged based on the socioeconomic characteristics of the neighbourhood rather than the individual's behaviour. In addition, there is a risk of weakening police-community relations as the community can feel like targets. There is, therefore, an increased chance due to software predictions that interactions will arise that would not otherwise exist.

The exploration of the impact of these technologies on the interaction between police and citizens can be situated within the framework of technological mediation theory. This theoretical perspective proposes that technologies play a role in shaping human experiences, practices and the relations between individuals and their environment. By employing mediation theory, scholars can dissect the diverse shapes of these relationships, scrutinise the junctures where a technology is used by its user, and discern the specific modalities of mediation at play. Contrary to the perception of technologies as external entities, this perspective emphasises technology's integral role in facilitating the expansion of human knowledge of the world, ethical decision-making processes, and even the formulation of metaphysical and religious frameworks (Verbeek, 2015).

Further, to enhance procedural justice, it is imperative to integrate supplementary components such as training initiatives and performance measures. Such efforts significantly influence the organisation and hierarchical dynamics. Establishing a correlation between technological advancements and the augmentation of procedural

justice entails an examination of their effect on the organisational justice perceptions among police officers. Moreover, it is essential to consider the ramifications of non-technological factors on overall organisational dynamics.

Finally, not much is known about the impact of the technologies on police legitimacy. Research suggests that BWCs can boost police legitimacy, while CAS and MTPs might affect officers' self-legitimacy. However, the broader impact of CAS and MTP on police legitimacy remains unclear, given limited public interaction with these technologies.

## REFERENCES

- Abbas, N., & Policek, N. (2021). 'Don't be the same, be better': an exploratory study on police mobile technology resistance. *Police Practice and Research*, 22(1), 849-868. <https://doi.org/10.1080/15614263.2020.1728271>
- Adams, I., & Mastracci, S. (2019a). Police Body-Worn Cameras: Development of the Perceived Intensity of Monitoring Scale. *Criminal Justice Review*, 44(3), 386-405. <https://doi.org/10.1177/0734016819846219>
- Adams, I., & Mastracci, S. (2019b). Police Body-Worn Cameras: Effects on Officers' Burnout and Perceived Organizational Support. *Police Quarterly*, 22(1), 5-30. <https://doi.org/10.1177/1098611118783987>
- Andreescu, V., & Kim, D. (2022). Drivers of police agencies' resistance to body-worn camera adoption. *International Journal of Police Science & Management*, 24(4), 437-452. <https://doi.org/10.1177/14613557221126492>.
- Ariel, B., Farrar, W.A., & Sutherland, A. (2015). The Effect of Police Body-Worn Cameras on Use of Force and Citizens' Complaints Against the Police: A Randomized Controlled Trial. *Journal of Quantitative Criminology*, 31, 509-535. <https://doi.org/10.1007/s10940-014-9236-3>.
- Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2016). Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. *European Journal of Criminology*, 13(6), 744-755. <https://doi.org/10.1177/1477370816643734>
- Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., Megicks, S., & Henderson, R. (2017). 'Contagious accountability': a global multisite randomized controlled trial on the effect of police body-worn cameras on citizens' complaints against the police. *Criminal Justice & Behavior*, 44, 293-316.
- Beck, C., & McCue, C. (2009). Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession? *The Police Chief*, 76(11), 18-24.
- Benbouzid, B. (2018). Quand prédire, c'est gérer : La police prédictive aux États-Unis. *Réseaux*, 211(5), 221-256. <https://doi.org/10.3917/res.211.0221>.

- Boba, R., & Crank, J.P. (2008). Institutionalizing problem-oriented policing: Rethinking problem solving, analysis, and accountability. *Police Practice and Research*, 9(5), 379-393. <https://doi.org/10.1080/15614260801980745>.
- Boivin, R., & D'Elia, M. (2020). Évaluation du projet pilote des caméras corporelles du Service de police de la Ville de Montréal. *Criminologie*, 53(1), 344-366. <https://doi.org/10.7202/1070513ar>.
- Carter, J.G., & Grommon, E. (2017). Officer perceptions of the impact of mobile broadband technology on police operations. *Policing and Society*, 27(8), 847-864. <https://doi.org/10.1080/10439463.2015.1112388>.
- Chainey, S., & Ratcliffe, J. (2005). *GIS and Crime Mapping*. John Wiley & Sons, Ltd.
- Christodoulou, C., Paterson, H., & Kemp, R. (2019). Body-worn cameras: Evidence-base and implications. *Current Issues in Criminal Justice*, 31(4), 513-524. <https://doi.org/10.1080/10345329.2019.1639590>.
- Coudert, F., Butin, D., & Le Métayer, D. (2015). Body-worn cameras for police accountability: Opportunities and risks. *Computer Law & Security Review*, 31(6), 749-762. <https://doi.org/10.1016/j.clsr.2015.09.002>.
- Daglar, M., & Argun, U. (2016). Crime Mapping and Geographical Information Systems in Crime Analysis. *Journal of Human Sciences*, 13(1), 2208-2221.
- Delpeuch, T. (2016). L'innovation institutionnelle : Une entreprise politique à base d'emprunts extérieurs : L'exemple de la diffusion des nouveaux instruments d'intelligence dans les forces de police. *Quaderni*, 91, 61-78. <https://doi.org/10.4000/quaderni.1011>.
- Demir, M. (2018). Citizens' perceptions of body-worn cameras (BWCs): Findings from a quasirandomized controlled trial. *Journal of Criminal Justice*, 60, 130-139. <https://doi.org/10.1016/j.jcrimjus.2018.09.009>.
- Demir, M., Apel, R., Braga, A.A., Brunson, R.K., & Ariel, B. (2020). Body worn cameras, procedural justice, and police legitimacy: A controlled experimental evaluation of traffic stops. *Justice Quarterly*, 37, 53-84.
- Demir, M., & Kule, A. (2022). The effect of body-worn cameras on satisfaction and general perceptions of police: Findings from a quasirandomized controlled trial. *European Journal of Criminology*, 19(4), 562-585. <https://doi.org/10.1177/1477370820905105>.
- Didier, E. (2015), « Compstat » à Paris : initiative et mise en responsabilité policière, *Champ pénal/ Penal field*, VIII. <http://journals.openedition.org/champpenal/7971>
- Dupont, B. (2004). La technicisation du travail policier : Ambivalences et contradictions internes. *Criminologie*, 37(1), 107-126. <https://doi.org/10.7202/008719ar>
- Dupont, B., Stevens, Y., Westermann, H., & Joyce, M. (2018). *Artificial Intelligence in the Context of Crime and Criminal Justice*. Canada Research Chair in Cybersecurity, International Centre for Comparative Criminology – Université de Montréal and Korean Institute of Criminology.

- Egbert, S. (2019). Predictive Policing and the Platformization of Police Work. *Surveillance & Society* 17(1/2), 83-88. <https://ojs.library.queensu.ca/index.php/surveillance-and-society/index>
- Egbert, S., & Leese, M. (2020). *Criminal Futures: Predictive Policing and Everyday Police Work* (1st ed.). Routledge. <https://doi.org/10.4324/9780429328732>.
- Ferguson, A.G. (2017). Policing predictive policing. *Washington University Law Review*, 94, 1109-1189.
- Gaub, J.E., Choate, D.E., Todak, N., Katz, C.M., & White, M.D. (2016). Officer Perceptions of Body-Worn Cameras Before and After Deployment: A Study of Three Departments. *Police Quarterly*, 19(3), 275-302. <https://doi.org/10.1177/1098611116653398>.
- Gonzalez Fuster, G. (2020). *Artificial Intelligence and Law Enforcement*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL\\_STU\(2020\)656295\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf).
- Goyvaerts, V., Maesschalck, J., & Seron, V. (2021). *Mogelijkheden en uitdagingen bij het gebruik van de bodycam door de geïntegreerde politie*. <https://doi.org/10.13140/RG.2.2.28519.57766>.
- Green, N. (2002). On the move: technology, mobility, and the mediation of social time and space. *Information Society*, 18(4), 281-292.
- Groff, E.R., Haberman, C., & Wood, J.D. (2020). The effects of body-worn cameras on police-citizen encounters and police activity: Evaluation of a pilot implementation in Philadelphia, PA. *Journal of Experimental Criminology*, 16(4), 463-480. <https://doi.org/10.1007/s11292-019-09383-0>.
- Grossmith, L., Owens, C., Finn, W., Mann, D., Davies, T., & Baika, L. (2015). *Police, Camera, Evidence: London's cluster randomised controlled trial of Body Worn Video*. College of Policing Limited and the Mayor's Office for Policing and Crime (MOPAC). [https://www.london.gov.uk/sites/default/files/bwv\\_report\\_nov\\_2015.pdf](https://www.london.gov.uk/sites/default/files/bwv_report_nov_2015.pdf).
- Hansen Löfstrand, C., & Backman, C. (2021). Control or protection? Work environment implications of police body-worn cameras. *New Technology, Work and Employment*, 36(3), 327-347. <https://doi.org/10.1111/ntwe.12201>.
- Hayes, J., & Ericson, L. (2012). *A Primer on Body-Worn Cameras for Law Enforcement*. National Law Enforcement and Corrections Technology Center (NLECTC). <https://www.ojp.gov/pdffiles1/nij/nlectc/239647.pdf>.
- Hedberg, E.C., Katz, C.M., & Choate, D.E. (2017). Body-Worn Cameras and Citizen Interactions with Police Officers: Estimating Plausible Effects Given Varying Compliance Levels. *Justice Quarterly*, 34(4), 627-651, <https://doi.org/10.1080/07418825.2016.1198825>.
- Hendrix, J.A., Taniguchi, T., Strom, K.J., Aagaard, B., & Johnson, N. (2019). Strategic policing philosophy and the acquisition of technology: Findings from a nationally representative survey of law enforcement. *Policing and Society*, 29(6), 727-743. <https://doi.org/10.1080/10439463.2017.1322966>.

- Houwing, L., & Ritsema Van Eck, G.J. (2020). Police Bodycams as Equiveillance Tools? Reflections on the Debate in the Netherlands. *Surveillance & Society*, 18(2), 284-287. <https://doi.org/10.24908/ss.v18i2.13925>.
- Hyatt, J.M., Mitchell, R.J., & Ariel, B. (2017). The effects of a mandatory body-worn camera policy on officer perceptions of accountability, oversight, and departmental culture. *Villanova Law Review*, 62(5), 1005-1035.
- Ilijazi, V., Milic, N., Milidragovic, D., & Popovic, B. (2019). An Assessment of Police Officers' Perception of Hotspots: What Can Be Done to Improve Officer's Situational Awareness? *ISPRS International Journal of Geo-Information*, 8(6), 260. <https://doi.org/10.3390/ijgi8060260>.
- Ioimo, R.E., & Aronson, J.E. (2004). Police field mobile computing: applying the theory of task-technology fit. *Police Quarterly*, 7(4), 403-428. <https://doi.org/10.1177/1098611103251113>.
- Jennings, W.G., Fridell, L.A., & Lynch, M.D. (2014). Cops and cameras: Officer perceptions of the use of body-worn cameras in law enforcement. *Journal of Criminal Justice*, 42(6), 549-556. <https://doi.org/10.1016/j.jcrimjus.2014.09.008>.
- Jennings, W.G., Lynch, M.D., & Fridell, L.A. (2015). Evaluating the impact of police officer body-worn cameras (BWCs) on response-to-resistance and serious external complaints: Evidence from the Orlando police department (OPD) experience utilizing a randomized controlled experiment. *Journal of Criminal Justice*, 43(6), 480-486. <https://doi.org/10.1016/j.jcrimjus.2015.10.003>.
- Koen, M.C., & Willis, J.J. (2020). Making sense of body-worn cameras in a police organization: A technological frames analysis. *Police Practice and Research*, 21(4), 351-367. <https://doi.org/10.1080/15614263.2019.1582343>.
- Koen, M.C., Newell, B.C., & Roberts, M.R. (2021). Body-worn cameras: Technological frames and project abandonment. *Journal of Criminal Justice*, 72, 101773. <https://doi.org/10.1016/j.jcrimjus.2020.101773>.
- Koen, M.C., Newell, B.C., & Roberts, M.R. (2023). The Pennybridge pioneers: Understanding internal stakeholder perceptions of body-worn camera implementation. *Journal of Crime and Justice*, 46(2), 194-210. <https://doi.org/10.1080/0735648X.2022.2112265>.
- Koen, M.C., Willis, J.J., & Mastrofski, S.D. (2019). The effects of body-worn cameras on police organisation and practice: A theory-based analysis. *Policing and Society*, 29(8), 968-984. <https://doi.org/10.1080/10439463.2018.1467907>.
- Koper, C.S., Lum, C., & Hibdon, J. (2015). The Uses and Impacts of Mobile Computing Technology in Hot Spots Policing. *Evaluation Review*, 39(6), 587-624. <https://doi.org/10.1177/0193841X16634482>.
- Koper, C.S., Lum, C., Willis, J.J., Woods, D.J., & Hibdon, J. (2015). *Realizing the Potential of Technology in Policing: A Multisite Study of the Social, Organizational, and Behavioral Aspects of Implementing Policing Technologies*. Department of Justice, National Institute of Justice.

- Laming, E. (2019). Police use of body worn cameras. *Police Practice and Research*, 20(2), 201-216. <https://doi.org/10.1080/15614263.2018.1558586>.
- Laming, E., Schneider, C.J., Watson, P.G., & Dubois, F. (2021). Les caméras portatives utilisées par les forces policières : Suppositions et implications. *Criminologie*, 54(1), 15-39. <https://doi.org/10.7202/1076692ar>.
- Laufs, J., & Borrión, H. (2022). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management*, 24(2), 190-209. <https://doi.org/10.1177/14613557211064053>.
- Lawshe, N. (2022). Investigating the influence of institutional perviousness on the adoption of body-worn cameras by United States police agencies. *Criminal Justice Studies*, 35(1), 1-17. <https://doi.org/10.1080/1478601X.2021.1910507>.
- Lee, M., Taylor, E., & Willis, M. (2018). Being held to account: Detainees' perceptions of police body-worn cameras. *Australian & New Zealand Journal of Criminology*, 53(3), 1-19. <https://doi.org/10.1177/0004865818781913>
- Lum, C., Koper, C.S., Willis, J., Happeny, S., Vovak, H., & Nichols, J. (2019). The rapid diffusion of license plate readers in US law enforcement agencies. *Policing: An International Journal*, 42(3), 376-393. <https://doi.org/10.1108/PIJPSM-04-2018-0054>.
- Manning, P.K. (1992). Technological dramas and the police: Statement and counter-statement in organizational analysis. *Criminology*, 30(3), 327-346.
- Meyer, M. (2020). *Essai-pilote des caméras-piétons (bodycam) dans le canton de Vaud et en ville de Lausanne*. Université de Lausanne. [https://www.vd.ch/fileadmin/user\\_upload/organisation/dse/polcant/fichiers\\_pdf/2020/Polcant/Rapport\\_d\\_%C3%A9valuation\\_bodycams\\_.pdf](https://www.vd.ch/fileadmin/user_upload/organisation/dse/polcant/fichiers_pdf/2020/Polcant/Rapport_d_%C3%A9valuation_bodycams_.pdf).
- Moore, M.H. (1992). Problem-Solving and Community Policing. *Crime and Justice*, 15, 99-158. <http://www.jstor.org/stable/1147618>.
- Mrozla, T.J., & Marin Hellwege, J. (2020). Gender composition and agency decision-making: Female officers' effect on body-worn camera acquisition. *Policing: An International Journal*, 43(4), 625-641. <https://doi.org/10.1108/PIJPSM-02-2020-0024>.
- Norman, A., & Allen, D. (2005). Deployment and Use of Mobile Information Systems: A case study of police work. In J. Krogstie, K. Kautz & D. Allen (Eds.), *Mobile Information Systems II* (pp. 203-228). Springer US. [https://doi.org/10.1007/0-387-31166-1\\_15](https://doi.org/10.1007/0-387-31166-1_15).
- Norris, C., & L'Hoiry, X. (2017). Times of crises and the development of the police national automatic number plate recognition system in the UK. In K. Boersma & C. Fonio (Eds.), *Big Data, Surveillance and Crisis Management* (1st ed.). Routledge. <https://www.taylorfrancis.com/chapters/edit/10.4324/9781315638423-11/times-crises-development-police-national-automatic-number-plate-recognition-system-uk-clive-norris-xavier-hoiry>.
- Nowacki, J.S., & Willits, D. (2018). Adoption of body cameras by United States police agencies: An organisational analysis. *Policing and Society*, 28(7), 841-853. <https://doi.org/10.1080/10439463.2016.1267175>.

- Nunn, S. (2001). Police information technology: Assessing the effects of computerization on urban police functions. *Public Administration Review*, 61(2), 221-234.
- Pelfrey, W.V., & Keener, S. (2018). Body-worn cameras and officer perceptions: A mixed-method pretest posttest of patrol officers and supervisors. *Journal of Crime and Justice*, 41(5), 535-552. <https://doi.org/10.1080/0735648X.2018.1479287>.
- Pica, D.N. (2006). *The rhythms of interaction with mobile technologies: Tales from the police*. London School of Economics and Political Science.
- Poirier, B. (2021). Comprendre le succès et l'échec de l'innovation policière : Une analyse du déploiement de caméras portatives dans un service policier. *Criminologie*, 54(1), 69-96. <https://doi.org/10.7202/1076694ar>.
- Pyo, S. (2020). Contingency factors explaining policy adoption: Body-worn camera policy across US states. *Policy Sciences*, 53(3), 413-435. <https://doi.org/10.1007/s11077-020-09398-9>.
- Pyo, S. (2022). Understanding the Adoption and Implementation of Body-Worn Cameras among U.S. Local Police Departments. *Urban Affairs Review*, 58(1), 258-289. <https://doi.org/10.1177/1078087420959722>.
- Randol, B.M. (2014). Modelling the Influence of Organisational Structure on Crime Analysis Technology Innovations in Municipal Police Departments. *International Journal of Police Science & Management*, 16(1), 52-64. <https://doi.org/10.1350/ijps.2014.16.1.327>.
- Rani, S., Sai, V., & Maheswar, R. (Eds.) (2022). *IoT and WSN based Smart Cities: A Machine Learning Perspective*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-84182-9>.
- Ratcliffe, J.H., Taylor, R.B., & Fisher, R. (2020). Conflicts and congruencies between predictive policing and the patrol officer's craft. *Policing and Society*, 30(6), 639-655. <https://doi.org/10.1080/10439463.2019.1577844>.
- Ravid, D.M., Tomczak, D.L., White, J.C., & Behrend, T.S. (2020). EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. *Journal of Management*, 46(1), 100-126. <https://doi.org/10.1177/0149206319869435>.
- Ready, J.T., & Young, J.T.N. (2015). The impact of on-officer video cameras on police-citizen contacts: Findings from a controlled experiment in Mesa, AZ. *Journal of Experimental Criminology*, 11(3), 445-458. <https://doi.org/10.1007/s11292-015-9237-8>.
- Redlein, A., & Höhenberger, C. (2020). Digitalisation. In A. Redlein (Ed.), *Modern Facility and Workplace Management: Processes, Implementation and Digitalisation* (pp. 139-176). Springer. <https://doi.org/10.1007/978-3-030-35314-8>.
- Rooseleers, L. (2023). *Apps voor politie: Een 'realist evaluation' van de impact van mobiele informatietechnologie op politionele besluitvorming en op de interactie tussen politie en burgers*, doctoral dissertation, KU Leuven.

- Rosenbaum, D.P. (2019). Critic: the limits of hot spots policing. In D. Weisburd & A. Braga (Eds.), *Police Innovation: Contrasting perspectives* (pp. 314-344). Cambridge University Press. <https://doi.org/10.1017/9781108278423.015>.
- Santos, R.B. (2014). The Effectiveness of Crime Analysis for Crime Reduction: Cure or Diagnosis? *Journal of Contemporary Criminal Justice*, 30(2), 147-168. <https://doi.org/10.1177/1043986214525080>.
- Saskia Bayerl, P., Jacobs, G., Deneff, S., van den Berg, R.J., Kaptein, N., Birdi, K., Bisogni, F., Cassan, D., Costanzo, P., Gascó, M., Horton, K., Jochoms, T., Mirceva, S., Krstevska, K., van den Oord, A., Otoi, C., Rajkovchevski, R., Reguli, Z., Rogiest, S., Stojanovski, T., Vit, M., & Vonas, G. (2013). The role of macro context for the link between technological and organizational change. *Journal of Organizational Change Management*, 26(5), 793-810. <https://doi.org/10.1108/JOCM-05-2013-0076>.
- Saulnier, A., St Louis, E., & McCarty, W. (2019). Procedural justice concerns and support for BWCs: Turning the lens to officer perceptions. *Policing: An International Journal*, 42(4), 671-687. <https://doi.org/10.1108/PIJPSM-09-2018-0137>.
- Saulnier, A., Bagg, J., & Thompson, B. (2021). Canadian Policing and Body-Worn Cameras: Factors to Contemplate in Developing Body-Worn Camera Policy. *Canadian Public Policy / Analyse de Politiques*, 47(2), 131-157. <https://www.jstor.org/stable/27034147>.
- Schuilenberg, M., & Soudijn, M. (2021). Big data in het veiligheidsdomein: onderzoek naar big data-toepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie. *Tijdschrift voor Veiligheid*, 1-16. <https://doi.org/10.5553/TvV/4001>.
- Shapiro, A. (2019). Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing. *Surveillance & Society*, 17(3), 456-472.
- Simmler, M., Brunner, S., Canova, G., & Schedler, K. (2023). Smart criminal justice: Exploring the use of algorithms in the Swiss criminal justice system. *Artificial Intelligence and Law*, 31(2), 213-237. <https://doi.org/10.1007/s10506-022-09310-1>.
- Singh, M. (2017) Mobile technologies for police tasks: An Australian study. *Journal of Organizational Computing and Electronic Commerce*, 27(1), 66-80, <https://doi.org/10.1080/10919392.2016.1263114>.
- Singh, M., & Hackney, R. (2011). *Mobile technologies for public police force tasks and processes: A t-Government perspective*, 19th European Conference on Information Systems (ECIS), Helsinki.
- Smith, J. (2019). To Adopt or Not to Adopt: Contextualizing Police Body-Worn Cameras Through Structural Contingency and Institutional Theoretical Perspectives. *Criminal Justice Review*, 44(3), 369-385. <https://doi.org/10.1177/0734016819847267>.
- Smykla, J.O., Crow, M.S., Crichlow, V.J., & Snyder, J.A. (2016). Police Body-Worn Cameras: Perceptions of Law Enforcement Leadership. *American Journal of Criminal Justice*, 41(3), 424-443. <https://doi.org/10.1007/s12103-015-9316-4>.

KEVIN EMLIT, MAXIME MAUQUOY AND LIES VANDE MEULEBROUCKE

- Snyder, J.A., Crow, M.S., & Smykla, J.O. (2019). Police Officer and Supervisor Perceptions of Body-Worn Cameras Pre- and Postimplementation: The Importance of Officer Buy-in. *Criminal Justice Review*, 44(3), 322-338. <https://doi.org/10.1177/0734016819846223>.
- Sørensen, C., & Pica, D.N. (2005). Tales from the police: Rhythms of interaction with mobile technologies. *Information and Organization*, 15, 125-149. <https://doi.org/10.1016/j.infoandorg.2005.02.007>.
- Sousa, W.H., Miethe, T.D., & Sakiyama, M. (2015). *Body Worn Cameras on Police: Results from a National Survey of Public Attitudes*. University of Nevada Las Vegas, Center for Crime and Justice Policy.
- Sousa, W.H., Coldren, J.R., Rodriguez, D., & Braga, A.A. (2016). Research on Body Worn Cameras: Meeting the Challenges of Police Operations, Program Implementation, and Randomized Controlled Trial Designs. *Police Quarterly*, 19(3), 363-384. <https://doi.org/10.1177/1098611116658595>.
- Tange, C. (2020). *Piloter la police à l'aide des statistiques. L'analyse locale au quotidien*. Bruylant.
- Taylor, E. (2016). Lights, Camera, Redaction... Police Body-Worn Cameras; Autonomy, Discretion and Accountability. *Surveillance & Society*, 14(1), 128-132. <http://ojs.library.queensu.ca/index.php/surveillance-and-society/>
- Taylor, E., & Lee, M. (2019). Points of View: Arrestees' Perspectives on Police Body-Worn Cameras and Their Perceived Impact on Police-Citizen Interactions. *The British Journal of Criminology*, 59(4), 958-978. <https://doi.org/10.1093/bjc/azz007>
- Terpstra, J., Fyfe, N.R., & Salet, R. (2019). The abstract police: A conceptual exploration of unintended changes of police organisations. *Police Journal: Theory, Practice and Principles*, 92(4), 339-359. <https://doi.org/10.1177/0032258X18817999>.
- Ter Veen, H., & Kop, N. (2021). *Innovatiekracht versterken. Een longitudinale processtudie naar technologisch innoveren bij de politie 2017-2020*. Politieacademie, Kennis & Onderzoek. <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/100632.PDF>.
- Vepřek, L.H., Sibert, L., Sehn, L., Köpp, L., & Friedrich, D. (2020). Beyond Effectiveness: Legitimising Predictive Policing in Germany. *Kriminologie – Das Online-Journal / Criminology – The Online Journal*, 423-443. <https://doi.org/10.18716/OJS/KRIMOJ/2020.3.3>.
- Verbeek, P.-P. (2015). Beyond interaction: a short introduction to mediation theory. *Interactions*, 22(3), 26-31. <https://doi.org/10.1145/2751314>
- Verhage, A., Easton, M., & De Kimppe, S. (2022). *Policing in Smart Societies – Reflections on the Abstract Police*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-030-83685-6>.
- Wain, N., Ariel, B., & Tankebe, J. (2017). The collateral consequences of GPS-LED supervision in hot spots policing. *Police Practice and Research*, 1-15. <https://doi.org/10.1080/15614263.2016.1277146>.

- White, M.D. (2014). *Police Officer Body-Worn Cameras: Assessing the evidence*. U.S. Department of Justice. [https://bja.ojp.gov/sites/g/files/xyckuh186/files/bwc/pdfs/diagnosticcenter\\_policeofficerbody-worncameras.pdf](https://bja.ojp.gov/sites/g/files/xyckuh186/files/bwc/pdfs/diagnosticcenter_policeofficerbody-worncameras.pdf).
- White, M.D., Todak, N., & Gaub, J.E. (2018). Examining Body-Worn Camera Integration and Acceptance Among Police Officers, Citizens, and External Stakeholders. *Criminology & Public Policy*, 17(3), 649-677. <https://doi.org/10.1111/1745-9133.12376>.
- Willis, J.J. (2022). 'Culture eats strategy for breakfast': An in-depth examination of police officer perceptions of body-worn camera implementation and their relationship to policy, supervision, and training. *Criminology & Public Policy*, 21(3), 713-737. <https://doi.org/10.1111/1745-9133.12591>.
- Wilson, D. (2019). Platform Policing and the Real-Time Cop. *Surveillance & Society*, 17(1/2), 69-75. <https://doi.org/10.24908/ss.v17i1/2.12958>.
- Završnik, A., & Badalic, V. (2021). *Automating crime prevention, surveillance, and military operations*. Springer. <https://doi.org/10.1007/978-3-030-73276-9>.



## 5 ADVANCING THE POTENTIAL OF VR IN POLICING

### *Exploring the role of deepfake technologies in research and training – A discussion in the context of over and under policing minorities*

Meret Asara Paululat, Bas Böing, Vlad Niculescu-Dinca and Peter W. de Vries

#### **Abstract**

*This study explores the potential of virtual reality (VR) in police training. It delves into the use of deepfake technology in an experiment investigating how racist stereotypes influence Dutch police officers' behaviour in stop-and-search scenarios. In a 2x2 experimental design, 87 officers encountered racist stereotypes and deepfake manipulations in the VR environment. Findings indicate widespread acceptance of VR in policing, consistent with prior research (De Vries et al., 2023), and contrary to previous perceptions, highlighting the near-perfect imperceptibility of deepfake, enhancing VR immersion. Notably, participants exposed to deepfake of a non-white person tended to avoid selecting said ethnic minorities for stop-and-search, hinting at a potential avoidance behaviour. Furthermore, we examined the impact of VR and deepfake on user experience measured through self-reported feelings of presence, engagement, enjoyment and embodiment of police officers in daily work. We used technological mediation theory to explore how these factors influence participants' perceptions and actions. The study reveals a unique mediation, intertwining individuals, technology, reality and simulation, with participants reporting dual experiences oscillating between immersion and grounding. Reflecting on this interplay, our study underscores the transformative potential of VR and deepfake in policing research and training but highlights the importance of preserving the fidelity of the virtual-to-real-world connection to harness these technologies' potential effectively.*

#### 5.1 INTRODUCTION

In recent years, virtual reality (VR) and deepfake technology advancements have ushered in transformative possibilities for policing practices, training and research. As these technologies gain prominence, their impact on law enforcement has become a subject of considerable interest. Specifically, the Dutch police has recently implemented large-scale VR training programmes, while many other countries, such as the US, Mexico, Belgium and Germany, have also adopted VR in their policing and military training (Kliem, 2019; Giessing & Frenkel, 2022).

MERET ASARA PAULULAT, BAS BÖING, VLAD NICULESCU-DINCA AND PETER W. DE VRIES

The integration of VR in policing programmes has emerged as a promising avenue for creating realistic and controlled environments that simulate various law enforcement or military scenarios.<sup>1</sup> From enhancing training exercises to providing a safe space for research, VR technology offers a unique platform for immersive experiences. Studies have demonstrated its efficacy in improving police training, allowing officers to navigate complex situations risk-free by virtual recreation of sensitive, dangerous or costly situations (Binsch et al., 2022; Cornet & Van Gelder, 2020).

## 5.2 THE ISSUES OF ETHNIC PROFILING AND RACIST STEREOTYPES

One research area in which VR has recently been used by the Dutch police is ethnic profiling among police officers. The issue of ethnic profiling in policing, particularly in the Netherlands, has gained significant attention amid accusations of racism and discriminatory practices (European Commission against Racism and Intolerance, 2020). Ethnic profiling involves singling out individuals based on their ethnicity, nationality or religion, leading to a decrease in trust among ethnic minorities in law enforcement. Instances of police discrimination, especially in stop-and-search procedures targeting Turkish and Moroccan minorities in the Netherlands, have been recognised, impacting both the affected communities and police legitimacy (van Steden et al., 2012)

Public discourse, fuelled by movements like Black Lives Matter and amplified on social media, has heightened awareness, but it also risks reinforcing a stereotype of a racist police force (Carney, 2016). Research suggests that racist stereotypes about the police may influence officers' behaviour in stop-and-search situations (Trinkner et al., 2019). Indeed, exposure to stereotypes may lead to stereotype threat, where individuals from relevant groups who fear confirming negative stereotypes end up acting in accordance with them (Steele & Aronson, 1995). On the other hand, some people actively resist stereotypes, a phenomenon of avoiding situations that would confirm the negative stereotype known as stereotype reactance. For example, police officers may try overly hard to counteract racist perceptions. In stop-and-search situations, officers who are aware of racial bias stereotypes might change their behaviour to avoid being seen as racist. This can sometimes lead to self-fulfilling prophecies, where their altered behaviour being too extreme towards the other side of the spectrum, such as avoiding minority groups all together, unintentionally reinforces the stereotypes they were trying to avoid (Krey et al., 2004).

---

<sup>1</sup> Recently, the potential of these technologies and programmes has also received recognition through the Europol Excellence Award being won by the Dutch national police. The programme using virtual reality and deepfakes won the award at the category 'Innovative Initiative in Ethics, Diversity and Inclusion' (Europol, 2023).

Despite concerns about potential consequences, there has not been a thorough investigation into how stereotype threat connects racist stereotypes of the general public to stop-and-search behaviour (Trinkner et al., 2019; McCarthy et al., 2021). The influence of racist stereotypes on stop-and-search behaviour is under-researched; past studies point to the adverse effects of both over- and under-policing. Over-policing, characterised by excessive law enforcement in marginalised areas and disproportionately impacting racial or ethnic minorities, may lead to increased feelings of insecurity and distrust in the justice system (Boehme et al., 2020; Johnson et al., 2022). Conversely, under-policing, inadequate security or intervention may result in adverse outcomes such as slow emergency responses and increased crime rates (Johnson et al., 2022). While the precise impact of stereotypes on stop-and-search behaviour is unknown, Trinkner's framework (2019) suggests that officers may adjust their behaviour based on prevailing stereotypes. Given the prevalent racist stereotype of aggressive and hostile policing, it is plausible that stereotype threat contributes to over-policing in stop-and-search activities (Gauthier & Graziano, 2018). Debates about this are a topic laden with political and social implications, making it particularly sensitive to discuss and research. As ethnic profiling increasingly enters public debates and is addressed within policing policies, increasing the likelihood that participants in related research projects might respond with increases in social desirability. Officers, aware of the public scrutiny and the potential implications of such studies, might alter their responses to align with what they perceive as socially or institutionally expected. This can skew the authenticity of the data gathered, complicating the analysis and interpretation of the results.

Despite these challenges, the topic's inherent complexity and relevance only heighten the importance of thorough and thoughtful investigation. While there is a risk that officers might cater their responses to expected norms, acknowledging this tendency is a crucial part of the research process. By understanding potential biases in responses, researchers can develop more refined methodologies that strive to capture genuine attitudes and behaviours in the future. Thus, even though participants might act in a manner they deem socially desirable, we submit that the insights gained from such studies remain relevant, providing a critical lens through which the dynamics of ethnic profiling and its broader societal impacts can be explored. Especially with topics like racist stereotyping in the context of ethnic profiling in police work, using VR environments for research or training is a significant opportunity that would not be possible otherwise due to its sensitive nature (Fox et al., 2009).

### 5.3 THE POTENTIAL AND ISSUES OF DEEPPAKES IN VR

Virtual reality as a technology for training and research has gained ground in the police context. Not only is it theorised that VR can recreate hyper-realistic scenarios from everyday police work to conduct studies in a safe and controlled environment, but it has

MERET ASARA PAULULAT, BAS BÖING, VLAD NICULESCU-DINCA AND PETER W. DE VRIES

also been proven that virtual reality can improve police training significantly by offering immersive experiences that enhance officers' decision-making skills, crisis management and situational awareness (Kleygrewe et al., 2023). Recent technological advancements have made it possible to utilise deepfake technology in realistic 360° VR simulations, i.e. VR environments based on 360° camera recordings. Deepfakes are artificially crafted images in which a person in an existing image or video is replaced with someone else's likeness (Kietzmann, 2019). By overlaying the face of one individual in a 360° VR setting with that of another person, deepfake technology enables the creation of multiple identical VR environments except for the appearance of the focal individual. In investigating racism, ethnic profiling and stereotypes, one could offer different participants realistic environments that differ only in the apparent ethnic background of the persons in it, eliminating variation in mimics, gestures and backgrounds (Fox et al., 2009). As such, this technology allows for studying critical societal phenomena in realistic, real-life settings while maintaining a maximum degree of experimental control and, thus, potentially drastically increasing the results' validity.

However, when working with VR and deepfake technology, it is crucial to understand if and how the technology influences its users' perceptions, experiences and actions. The colloquial conception of technology describes technology as merely neutral devices, means for chosen human ends (Encyclopaedia Britannica, 2023). However, in the past, various schools of thought have strongly challenged this conception from the perspective of history, sociology and philosophy of technology. According to these insights and analyses, technologies are more adequately conceptualised as actively mediating between people and the world (Ihde, 2009; Verbeek, 2005; Niculescu-Dinca 2021). The theory of technological mediation describes technology as actively mediating social structures, interpersonal connections and human behaviour through design, functionalities and affordances that can shape how individuals think, act and engage with the world (Verbeek, 2016). It contends that how people view, engage with and interact with the outside world is strongly mediated by various forms of technology. For instance:

the reality of a star is profoundly mediated by telescopes, brain activity by MRI scanners, and the health condition of a foetus by ultrasound devices. Such mediations are not merely neutral 'intermediaries': What a star, the brain, and an unborn child are for us cannot be understood without taking into account the mediating role of technologies in our perception and understanding of them. (Verbeek, 2025, p. 29)

Similarly, (video) calling mediates between people in different locations, shaping their perception of each other, significantly enhancing or diminishing certain features and sensorial experiences. Or, in the policing domain, what is a suspect, suspicious behaviour or a problematic area are mediated by information infrastructures such

as geographic information systems, profiling algorithms or predictive analytics (Niculescu-Dinca, 2018). Social norms, power dynamics and communication patterns can all be changed by technological mediation as people use technologies in various types of relations: embodying them, as with glasses or binoculars, interpreting their output in a hermeneutic relation, interacting with them in an alterity relation or when they shape their experiences from the background (Ihde, 1990; Verbeek, 2005; 2016). Therefore, it is crucial to consider a potential mediation in the context of such study designs (Kyrre & Crease, 2015).

At the same time, a deepfaked VR environment becomes a new technology that subsequently calls for analysis, potentially introducing a new type of technological mediation. This is because VR mediates not only between the world and the individual, but also between the individual and a metaverse or alternate reality, while simultaneously aiming to replicate the outside world. Mediation theory has mainly analysed human-technology-world relations (embodiment, hermeneutic, alterity, background, augmentation, etc.; see Ihde, 1990; Verbeek, 2015) in which 'the world' has largely been assumed constant and unitary. However, VR environments introduce a new relation in which a 'new world' is simulated, enhancing/changing the human experiences. At the same time, the user is still able to perceive reality (e.g. through other senses, knowledge frameworks). Therefore, given its novelty and the methodological aims of such studies to infer conclusions about the behaviour of participants in real-world scenarios, we argue for more theoretical and empirical investigations of the mediating influence of VR environments.

The concept of immersion has been utilised in past research to gain insight into the degree of mediation (Barbot & Kaufman, 2020). Immersion describes psychological and cognitive mechanisms responsible for producing a sensation of immersion in a virtual or simulated world. It focuses on the elements that conceptualise the degree to which people have realistic experiences in various settings. Past research has found presence, engagement, enjoyment and embodiment to be of specific importance when analysing immersion (Cornet & Van Gelder, 2020). Presence refers to the sensation of 'being there', completely engrossed in and linked to the virtual world, seeing it as real and tactile in the context of virtual reality or immersive experiences (Witmer & Singer, 1998). Engagement describes individuals' involvement, interest and attention in a task or event. In virtual reality or immersive experiences, it refers to the degree to which users actively engage with, communicate with and react to the virtual world.

Furthermore, enjoyment describes the pleasant emotional state or pleasure from a task or event (De Vries et al., 2023). Lastly, embodiment aims to capture the experience of possessing and controlling an avatar or virtual body inside a virtual world. It entails having the impression that one's virtual self is an extension of oneself, which heightens one's sensation of presence in and identification with the virtual environment (Banakou et al., 2016). Ultimately, this study will look at the *user experience*, representing the

MERET ASARA PAULULAT, BAS BÖING, VLAD NICULESCU-DINCA AND PETER W. DE VRIES

degree of immersion, to assess the mediating role of the technologies involved (see Figure 5.1).

However, due to the lack of literature and previous research on the impact of deepfake technology specifically, its relationship with user experience and stop-and-search behaviour will be analysed more holistically, combining a VR experiment with gathering police officers' opinions.

Overarchingly, this study aims to investigate the impact of racist stereotypes on police behaviour during stop-and-search scenarios and to explore how VR and deepfake technologies may influence the perceptions and stop-and-search actions of police officers, ultimately hoping to provide insights into how these technologies can be used effectively in training and research.

#### 5.4 THE DEEPAKE STUDY

The current study included two manipulations. The first is the *racist stereotype*. In the experimental group, participants were confronted with a video of police officers being accused of racism. The control group was shown a racism-unrelated video. The second manipulation is the *'deepfake'*. This determines whether the VR environment includes a person from an ethnic minority or only individuals with white physical appearances. Ultimately, the dependent variable, 'stop-and-search behaviour', was measured by the behaviour the police officers showed in the VR environment in hopes of understanding officers' real-life behavioural reactions. This experiment was followed by a questionnaire that included items asking about the 'user *experience*', amongst other questions. These questions were included to account for a potential technological mediation.

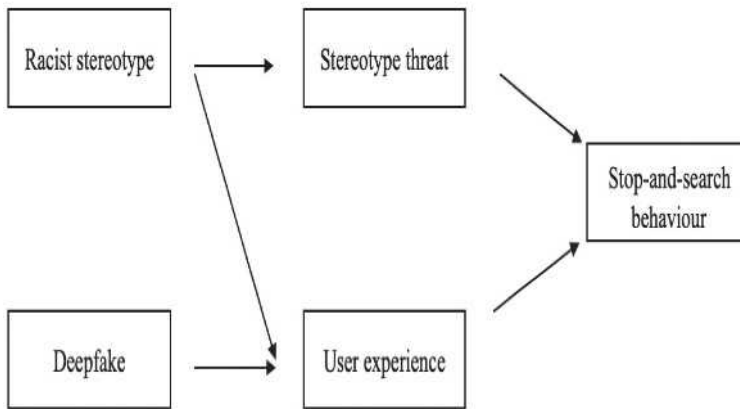
*Hypothesis 1:* Watching the racist stereotype video influences Dutch police officers' stop-and-search behaviour; specifically, exposure to the racist stereotype causes more over-policing.

*Hypothesis 2:* The police officers' level of stereotype threat explains the relationship between the watching the racist stereotype video and stop-and-search behaviour.

*Hypothesis 3:* The police officers' level of user experience explains the relationship between watching the racist stereotype video and stop-and-search behaviour.

*Research Question:* How do the VR deepfake technology and user experience affect stop-and-search behaviour?

Figure 5.1 Conceptual model



## 5.5 METHODS

### 5.5.1 Participants

Ninety-six police officers were gathered through purposive sampling utilising a LinkedIn post. All police stations across the Netherlands were invited to respond to the conducting of a social psychological experiment using VR technology. Before analysing the data, several participants had to be removed from the dataset to obtain valid results. Specifically, nine participants from the initial 96 police officers were removed because they used the wrong VR goggles and could not clearly be placed in a condition. Therefore, after deleting invalid participants, 87 Dutch police officers (65M, 22F,  $M_{age} = 35.05$ ,  $SD_{age} = 9.87$ ) represented the final sample for analysis. The officers or detectives had to have stop-and-search experience to be included. The self-reported working experience was assessed on a scale ranging from 1 to 5, where 1 indicates a working experience of less than 10 years, 2 equals 10-20 years, 3 means 20-30 years, 4 is 30-40 years, and 5 represents a working experience of more than 40 years. Based on this scale, the police officers had an average working experience of 1.87 ( $SD = 0.96$ ). Participants worked at the police stations in Amsterdam, Rotterdam, Utrecht, Wageningen and Zwolle.

### 5.5.2 Procedure

Prior to the start of the experiment, the study was reviewed and approved by the Ethics Committee of the University of Twente.

#### 5.5.2.1 Before VR-environment phase

For the data collection, at least two researchers travelled to the respective police stations within the Netherlands. Upon arrival, two or three stations for conducting the experiment were set up, including a laptop, Oculus VR goggles and headphones. All participants were given a short introduction to the structure of the experiment. The exact aim of the study was not disclosed in advance. Participants were told that the study investigated how public opinion influences police officers. Next, participants were given a digital informed consent sheet and a short pre-questionnaire to assess demographic information on a laptop using Qualtrics XM as part of the subsequent questionnaire.

Subsequently, participants were shown a short video with headphones on. Forty-one participants saw a video, namely the stereotype threat manipulation from YouTube posted by the account Godgiven, depicting Dutch officers being accused of ethnic profiling. The video showed a black individual videoing himself while talking to two white police officers in the Netherlands. Concretely, he is videoing the officers while calling them racist and elaborating that this is normal policing practice in the Netherlands. He speaks loudly into the camera, explaining that he was pushing two rented bicycles, which would not have been suspicious if he was white. The video is 2:59 mins long and in English (Fabri, 2020). The other half of the police officers (46) were shown a non-racism-related video. This video originated from the social media platform X (formerly Twitter) and was posted by the account KombijdePolitie. It depicts a police representative sitting in a car explaining recent successes. It is 0:44 mins long and in Dutch (KombijdePolitie, 2023).

Subsequently, all participants put on the VR goggles and headphones. Before entering the environment, the researchers explained that a casual street scenario would take place and a stop-and-search task could be carried out if perceived to be necessary, in which case the participant could select a person by simply staring at them for two seconds. This was also explained again in a short introduction to the environment itself. Moreover, it was explicitly stated that it was not required to choose a person, in which case the participant would return the glasses to the researchers.

#### 5.5.2.2 360° VR Environment

Half of the participants who saw the stereotype threat video and half of the participants who saw the non-racism-related video were presented with a VR environment in which the person sitting on a scooter has the facial characteristics of a white person. The other half of the police officers were shown a version of the deepfake VR environment in which the person on the scooter possesses non-white facial characteristics. These were applied

to the originally white-looking person using deepfake technology. The participants found themselves virtually in the financial district of Amsterdam. Surrounding them, four men are standing at different distances. One man is sitting on a scooter, one is on his phone, one is in a suit, and one is looking around. In the background, there is typical street noise, pedestrians, cyclists and cars. The person on the scooter is positioned closest to the viewer.

After selecting one of the four individuals, or if the participant decided not to select anyone, the VR part was finished. Then, the police officers selected ‘feedback’ and received a code depending on which person was chosen, which had to be indicated in the following questionnaire. The officers who did not select a person did not receive a code and subsequently indicated that in the questionnaire. The overview of people that could be selected in the VR can be found in Figure 5.2.

**Figure 5.2** Persons overview



The people depicted in the VR will be referred to as person 1, person 2, person 3 and person 4. Importantly, person 1 possesses facial characteristics associated with a migrant background in the deepfake condition and white facial characteristics in the original VR version in which deepfake technology was not used. All other individuals remain the same in both VR versions.

Considering all manipulations, the experiment divided participants into four groups. The first group, which consisted of 20 participants, watched a racist stereotype video and saw a white man on a scooter. The second group, comprising 21 participants, viewed the same racist stereotype video but saw a man on a scooter who appeared to be non-white. The third group, with 23 participants, watched a non-racism-related video and saw a man on a scooter with white looks. Finally, the fourth group, also with 23 participants, viewed a non-racism-related video but saw a man on a scooter with non-white looks. The 87 participants were randomly assigned to each group before the start of the experiment.

### 5.5.2.3 *Post-VR environment phase*

After finishing the VR game, participants completed the central part of the questionnaire. Questions were asked regarding the participant’s motivations and intentions underlying the decision to choose or not choose a person (i.e. ‘It is possible that you addressed

someone in the simulation. If so, what do you think was the reason for this?'). Additionally, questions were asked regarding user experience, self-legitimacy, stereotype threat, workplace racial anxiety, force support, stigma feelings and training willingness. After responding to all questionnaire items, the participants were asked to accept a digital post-consent form, and finally a thank-you notice was displayed. Upon completing the questionnaire, participants were offered further explanations about the true nature of the study. Additionally, there was space for debriefing and open conversations. Afterwards participants were given the opportunity to withdraw their participation after they were told the true character of the study.

## 5.6 MEASURES

### 5.6.1 *Stop-and-search behaviour*

Stop-and-search behaviour was categorised by hand based on the answers to the open questions. Thus, stop-and-search behaviour was classed as over-policing (2), under-policing (0), or neutral policing (1) based on the availability and strength of reasoning for selecting, talking to or checking someone's ID.

Over-policing (2) was classified when officers checked someone's ID without any clear indication of why they did so, did not provide a clear and appropriate reason that aligned with policing standards for talking to the person, or mentioned discriminatory reasons for stopping and checking someone.

Neutral policing (1) was classified when officers did not select anyone, chose to engage in conversation with individuals simply to chat, or provided a reason for checking someone that was consistent with policing standards. Examples include seeing someone on a scooter parked on the pavement, or noticing a person riding a bike without a helmet.

Under-policing (0) was classified when officers did not select anyone for a stop-and-search without stating a clear reason, even if they mentioned finding someone suspicious. For example, they might have noted finding a person on a scooter suspicious but decided not to take any action.

This variable was named SAS (Stop and Search). The variable PSAS was also created to include an additional way of measuring stop-and-search behaviour, which constituted the person selected.

All other additional questions in the present study could be answered on a 5-point Likert scale, ranging from 'Strongly disagree' (1) to 'Strongly agree' (5).

### 5.6.2 *User experience*

Seven items measuring participants' quality of user experience to test for a potential technological mediation were incorporated based on the scale utilised by De Vries et al. (2023). This measure consisted of presence, engagement and enjoyment (Barbot & Kaufman, 2020; Cornet & van Gelder, 2020). Consistency measures were calculated for this scale and revealed a Cronbach's alpha of .78 and a Guttman's lambda2 of .80. An example item is 'During the simulation, interaction with the other people felt realistic'.

### 5.6.3 *Stereotype threat*

A five-item scale was used to determine the police officers' perceived stereotype threat. For example, the items contain statements like 'I worry that people may think of me as racist because I am a police officer'. The scales' reliability was assessed, suggesting acceptable internal consistency based on Cronbach's alpha = .78 (n=87). Since Cronbach's alpha is vulnerable to a low number of items, Guttman's lambda2 was determined, suggesting a high degree of internal consistency with a Guttman's lambda2 of .82. Therefore, the scale chosen was determined to be reliable.

### 5.6.4 *Open questions*

To gather qualitative insights, the questionnaire included several open questions. First, after leaving the VR environment, the police officers were asked to continue by filling out the questionnaire. Here, they were asked about their motives and reasons for why they did or did not select a person in the VR environment. The open questions were: 'It is possible that you addressed someone in the simulation. If so, what do you think was the reason for this?' and 'If you did not address anyone, what do you think was the reason for this?'. Secondly, to give additional information about the user experience regarding the environment, police officers were asked, 'How do you feel about the VR environment? Explain the extent to which you felt it was realistic and reflected your actions in real life (please explain why)'. Moreover, to gather qualitative insights on how the police officers feel emotionally affected by the publicity all around the topic of institutional racism, they could answer the question, 'Would you tell us a little more about whether, and if so, in what ways you, as a police officer, feel emotionally affected by the public debate about structural racism in policing?'.

A thematic analysis was used to analyse the open question regarding user experience to better understand the technology's impact. The primary objective was to develop separate themes based on the participant's responses to offer broad perspectives on the

MERET ASARA PAULULAT, BAS BÖING, VLAD NICULESCU-DINCA AND PETER W. DE VRIES

influence of the utilised technology. The theme analysis followed Braun and Clarke's (2006) six-step paradigm.

## 5.7 RESULTS

Investigating the impact of the manipulations and understanding the differences between the conditions, the average user-experience score was 2.54 ( $M = 2.54$ ,  $SD = 0.55$ ). For the condition with a racist stereotype and deepfake manipulation, the average score was 2.47; for the condition with a racist stereotype and no deepfake manipulation, it was 2.52; for the condition without a racist stereotype and with deepfake manipulation, it was 2.5; and for the condition without a racist stereotype and without deepfake manipulation, it was 2.64.

Correlation analysis revealed a substantial negative correlation between the presence of deepfake and the selection of person 1 ( $r = -.24$ ), indicating that participants were less likely to choose person 1 in virtual stop-and-search situations when encountering the deepfake version of the VR environment, which portrayed person 1 as a non-white person. In contrast, there was a significant positive association between deepfake and the selection of person 2 ( $r = .36$ ). Additionally, user experience showed a negative correlation with self-legitimacy ( $r = -.26$ ), indicating the importance of high self-legitimacy for a better user experience. Furthermore, a correlation was found between user experience and neutral policing ( $r = .24$ ), suggesting a potential impact of a high user experience of the VR on recorded behaviour. Lastly, user experience was highly correlated with willingness to participate in training ( $r = .32$ ). No correlation was found related to stereotype threat.

### 5.7.1 Main analysis

A multivariate analysis of variance (MANOVA) was conducted with the deepfake and racist stereotype, on various outcome variables including the stop-and-search behaviour, stereotype threat, self-legitimacy, user experience and training willingness. The analysis revealed non-significant effects for the main factors of deepfake (Wilks'  $\Lambda = 0.12$ ,  $F(8, 76) = 1.16$ ,  $p = 0.33$ ) and condition (Wilks'  $\Lambda = 0.062$ ,  $F(8, 76) = 0.62$ ,  $p = 0.75$ ). Additionally, the interaction between the deepfake and racist stereotype was insignificant, along with all other variables (Wilks'  $\Lambda = 0.08$ ,  $F(8, 76) = 0.89$ ,  $p = 0.52$ ). According to these results, stop-and-search behaviour, stereotype threat and user experience were not significantly impacted by either the encounter with the racial stereotype in a film or the exposure to an ethnic minority in the VR environment. As a result, each of the three assumptions must be disproven.

It is important to note that the development of the stop-and-search behaviour variable based on the actions of the police officers in the VR may have limits in accurately depicting their actions.

Subsequently, the multinomial logistic regression analysis with the person selected (PSAS) showed no significant effects of deepfake on PSAS ( $\beta = 0.086, p > .05$ ), racist stereotype on PSAS ( $\beta = 0.715, p > .05$ ), and the deepfake: interaction on PSAS ( $\beta = 0.202, p > .05$ ) for person 1. Similarly, for person 2, person 3 and person 4, there were no significant effects of deepfake, racist stereotype or the deepfake interaction on PSAS (all  $p$ -values  $> .05$ ).

While not statistically significant, the following is worth mentioning because it suggests a potential trend or pattern that might be worth exploring further with more data or a different analysis. A one-unit increase in the deepfake variable was associated with a 1.09 increase in choosing person 1 compared to the baseline category we found. The odds of selecting person 2 increased by approximately 724,830.27 in the condition with deepfake manipulation. These findings imply that police officers would be far more inclined to select person 2 over person 1 if they saw an ethnic minority as person 1 in the VR environment. This result is consistent with correlational analysis and qualitative insights that had previously revealed that even passing contact with someone from a minority ethnic group might prevent checking someone with a migrant background and cause the focus to shift to person 2.

### 5.7.2 *Thematic analysis*

Lastly, a thematic analysis of the open question regarding user experience with 71 answers was conducted. The thematic analysis followed Braun and Clarke's (2006) six-step paradigm, systematically understanding and interpreting themes in qualitative data. It begins with familiarisation and immersion in the data, followed by coding to identify patterns. Initial themes are generated, reviewed, defined and named, leading to a final report that presents the themes with supporting evidence. This approach provides a rigorous framework for uncovering meaningful insights in qualitative data. Therein, seven major themes of officers' perceptions of the technology emerged (see Table 5.1). Each theme was divided into 0 to 2 codes, each with corresponding 0 to 3 sub-codes. Each answer could have multiple themes.

**Table 5.1 Themes of Officers' Thoughts and Opinions**

Theme	Codes	Sub-codes	Example of Theme	N
Feelings	Natural	1. Realistic	'People in real life naturally react to your nonverbal communication.'	31
	Distorted	1. Interrupted 2. Contradiction 3. Unrealistic		6 14 6
Actions	Own action		'I don't immediately act the same way I would normally act on the street.'	3
	Other actions			8
Problems with VR	Distance		'I felt I was very close to the person on the scooter.'	6
	Bugs			2
	Answer questions			4
Description			'Busy and urban environment with many different people.'	13
Enjoyment			'Fun and very nice.'	4
Usefulness			'I think it's a good way of training and making yourself aware.'	14
Other			'I would mimic some larger simulations and recreate more stressful situations.'	3

*Note:* The officers' thoughts and opinions are illustrated in terms of seven themes. Codes are given for the three themes 'Feelings', 'Actions' and 'Problems VR', while sub-codes are given for 'Natural' and 'Distorted'. Examples are provided verbatim, and the frequency is depicted for each theme and code.

### Feelings

The theme of *Feelings* (N,57) was identified in the data. This theme was divided into two principal codes, namely *Natural* (N,31), describing the environment as feeling natural, and *Distorted* (N,26), describing the environment as feeling unnatural. *With its two main codes, this theme was the most common and evident* in its distribution. It describes participants elaborating on how they felt during the VR. The code *Natural* was composed of one sub-code called *Realistic* (N,31), allocated in cases where participants described the environment as very realistic. An example of this was 'Very realistic, multiple different people'. The code *Distorted* was made up of three sub-codes. *Interrupted* (N,6) describes instances where participants were reminded of the real world. *Contradiction* (N,14) describes a potential partial immersion given that participants were reminded by

something that the environment was still a simulation while reporting feeling immersed. Lastly, *Unrealistic* (N,6) describes participants finding the VR environment somewhat unrealistic. This could mean noticing things in the VR environment that stood out as different from the real world, such as people behaving differently in VR. Participants mentioning that VR is unrealistic might be only partially immersed based on their comment describing being reminded of the differences between VR and the real world.

### **Actions**

The next theme identified was *Actions* (N,11) consisting of the main codes *Own actions* (N,3), referring to one's own actions as unrealistic, and *Others' actions* (N,8), referring to others' actions as unrealistic. An example item was 'I don't immediately act the same way I would normally act on the street'. This indicated that participants saw the people in the VR more as actors than as real-life humans to interact with, potentially highlighting that the VR had a game-like character to some.

### **Problems with VR**

Another identified theme is *Problems with VR* (N,12). One example was 'I felt I was very close to the person on the scooter'. This theme consisted of three codes: *Distance* (N,6), indicating issues with proximity in the VR, *Bugs* (N,2), and lacking *Answer options* (N,4). Participants receiving this code of *Problems* encountered some technical issues, suggesting impaired immersion.

### **Description**

The main theme *Description* (N,13) was identified by describing participants simply reporting the environment in the open question. An example item was 'Busy and urban environment with many different people'. This code highlighted that some participants experienced a level of immersion where they described the simulation as real.

### **Enjoyment**

Another theme identified was the theme of *Enjoyment* (N,4), describing how much fun participants found the VR. An example item of this was 'Fun and very nice'. Receiving this code meant the participants had a good time, conversely making them more likely to commit to the experience, thus improving the potential for immersion.

### Usefulness

The main theme *Usefulness* (N,14) was identified, describing participants stating how useful they found the VR. An example item was ‘I think it’s a good way of training and making yourself aware’. Participants receiving this code most likely saw a higher purpose in the VR and found it more helpful.

### Other

Lastly, the theme *Other* (N,3) was identified for any user input that did not fit any other theme. An example was ‘I would mimic some larger simulations and recreate more stressful situations’. This code covered all additional sentiments that did not match the other codes but were still deemed insightful.

The explorative thematic analysis of the experience highlights the importance of the recurring codes of contradicting and describing. On the one hand, the code *Contradiction* indicated a partial immersion, given that participants, while reporting feelings, emerged and were reminded by something that the environment was still a simulation. On the other hand, the code *Description* highlighted that some participants experienced a level of immersion where they described the simulation as if it were real.

## 5.8 DISCUSSION

Our study aimed to shed more light on the multifaceted potential of VR innovations while exploring the impact of racist stereotypes on police behaviour in stop-and-search scenarios. The first hypothesis, being that exposure to racist stereotypes influences Dutch police officers’ stop-and-search behaviour, can be rejected based on the insignificant results. No significant differences between the conditions suggest that the video manipulation showing the racist stereotype did not make a difference in officers’ stop-and-search behaviour. Secondly, the study investigated the hypothesis that police officers’ level of stereotype threat explains the relationship between racist stereotypes and stop-and-search behaviour. No significant associations were found, which indicated stereotype threat does not explain the relationship between the racist stereotype and stop-and-search behaviour. Thirdly, the study aimed to understand whether or not the police officers’ level of user experience explains the relationship between racist stereotypes and stop-and-search behaviour. In this respect, no associations were found, so the hypothesis can be rejected. However, a correlation between user experience and self-legitimacy was found.

This study specifically focused on better understanding the impact of VR and deepfake technology. In this regard, it was found that contradiction within participants’ opinions and descriptions was of high importance. Many participants said they found

the VR very realistic but, at the same time, called it a simulation. Moreover, many simply described the environment as real, which might indicate immersion. It was also found that participants did not notice the deepfake technology, potentially making this technology viable for future research. While the deepfake could not be detected, the presence of the deepfaked ethnic minority was shown to be important. In the correlation analysis, a substantial negative correlation between deepfake and selecting person 1, the ethnic minority, was shown, while simultaneously deepfake and person 2 had a significant positive correlation. This might indicate an avoidance behaviour towards the ethnic minority person. The multinomial regression also reflected this tendency; however,  $p$ -values were insignificant.

### 5.8.1 *Participant behaviour*

The findings of the study indicate that confronting police officers with racist stereotypes did not have a significant effect on their stop-and-search behaviour. This contrasts with the initial theoretical expectation, which proposed that accusations of racism could become a self-fulfilling prophecy and influence enforcement actions (Trinkner et al., 2019). The stereotype threat theory, where individuals act in line with stereotypes about them, suggested that confronting officers with stereotypes would impact their behaviour. However, some researchers hold contrary opinions, suggesting that when stereotypes are overtly presented, individuals may exhibit stereotype reactance and purposefully act in opposition to the stereotype (Hakim et al., 2017).

Exploring potential reasons for the discrepancy, one explanation could be that the manipulation of showing the stereotype video was ineffective, supported by the non-significant results. This suggests that racist stereotypes may not be directly relevant to the outcome behaviour in this context. Another interpretation could be that police officers are constantly confronted with such stereotypes in their daily lives, rendering video manipulation less impactful as everyone experiences a similar level of exposure to racist stereotypes regardless of watching the video. This interpretation aligns with previous research highlighting the prevalence of stereotypes in officers' everyday experiences (ACLU, 2019). This might be explained by the theory of chronic stereotype threat, describing the long-term, continual experience of stereotype threat that people from stigmatised groups may encounter. Chronic stereotype threat is continuous and pervasive, affecting several elements of a person's life, in contrast to acute stereotype threat, which only happens in certain circumstances (Woodcock et al., 2012). Additionally, the limited number of participants in each condition could contribute to the lack of apparent significant differences. However, even though no effect was found, that does not mean that an effect does not exist. These results have theoretical implications, suggesting that it is not the immediate confrontation with stereotypes but

rather the recurring exposure in everyday life that may influence outcome behaviour (Hakim et al., 2017).

The discrepancy with the initial theoretical expectations may be attributed to ineffective video manipulation or the continuous exposure to stereotypes in officers' daily lives (Hakim et al., 2017). These results suggest the need to consider the cumulative impact of stereotype exposure and to refine experimental designs better to capture the influence of stereotype perception on behaviour. No mediations could be identified of stereotype threat or user experience between racist stereotypes and deepfake and stop-and-search behaviour. More concretely, the relevance of the potential mediators cannot be conclusively determined. The original theoretical framework continues to hold up as a possible basis for future research (Casad & Bryant, 2016). The rejection of the main relationship and the insignificance of the proposed mediators suggest that further investigation is needed to better understand the dynamics between racist stereotypes, stereotype threats and behaviour.

Unexpectedly, the study's results revealed a substantial negative correlation between encountering a deepfake version of the VR environment and choosing person 1, who represented an ethnic minority. Participants showed a reduced inclination to select person 1 in virtual stop-and-search situations when they encountered the deepfake portrayal. In contrast, there was a significant positive association between deepfake and person 2, indicating a tendency to avoid the ethnic minority individual and instead select the next best person. Other analyses also reflected this tendency, although with insignificant  $p$ -values.

Reflecting on the initial theoretical conflict between the notions of stereotypes leading to over-policing and under-policing, proposed by Trinkner et al. (2020), neither theory explained the observed findings. The tendency observed in this study might point toward an under-policing and avoidance approach by the police when interacting with ethnic minorities (McCarthy, 2021). However, this theory does not fully account for the subsequent increase in approaching other people instead of the minority individual. Considering new theoretical perspectives, stereotype reactance could explain why officers purposefully acted in opposition to the racist stereotypes by not selecting the ethnic minority (Hakim et al., 2017). However, no differences were found between conditions regarding exposure to the stereotype video, leaving the role of stereotypes in these findings unclear.

Another potential explanation for the findings could be the setting the study was conducted in. As this study was conducted within police stations in close proximity to subordinates and colleagues, it is possible that test subjects wanted to adhere to social norms of not appearing discriminatory. Similarly, this tendency could also apply to actual on-duty stop-and-search behaviour, where the social desirability of not being perceived as racist may lead to a disproportionate avoidance out of fear of being labelled as such (McCambridge et al., 2014).

However, it is essential to note that these findings only indicate a potential tendency and require further investigation. The small sample size, particularly in some conditions with only 20 participants, as highlighted by the insignificant  $p$ -values, limits the generalisability of the results. Given the topic's sensitive nature, practical implications for the future in this regard cannot be drawn solely from this study. Nevertheless, further investigation into the avoidance tendency would provide valuable insight that would be helpful in decreasing ethnic profiling within police forces.

Considering previous research, it seems unlikely that this tendency observed in the study would directly apply to on-street behaviour, considering the well-documented disproportionate representation of ethnic minorities in police stops (Leun & Woude, 2011). Nonetheless, the fear of being perceived as racist or discriminatory, whether leading to avoidance only in an observation setting or also in a natural work setting, needs to be further addressed. Ultimately, this fear not only hinders the police officers themselves by impeding open discourse and potentially influencing research results, but it also leads to impaired behaviour toward ethnic minorities, negatively impacting police-community relationships (Tracey, 2016).

#### 5.8.2 Reflection on VR and deepfake

The explorative thematic analysis of user experience highlighted the importance of the recurring contradicting and describing topics. On the side of contradicting, this indicated a partial immersion, given that participants simultaneously reported feeling immersed and indicated that they were reminded of reality. On the other hand, the code *Description* highlighted that some participants experienced a level of immersion by describing the simulation as if it was real.

Regarding the code *Contradiction*, technological mediation theory posits that technology mediates our experiences and interactions with the world. In this context, the analysis highlights the contradictory nature of participants' perceptions. On the one hand, they acknowledge the simulated nature of the technology, recognising it as a constructed representation. On the other hand, their experience of the technology evokes a strong sense of realism, blurring the boundaries between the virtual and the real. These findings align with prior theory highlighting the impact of technology on perception, suggesting that the technology bridges the gap between the user and the virtual environment, enabling a relatively high but often interrupted degree of embodiment (Feenberg, 2009). The participants' descriptions of the environment as if it were real indicate that they may have suspended their disbelief and fully embraced the simulated experience. According to mediation theory, this would indicate full embodiment (Verbeek, 2016).

Typically, when using technology as a medium, such as a laptop, to mediate between individuals and reality, people do not lose their sense of reality. However, with the

*MERET ASARA PAULULAT, BAS BÖING, VLAD NICULESCU-DINCA AND PETER W. DE VRIES*

emergence of new forms of mediation, such as VR, some individuals seem to disconnect from the real world and perceive VR as a fully detached simulation, separate from our present reality. This poses challenges when applying research findings from VR to the real world.

This disconnection is particularly evident in individuals displaying a pattern of contradiction, as they often refer to the VR environment as a simulation or a game, indicating a clear separation between the virtual world and reality. Conversely, individuals who describe the VR environment as if they were actually present demonstrate a high level of immersion and embodiment and intuitively connect the virtual world to our real world. This connection makes behavioural tendencies observed in the virtual environment more applicable to real-life contexts.

Now, looking back at the technological emphasis of this study, the deepfake technology could not be detected by the participants. The revolutionary combination of technologies becomes subject to many new exciting use cases. However, this also raises the question of whether or not current theory can account for the impact of such new technologies. As we saw in our study, the current forms of technological mediation might no longer account for these new technologies. The current mediation theories describe a mediation of the technology between the individual and the real world. However, the new advancement of deepfake in a VR setting might call for developing a new category in the mediation framework. Specifically, the technology might not mediate between the individual and the real world but between the individual and a simulation from which we still want to draw conclusions about the real world, whereby, while being a simulation, it still needs to be connected to the real world. Therefore, it is crucial to develop this idea of a new framework that further keeps up with new technological developments to account for the mediating effects of technology in future research and training.

In practical terms, when working with VR or other forms of virtual representation aimed at simulating reality, such as deepfakes, it might be essential to consider this new type of mediation to ensure that users maintain a strong connection between the virtual world and reality. This connection allows for full immersion and facilitates the application of findings and insights derived from virtual experiences to real-life situations. By acknowledging and preserving the fundamental laws and principles of the real world within the virtual environment, researchers can increase the transferability and relevance of their findings in practical contexts.

The broader implications for international policing practices necessitate the development of standardised methods for handling the effects of mediations when utilising advanced technologies, particularly in training scenarios. A uniform approach to assessing the strength and impact of these mediations is essential to align training with real-life practices accurately. This alignment ensures that law enforcement officers are better prepared for field operations, ultimately enhancing effectiveness and safety. Furthermore, it is crucial for research to establish unified methodologies

for incorporating new types of mediation, alongside a common lexicon to discuss and evaluate their effects comprehensively. Ethical considerations are paramount, especially regarding data protection and the potential misuse of technology. As these technologies become more prevalent, safeguarding personal information and preventing abuse must be prioritised. Additionally, detailed exploration of how these findings could shape future research directions and policy-making in law enforcement is necessary.

## 5.9 LIMITATIONS AND FUTURE DIRECTIONS

The VR environment used in the study did not provide participants with the option of not making a selection during the stop-and-search scenarios. The only option of not making the selection was taking off the glasses and finishing the experiment. This artificial constraint may have influenced participants' behaviour and decision-making, as they were tempted to choose one of the available options rather than having the freedom to refrain from selecting. This limitation could have affected the ecological validity of the VR scenarios.

Due to technical constraints, the person representing an ethnic minority in the VR environment, specifically the person on the scooter, had to be positioned closer to the participant due to technical limitations from the development of the VR environment that were out of our control. This discrepancy in proximity may have inadvertently influenced participants' selection biases and behaviours. The altered position of the deepfake character may have created an unintentional cue or bias that influenced participants' decisions, potentially compromising the validity of the findings. While this proximity difference is also typical in real-life policing scenarios, it might have had a different impact in an unfamiliar virtual reality setting. These restrictions underline the need for caution when analysing the study's findings.

Besides these limitations, this study brings forth new insights, opening up new avenues for further research. It underlines the need for more research on how stereotypes affect stop-and-search behaviour in police officers. Future research might build upon this study's findings by using a more nuanced approach in grouping individuals into conditions according to their perception of the prevalence and strength of the racist stereotypes they face. Participants who report a high perception of these stereotypes could replace those exposed to racist stereotype manipulation in previous experiments. By incorporating participants' subjective experiences, future research can better capture the influence of stereotype perception on behaviour. Furthermore, future studies should take a comprehensive stance to explore how fear, social desirability and chronic stereotype threat affect policing behaviour, specifically in the direction of avoidance.

On a theoretical level, there should be further investigation into the potential new kind of mediation. This study highlighted the need for new theoretical developments to

MERET ASARA PAULULAT, BAS BÖING, VLAD NICULESCU-DINCA AND PETER W. DE VRIES

keep up with VR and deepfake technology advancements. Furthermore, there needs to be more research on how these theoretical insights can be practically applied in future research and VR training programmes for police officers and beyond.

## 5.10 CONCLUSION

Overall, this study contributes to the understanding of the complex dynamics between racist stereotypes, police officers' behaviour, and the potential of VR and deepfakes as technologies for research and intervention. Perhaps most importantly, this study underscores the transformative potential of VR and deepfake technology in policing research and training programmes. At the same time, we emphasise the need to pay special attention to preserving the fidelity of the virtual-to-real-world connection as imperative for effectively harnessing these technologies' potential. This study paves the way for future research to address the challenges and advance knowledge in this critical area by highlighting the need for nuanced investigations, and pointing to a potential new type of technological mediation. Ultimately, the insights gained from this study can inform efforts to promote fair and unbiased policing practices and also support the improvement of future technology-based police training and research projects.

## ACKNOWLEDGEMENTS

We would like to thank all the police officers who took part in this study. We would also like to thank Tobias Siepenkort, who contributed to the success of this project with his Bachelor's thesis.

## REFERENCES

- ACLU (2019). *The Persistence Of Racial And Ethnic Profiling In The United States*. American Civil Liberties Union. <https://www.aclu.org/report/persistence-racial-and-ethnic-profiling-united-states>
- Banakou, D., Hanumanthu, P.D., & Slater, M. (2016). Virtual embodiment of white people in a black virtual body leads to a sustained reduction in their implicit racial bias. *Frontiers in Human Neuroscience*, 10. <https://doi.org/10.3389/fnhum.2016.00601>
- Barbot, B., & Kaufman, J.C. (2020). What makes immersive virtual reality the ultimate empathy machine? Discerning the underlying mechanisms of change. *Computers in Human Behavior*, 111, 106431. <https://doi.org/10.1016/j.chb.2020.106431>
- Binsch, O., Oudejans, N., Kuil, M., Landman, A., Smeets, M.M.J., Leers, M.P., & Smit, A. (2022). The effect of virtual reality simulation on police officers' performance and

- recovery from a real-life surveillance task. *Multimedia Tools and Applications*, 82(11), 17471-17492. <https://doi.org/10.1007/s11042-022-14110-5>
- Boehme, H.M., Cann, D., & Isom, D.A. (2020). Citizens' Perceptions of Over- and Under-Policing: A look at race, ethnicity, and community characteristics. *Crime & Delinquency*, 68(1), 123-154. <https://doi.org/10.1177/0011128720974309>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>
- Carney, N. (2016). All lives matter, but so does race: Black Lives Matter and the evolving role of social media. *Humanity & Society*, 40(2), 180-199. <https://doi.org/10.1177/0160597616643868>
- Casad, B.J., & Bryant, W.J. (2016). Addressing Stereotype Threat is Critical to Diversity and Inclusion in Organizational Psychology. *Frontiers in Psychology*, 7(8). <https://doi.org/10.3389/fpsyg.2016.00008>
- Cornet, L.J.M., & Van Gelder, J.-L. (2020). Virtual reality: a use case for criminal justice practice. *Psychology, Crime & Law*, 26(7), 631-647. <https://doi.org/10.1080/1068316x.2019.1708357>
- De Vries, P., Böing, B., Mulder, E., & van Gelder, J.-L. (2023). Sugarcoating a Bitter Pill – VR Against Police Ethnic Profiling. In A. Meschtscherjakov, C. Midden & J. Ham (Eds.), *Persuasive Technology: 18th International Conference, PERSUASIVE 2023, Eindhoven, The Netherlands, April 19-21, 2023, Proceedings* (pp. 22-35). Springer. [https://doi.org/10.1007/978-3-031-30933-5\\_2](https://doi.org/10.1007/978-3-031-30933-5_2).
- Encyclopaedia Britannica (2023, 17 December). *Technology | Definition, Examples, Types & Facts*. Encyclopaedia Britannica. <https://www.britannica.com/technology/technology>
- European Commission against Racism and Intolerance (ECRI) (2020). Homepage. <https://www.coe.int/en/web/european-commission-against-racism-and-intolerance>
- Europol (2023). *Netherlands, France and Estonia win the 2023 Europol Excellence Awards in Innovation*. Europol. <https://www.europol.europa.eu/media-press/newsroom/news/netherlands-france-and-estonia-win-2023-europol-excellence-awards-in-innovation>
- Fabri, G.V. [Godgiven]. (2020, 15 December). Etnisch Profileren Politie Rotterdam [Racial Profiling Dutch Police] [Video]. YouTube. <https://www.youtube.com/watch?v=F-G625PkXIE>.
- Feenberg, A. (2009). Peter-Paul Verbeek: Review of What Things Do. *Human Studies*, 32(2), 225-228. <https://doi.org/10.1007/s10746-009-9115-3>.
- Fox, J., Arena, D., & Bailenson, J.N. (2009). Virtual Reality. *Journal of Media Psychology*, 21(3), 95-113. <https://doi.org/10.1027/1864-1105.21.3.95>.
- Gauthier, J.F., & Graziano, L.M. (2018). News media consumption and attitudes about police: in search of theoretical orientation and advancement. *Journal of Crime and Justice*, 41(5), 504-520. <https://doi.org/10.1080/0735648x.2018.1472625>

- Giessing, L., & Frenkel, M.O. (2022). Virtuelle Realität als vielversprechende Ergänzung im polizeilichen Einsatztraining – Chancen, Grenzen und Implementationsmöglichkeiten. In M. Staller & S. Koerner (Eds.). *Handbuch polizeiliches Einsatztraining: Professionelles Konfliktmanagement – Theorie, Trainingskonzepte und Praxiserfahrungen* (pp. 677-692). Springer eBooks. [https://doi.org/10.1007/978-3-658-34158-9\\_36](https://doi.org/10.1007/978-3-658-34158-9_36)
- Hakim, C., Kurman, J., & Eshel, Y. (2017). Stereotype Threat and Stereotype Reactance: The Effect of Direct and Indirect Stereotype Manipulations on Performance of Palestinian Citizens of Israel on Achievement Tests. *Journal of Cross-Cultural Psychology*, 48(5), 667-681. <https://doi.org/10.1177/0022022117698040>
- Home Office (2022, 27 October). *Police powers and procedures: Stop and search and arrests, England and Wales, year ending 31 March 2022*. GOV.UK. <https://www.gov.uk/government/statistics/police-powers-and-procedures-stop-and-search-and-arrests-england-and-wales-year-ending-31-march-2022/police-powers-and-procedures-stop-and-search-and-arrests-england-and-wales-year-ending-31-march-2022>
- Ihde, D. (2009). *Postphenomenology and Technoscience: The Peking University Lectures*. <https://philpapers.org/archive/IHDPAT-2.pdf>
- Johnson, L.M., Devereux, P.G., & Wagner, K.D. (2022). The group-based law enforcement mistrust scale: psychometric properties of an adapted scale and implications for public health and harm reduction research. *Harm Reduction Journal*, 19(1), 60. <https://doi.org/10.1186/s12954-022-00635-3>
- Junger-Tas, J. (1997). Ethnic Minorities and Criminal Justice in the Netherlands. *Crime and Justice*, 21, 257-310. <https://www.jstor.org/stable/1147633>.
- Kietzmann, J., Lee, L.W., McCarthy, I.P., & Kietzmann, T.C. (2019). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135-146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Kleygrewe, L., Hutter, R.I.V., Koedijk, M., & Oudejans, R.R.D. (2023). Virtual reality training for police officers: a comparison of VR and real-life training responses. *Police Practice and Research*, 25(1), 18-37. <https://doi.org/10.1080/15614263.2023.2176307>.
- Kliem, V. (2019, 5 June). Virtual Reality: the next step in police training. *Force Science – Research | Training | Consulting*. <https://www.forcescience.com/2019/05/virtual-reality-the-next-step-in-police-training/>
- KombijdePolitie [@KombijdePolitie]. (2023, 13 March). Drugs, ontvoeringen, vermissingen – de spannendste zaken heb ik vooral meegemaakt in het bos [Video]. X. <https://twitter.com/KombijdePolitie/status/1635173854757949441>.
- Kray, L.J., Reb, J., Galinsky, A.D., & Thompson, L. (2004). Stereotype reactance at the bargaining table: The effect of stereotype activation and power on claiming and creating value. *Personality and Social Psychology Bulletin*, 30, 399-411. <https://doi.org/10.1177/0146167203261884>.
- Kyrre, J., & Crease, R.P. (2015). *Technoscience and Postphenomenology*. Lexington Books.
- Leun, J.P. van der, & Woude, M.A.H. van der (2011). Ethnic profiling in the Netherlands? A reflection on expanding preventive powers, ethnic profiling and a changing social

- and political context. *Policing and Society*, 21(4), 444-455. <https://doi.org/10.1080/10439463.2011.610194>
- McCambridge, J., Witton, J., & Elbourne, D.R. (2014). Systematic review of the Hawthorne effect: New concepts are needed to study research participation effects. *Journal of Clinical Epidemiology*, 67(3), 267-277. <https://doi.org/10.1016/j.jclinepi.2013.08.015>
- Mccarthy, M., Trinkner, R., & Atiba Goff, P. (2021). The Threat of Appearing Racist: Stereotype Threat and Support for Coercion Among Australian Police Officers. *Criminal Justice and Behavior*, 48(6), 009385482199351. <https://doi.org/10.1177/0093854821993513>
- Niculescu-Dinca, V. (2018). Towards a Sedimentology of Information Infrastructures: A Geological Approach for Understanding the City. *Philosophy & Technology*, 31(3), 455-472.
- Niculescu-Dinca, V. (2021). Theorizing Technologically Mediated Policing in Smart Cities: An Ethnographic Approach to Sensing Infrastructures in Security Practices. *Philosophy of Engineering and Technology*, 75-100. [https://doi.org/10.1007/978-3-030-52313-8\\_5](https://doi.org/10.1007/978-3-030-52313-8_5)
- Steele, C.M., & Aronson, J. (1995). Stereotype threat and the intellectual test performance of African Americans. *Journal of Personality and Social Psychology*, 69(5), 797-811. <https://doi.org/10.1037/0022-3514.69.5.797>
- Tracey, T.J.G. (2016). A note on socially desirable responding. *Journal of Counseling Psychology*, 63(2), 224-232. <https://doi.org/10.1037/cou0000135>
- Trinkner, R., Kerrison, E.M., & Goff, P.A. (2019). The force of fear: Police stereotype threat, self-legitimacy, and support for excessive force. *Law and Human Behavior*, 43(5), 421-435. <https://doi.org/10.1037/lhb0000339>
- Van Steden, R., Boutellier, H., Scholte, R.D., & Heijnen, M. (2012). Beyond Crime Statistics: The construction and application of a criminogenity monitor in Amsterdam. *European Journal on Criminal Policy and Research*, 19(1), 47-62. <https://doi.org/10.1007/s10610-012-9179-x>
- Verbeek, P.P. (2005). *What things do: Philosophical Reflections on Technology, Agency, and Design*. Penn State University Press.
- Verbeek, P.P. (2015). COVER STORY. Beyond interaction: a short introduction to mediation theory. *Interactions*, 22(3), 26-31.
- Verbeek, P.P. (2016). Toward a Theory of Technological Mediation: A Program for Postphenomenological Research. In J.K. Berg, O. Friis & R.C. Crease, *Technoscience and Postphenomenology: The Manhattan Papers* (pp. 189-204). Lexington Books.
- Witmer, B.G., & Singer, M.J. (1998). Measuring presence in virtual environments: a presence questionnaire. *Presence: Teleoperators & Virtual Environments*, 7(3), 225-240. <https://doi.org/10.1162/105474698565686>.
- Woodcock, A., Hernandez, P.R., Estrada, M., & Schultz, P.W. (2012). The consequences of chronic stereotype threat: Domain disidentification and abandonment. *Journal of Personality and Social Psychology*, 103(4), 635-646. <https://doi.org/10.1037/a0029120>



## 6 FROM CODE TO COURTROOM

### *The role of encryption in the Dutch criminal justice system*

Saskia Westers, Maike Berkenpas, Jurjen Jansen, Wendy Schreurs, Greg Alpar and Kimberly Bluhm

#### **Abstract**

*Encryption is the process of encoding information to prevent unauthorised access. Within the context of law enforcement and the justice system, encryption presents unique challenges and opportunities, which will be the focus of this chapter. Our results stem from a previous study that concentrated on the role of encryption in police investigations (Jansen et al., 2023). The findings were based on a literature review, interviews and a survey. We conducted an additional literature review regarding legislation to extend the scope of this chapter.*

*Existing legislation is not adequately equipped to handle the rapid evolution of encryption and other digital technologies. Unique challenges have prompted innovative solutions in police practice. For instance, police officers employ novel strategies to access encrypted data, such as obtaining access to Google accounts to retrieve backups of WhatsApp messages. Once data are decrypted, they not only yield potential broader intelligence, but are also considered trustworthy evidence because it seems unlikely that this data has been altered. Consequently, defence attorneys initiated an unprecedented international collaboration to establish the unlawfulness of data collection methods, as evidenced by cases involving EncroChat evidence. Moreover, to expedite legal proceedings, procedural agreements are increasingly used when addressing the admissibility of evidence.*

*The evolving digitalisation of crime has led to the introduction of the Dutch Innovation Criminal Procedure Act, which is a pilot aimed at modernising the Code of Criminal Procedure. This legislation needs to align with the challenges posed by encryption. Additionally, the judiciary and the public prosecution service should be well equipped with the knowledge and expertise necessary to effectively navigate the complexities of encryption. Our findings aim to inform the public debate on the evolving role of encryption in the legal landscape.*

#### **6.1 INTRODUCTION**

This study is about encryption, which can be defined as the process of encoding information to prevent unauthorised access. Encryption is increasingly prevalent in all forms of crime and, consequently, in criminal investigations. Two factors contribute to this trend. Firstly, encryption is commonly integrated into software and hardware

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

and is therefore easily accessible to criminals. Secondly, the ability to conceal relevant information and communications significantly facilitates criminal activity. As a result, law enforcement agencies (LEAs) encounter encryption more frequently in criminal investigations. Previous research has highlighted the prominent role of encryption in criminal investigations (Jansen et al., 2023).

Building upon that previous study, this chapter shifts its focus to the role of encryption in Dutch criminal cases following investigations. Specifically, we examine the role of encryption within the context of law enforcement and the justice system, considering its unique challenges and opportunities. To shed light on this role, we address the following main research question: what is the role of encryption in criminal cases? This question can be broken down into three sub-questions: (1) What is the nature of encryption in criminal cases? (2) What is the role of encryption in evidence gathering in criminal cases? (3) What is the role of encryption in the criminal prosecution and judicial resolution of these cases? Our findings aim to contribute to the public debate about the evolving role of encryption in the legal landscape.

The next section outlines the methods used. Thereafter, we discuss the presence and types of encryption used in criminal cases, followed by the role of encryption in gathering evidence in criminal cases. We then dwell on the role of encryption in the prosecution of criminal cases through the Public Prosecution Service and judiciary. The chapter ends with a discussion and conclusion.

## 6.2 METHODS

In this section, we describe the methods. First of all, we re-examined the data that were collected in the study by Jansen et al. (2023). In particular, this involved an online survey amongst police officers ( $n=177$ ) and interviews with police officers, the Public Prosecution Service, judges and other experts ( $n=27$ ). These data were gathered in 2021 and 2022. More details on these methods can be found in Jansen et al. (2023). Note that the statements of respondents recorded in the results section have been translated from Dutch to English.

For this chapter, an additional literature review regarding legislation and an additional descriptive analysis of judicial decisions were carried out. Databases such as Science Direct, Google Scholar and the digital library of NHL Stenden University of Applied Sciences were used for the additional literature review. We employed search terms specifically targeting encryption in criminal cases. These terms included synonyms and acronyms in Dutch and English related to concepts such as encrypt\*, criminal cases, innovation law and process rights. Additionally, when identifying relevant articles, we utilised their bibliographies and Google Scholar to uncover more related and recent articles (using the snowball method). This method is used for answering sub-questions 2 and 3.

Published judicial outcomes in the Netherlands were used to illustrate the presence of various forms of encryption in criminal cases. This method was employed for answering sub-question 1. We retrieved data from the website of the Dutch judiciary (rechtspraak.nl), which offers access to a selection of judicial decisions. Less than 5% of the approximately 1.5 million verdicts issued annually are published (NOS, 2021). The selection of cases for publication depends on factors such as case significance, legal domains and the desirability of publication. Typically, important rulings from the Supreme Court (the highest judicial authority in the Netherlands) and judgments concerning the most serious crimes are included.

This database was used to explore the presence of different forms of encryption in judicial rulings in more serious crimes. We collected data on the number of cases involving different types of encryption over the past eight years (2016-2023). Similar encryption types were considered in our previous study (Jansen et al., 2023). It is important to note that a significant number of cases are excluded from this database, which may affect the accuracy of determining the prevalence of encryption-related cases and potentially compromise the generalisability of our results. Hence, we merely investigate this data source to observe trends rather than to make statements about prevalence.

## 6.3 RESULTS

### 6.3.1 *What is the nature of encryption in criminal cases?*

To provide meaningful insights into the role of encryption in criminal cases, it is essential to understand the presence and types of encryption used in such cases. First, different categories of encryption are defined. Second, we explore the presence of encryption in criminal cases by using interviews and data from judicial rulings in more serious crimes.

#### 6.3.1.1 *Types of encryption*

Consistent with the earlier study (Jansen et al., 2023), we used four categories of encryption: (1) encrypted communication; (2) encrypted devices and data; (3) encrypted online services; and (4) technologies to conceal digital locations. While the first three types encrypt communication content and files, the fourth type hides network locations. The user's device initiates encryption in all but encrypted online services, where the provider handles it. Finally, the first two types differ in which part of the user's device performs the encryption. Although technically this distinction refers to encryption strategies rather than actual types of encryption, we use the term 'types of encryption' to align with practical usage in real-world, investigative contexts. We elaborate further on these below.

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

*Encrypted communication.* This category includes services such as cryptophone providers and end-to-end encryption (E2EE)<sup>1</sup> from platforms such as WhatsApp, Telegram and ProtonMail. Cryptophone providers, such as Ennetcom, EncroChat and Sky ECC, ensure anonymity by eliminating publicly used messaging applications (e.g. WhatsApp) and external communication components such as the microphone, camera and GPS antenna. Additionally, cryptophone providers frequently include an option to easily erase all data from the device. In publicly used messaging applications, such as encrypting messages, video and audio calls on Meta's WhatsApp and Facebook Messenger, and Signal, the Signal Protocol, a well-studied cryptographic system, is utilised. Email services employ multiple layers of encryption, with the globally adopted standard being OpenPGP. A prominent encrypted email service with millions of users is ProtonMail, which employs E2EE and stores encrypted data on private physical servers for enhanced security. To ensure security, various encryption methods are combined, including AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) and, now increasingly, post-quantum cryptography. Devices, providers' apps and services that provide encrypted communication include cryptophone providers, Sky ECC, Ennetcom, EncroChat, ProtonMail, WhatsApp, Telegram, Facebook Messenger, Snapchat and Signal.

*Encrypted devices and data.* This category includes encrypted smartphones and hard or solid-state drives. Encrypted mobile phones (controlling access with a PIN code, facial recognition or fingerprint) and other devices, such as laptops and desktop computers, make use of encrypted data storage. Other relevant encrypted storage technologies include encrypted data carriers such as USB sticks and hard drives, and volume encryption software, such as VeraCrypt, BitLocker and FileVault.

*Encrypted online services.* Encrypted online services refer to social media accounts, encrypted cloud storage and bulletproof hosting, in which access is often restricted by password protection. Oerlemans (2019) defines a bulletproof hosting service as a company that rents server space to clients, enabling them to intentionally host various types of content, including illegal material. The term bulletproof refers to the perceived protection that these services offer against LEAs and other parties attempting to take the material offline.

*Technologies to conceal digital locations.* Anonymising technologies are offered to users to enhance anonymity by enabling them to browse the web without revealing their identity or location. Through a VPN (virtual private network), one or more devices, such as servers, computers and phones, can connect to a private network over the internet. Within this network, data can be transmitted without interception or

---

1 End-to-end encryption (E2EE) ensures secure communication channels where only the intended recipient can access the data, with service providers unable to read the information. Popular applications such as WhatsApp, Signal and Telegram employ E2EE, making interception difficult for enforcement agencies.

traceability. Another service, the so-called dark web (also known as the darknet), is a restricted part of the internet inaccessible via traditional servers and search engines. All communication on this part of the internet is encrypted. Accessing the dark web anonymously requires a special browser. For instance, a Tor browser can access a part of the dark web. While these technologies conceal IP addresses in various ways, they do not necessarily guarantee user anonymity. For instance, using one's real name on a 'dark market' exposes their identity to all visitors. VPN and Tor are technologies that make it possible to setup a secure, encrypted connection with a service provider (VPN server or Tor endpoint) via which parts of the (public) web can be accessed. In this way, both encryption and location hiding can be achieved simultaneously.

### 6.3.1.2 *Presence of encryption in criminal cases*

Interviews with judges and examining magistrates (EMs) ( $n=5$ ) and a public prosecutor indicate that encryption is increasingly present in criminal cases. One judge says that five years ago, cases involving encryption were rare, and they expect many cases involving encryption will follow. One EM states that the presence has multiplied, referring not to standard encryption as in WhatsApp, but to technologies designed primarily to apply encryption, such as Sky ECC, EncroChat and their successors. More specifically, they encounter encryption in criminal cases in the form of not only widely used smartphones (locked by a PIN code or facial recognition), encrypted messaging services, cloud storage, Signal, Telegram and WhatsApp, but also cryptophones, the dark web (child sexual abuse material (CSAM)), BitLocker and Tor (illegal dark web marketplaces). ProtonMail is also observed in cases, particularly related to drug trafficking, weapon offences, sexual offences and terrorism suspicion, but to a lesser extent. Bulletproof hosting is less frequently observed in cases, occurring, for example, in matters involving the provision of criminal services and the storage of files containing stolen credit card data.

Furthermore, to delve deeper into the observed upward trend of encryption in criminal cases, we mapped out the 'prevalence' of encryption applications within Dutch criminal cases involving serious crimes. Table 6.1 provides an extended overview of encryption applications referenced in judicial decisions spanning the years 2016 to 2023. Encrypted forms of communication, specifically WhatsApp, are particularly notable. Other encrypted messaging services, such as Snapchat, Telegram, Facebook Messenger and Signal, have been cited hundreds of times in court rulings in recent years. Furthermore, smartphones, which are often encrypted devices, are increasingly common in judicial rulings.

Cryptophone providers such as EncroChat, Sky ECC, Ennetcom and PGP Safe appear to be increasingly featured in criminal cases as well. This can be explained by the fact that Ennetcom was shut down in 2016 and PGP Safe in 2017. EncroChat was infiltrated, and Sky ECC was taken down in 2021. Since then, decrypted messages from these services have been used in criminal investigations (Jansen et al., 2023) as well as

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

in criminal cases (Table 6.1). Although the findings in Table 6.1 are based on a relatively small percentage of court cases, it seems to back the trend of an increasing presence of encryption, similar to the trend described by the interviewee's perspective.

**Table 6.1** Number of legal judgments including a type of encryption (rechtspraak.nl)

Application of encryption	2016	2017	2018	2019	2020	2021	2022	2023	Total
<i>Encrypted communication</i>									
WhatsApp	374	588	778	845	1193	1608	1675	1953	9014
Snapchat	5	20	39	56	108	168	262	326	984
Telegram	23	54	47	60	151	151	198	246	930
EncroChat	0	0	0	2	15	106	204	214	541
Facebook Messenger	15	28	52	60	79	92	58	83	467
Sky ECC	0	0	0	0	6	29	114	206	355
Signal	13	18	15	17	18	37	76	128	322
Ennetcom	6	0	9	11	8	38	81	60	213
Cryptophone	0	1	1	14	9	35	37	60	157
PGP Safe	1	0	2	7	5	15	56	15	101
ProtonMail	0	0	1	1	5	2	7	5	21
<i>Encrypted devices and data</i>									
Smartphone	67	102	119	136	100	132	135	175	966
VeraCrypt	0	0	0	1	1	0	1	1	4
FileVault	0	0	1	0	1	0	0	0	2
BitLocker	0	0	0	1	0	0	0	0	1
<i>Encrypted online services</i>									
Encrypted cloud storage	2	4	7	3	5	6	9	11	47
Bulletproof hosting	0	0	1	2	1	0	0	0	4
<i>Technologies to conceal digital locations</i>									
Tor (The Onion Router)	12	17	29	18	20	26	30	35	187
VPN (virtual private network)	4	5	12	13	21	12	14	19	100

### 6.3.2 What is the role of encryption in evidence gathering in criminal cases?

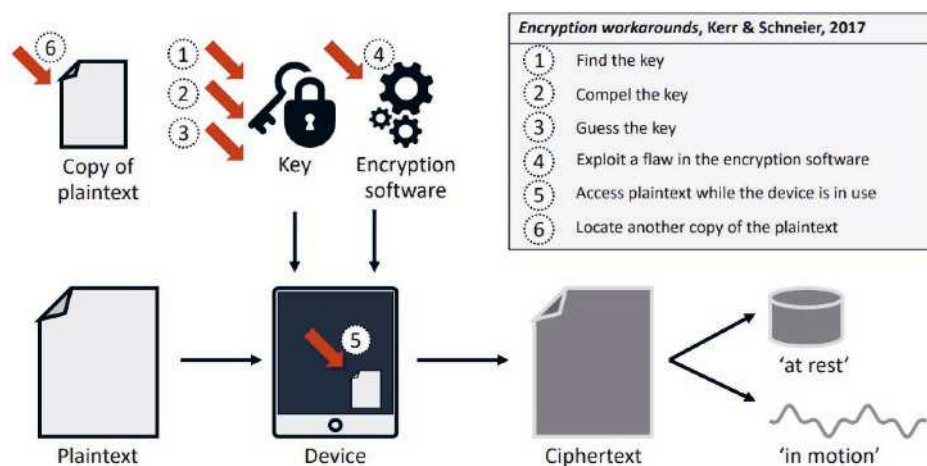
Investigative authorities have various ways to deal with encryption in criminal investigations. We explore several investigative methods and focus on unique challenges and opportunities in gathering and use of (previously) encrypted data for evidence.

### 6.3.2.1 Obtaining decrypted data

In our prior study (Jansen et al., 2023), we asked law enforcement officers (LEOs) in a survey ( $n=177$ ) about the strategies they use for accessing encrypted data during investigations. In this section, we delve into these investigative approaches in greater detail.

According to over half of the surveyed LEOs, the following strategies are often or always used to decrypt data: (1) outsourcing to another department or party; (2) technically cracking data; (3) bypassing encryption; and (4) employing alternative investigative means. *Outsourcing data decryption* involved requesting assistance from police departments or the Netherlands Forensic Institute (NFI). *Technical data cracking* can be achieved through methods such as internet tapping or phone tapping and brute force, where a program systematically tries passwords and encryption keys. Both the police and the NFI employ brute force. Brute forcing requires significant capacity, which is scarce. Therefore, efforts are typically initiated by first trying to *bypass encryption*. For instance, the police may search for insufficient key management among suspects or attempt to guess a key. See Figure 6.1 for more strategies to bypass encryption. *Alternative investigative means* include interrogation or observation of a suspect, as well as house searches.

**Figure 6.1** Different strategies to bypass encryption (based on Kerr & Schneier, 2017)



Less frequently used methods, according to the respondents, include (5) apprehension with open devices and (6) voluntary cooperation from suspects, for example by surrendering a key. By arresting a suspect with devices that are not encrypted (referred to as 'open'), encryption is bypassed, granting investigative authorities direct access to the data on the digital devices. Such an arrest requires preparation and is time-sensitive,

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

as it is essential that the suspect does not lock the accounts or devices during the brief time of arrest, making the encrypted data inaccessible to LEOs. Interviewees indicate that a network search (section 125j Dutch Code of Criminal Procedure (CCP)) can be utilised to determine when the suspect is active online to make a timely arrest. The voluntary cooperation of suspects is anchored in section 32(b) of the Cybercrime Convention.

In the survey, the least-mentioned ways to obtain decrypted data are by applying the so-called hacking power (*'hackbevoegdheid'* in Dutch; sections 126nba, 126uba and 126zpa CCP) and the decryption order (*'decryptiebevel'* in Dutch; section 126nh, para. 1 CCP). These powers are rarely used as they are only permitted under strict conditions. Hacking power is the last resort to gain access to encrypted data and takes place at an earlier stage in the investigative process when the suspect is actively using their encrypted system. Only the Digital Intrusion Team (DIGIT) of the Dutch police has the authority to hack a system. This team was established in 2019 after the Computer Crime III Act was introduced. This law gave hacking power a basis in the Code of Criminal Procedure (Van Uden & Van den Eeden, 2022).

The decryption order enables authorities to compel assistance in granting access to encrypted data. Assistance may be compelled from any person 'who can reasonably be suspected of having knowledge of the method of encryption' (section 126nh CCP), but not the suspect because they have the right to remain silent. Nevertheless, a Dutch judge ruled that the forced provision of a suspects' fingerprint to unlock a smartphone is permissible, provided it is proportional and subsidiary (ECLI:NL:RBNHO:2019:1568). Interviewed prosecutors indicate that this is not in conflict with the principle of *nemo tenetur*. One of them explains:

The CCP has long had the provision that you must also cooperate in shaving your hair, participating in photo lineup, and providing fingerprints and DNA under certain circumstances, and this is one of them.

Moreover, this decryption order applies to others besides suspects, such as system administrators (section 125kv CCP). The obligation to decrypt applies only to the extent that the addressee can do so (Oerlemans, 2020).

An additional investigative strategy is to make legal assistance requests for data from providers, amongst other parties (section 126ng CCP). National legal frameworks often differ between countries, within and outside the EU, which can create an obstacle for the investigation process and the possible collection of potentially relevant data. As a result of E2EE, providers can often only provide metadata. Metadata is information about items, files and other data. Metadata can describe items and include data about the creation and continuation of an item, which can be useful for LEAs. Interviewees mention that these data requests can take a lot of time, sometimes up to two years, which leads to delays in criminal investigations. Moreover, US authorities set high

standards for legal assistance requests. There must be probable cause and a case that warrants it (more serious crimes). An EM is required to give permission for a legal assistance request. Based on the prior study (Jansen et al., 2023), it is foreseeable that legal assistance requests may not lead to any result, or not within a reasonable time-frame. Consequently, in some cases LEAs have tried to find creative ways to bypass encryption, in which they sometimes succeed and other times they do not. In court ruling ECLI:NL:RBDHA:2021:8421, the prosecution requested a new SIM card to gain access to a victim's WhatsApp conversations. The victim's phone has never been recovered and the idea was that the victim had two other phones, which were not active recently and did not contain WhatsApp data. LEAs wanted to reset the password of the Google account to gain access to the WhatsApp backup that might be in the Google account. This request was rejected by the EM, because the case was similar to the hacking power – which may only be used on a suspect and not a victim – and the request was also not well founded.

In another cited case (ECLI:NL:RBDHA:2022:4288), the same method was allowed, as the victim in this investigation had passed away. The prosecution asked to gain access to the suspect's Google account to get into the WhatsApp backup. This request was based on section 181 juncto 177 CCP with the application of section 126ng. An EM ruled that this indirect method of providing access was not a circumvention of the hacking power (section 126nba CCP). In this case permission was granted to secure messages that were received up to 11 days after the confiscation of digital devices (section 181, para. 3 CCP). These cases exemplify that our current legal code needs adjustments because of the digitisation of crime, which is the main goal of the Innovation Act.

### **6.3.2.2 *Role of encryption in how an investigation proceeds of an investigation***

Encryption can have both a negative and positive role in how an investigation proceeds. A negative aspect is the increasing use of encryption, anonymisation techniques and the dark web. This makes it more difficult for investigative agencies to find information about a suspect's physical location or criminal infrastructure, or to collect digital evidence (Europol & Eurojust Public Information, 2018). Interviewees mention that it is disadvantageous when encryption cannot be cracked or bypassed. Consequently, the likelihood of a successful prosecution or conviction by the Public Prosecution Service (PPS) diminishes.

After data are decrypted, this generally contributes positively to successful prosecution. Several interviewees note that a beneficial aspect of this process is the false sense of security encryption gives criminals who use it for illegitimate practices. Because criminals believe they are protected by encryption, they tend to communicate more openly than they would without encryption (Driessen, 2021). Successfully decrypting messaging services such as EncroChat and Sky ECC has changed the so-called intelligence image of criminal investigations in a positive sense, because investigators have a more complete picture of (international) networks and collaborations. This

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

creates a wealth of data and therefore opportunities for detection. The question is to what extent such successes can be repeated in the future, as it is known that the police have gained access to such crypto services. One interviewee noted that:

No one trusts their criminal cryptophone anymore because the police have successfully targeted the provider several times with a wealth of information. Criminals learn from that. Now they divide communication across multiple systems and obscure communication.

The former head of the Dutch police investigation unit, Andy Kaag, emphasises that encryption and specifically cryptophones are indispensable in the criminal underworld, even after several hacks (Driessen & Meeus, 2021). He says: ‘as long as they operate worldwide, they will have to communicate’, describing the criminals’ need for encrypted communication as an Achilles’ heel. In 2023, after several hacks of encrypted messaging services, Dutch law enforcement took down another crypto communication service provider, Exclu (Openbaar Ministerie, 2023a). Andy Kaag stated: ‘for us this will be business as usual’ (Laumans & Vugts, 2023). Groothoff and Jansen (2022) cite two exemplary cases where decrypted crypto communication played a significant role, which are the convictions of Noffel F. (Rb. Amsterdam 19 April 2018, ECLI:NL:RBAMS:2018:2504) and Omar L. (Rb. Gelderland 26 June 2019, ECLI:NL:RBGEL:2019:2830) for organising liquidation(s) and organised crime. As the suspects and their co-defendants (wrongly) relied on the encryption of their messages, the sequence of events surrounding the liquidations could be reconstructed minute by minute (Groothoff, 2023). These cases illustrate the immense value that this type of evidence can have in combating serious crime.

A disadvantage of gaining access to a large amount of previously encrypted data is its labour-intensive nature: ‘it consumes quite a bit of capacity throughout the entire (criminal justice) chain’. It requires time and capacity to both gain access to encrypted data and analyse all the potentially relevant decrypted data. An interviewed police officer stated: ‘We used to look for a needle in a haystack and now we have a haystack of needles’. This highlights a transition from seeking evidence for individual cases to having an abundance of evidence for various criminal offences. Another interviewee stated: ‘While it’s beneficial to access a wealth of data by decrypting encrypted data, it is unfortunate that there is insufficient tactical capacity to effectively follow up on this.’

### 6.3.3 *What is the role of encryption in the criminal prosecution and judicial resolution of these cases?*

As mentioned earlier, encryption seems to be increasingly prevalent in criminal investigations and cases. In this section, we examine its function in criminal prosecution,

exploring perspectives from both the prosecution and defence. Subsequently, we analyse the role of encryption in the judicial resolution of cases.

### 6.3.3.1 *Criminal prosecution*

There is a lack of adequate overview of the duration of proceedings in criminal cases where encryption is involved. Interviews with judges and EMs mainly pointed out that encryption slows down the judicial process. Encryption appears to delay the progression of cases when access to encrypted data is not yet available. One prosecutor stated in an interview regarding encryption in investigation:

Does that lead to people being acquitted because we do not have access? Yes, it does. Does it mean that we could have prosecuted and convicted those individuals if we had access? We cannot say because we don't know if there was evidence.

One of the judges mentioned that all major criminal cases based on decrypted data from cryptophones have become 'sluggish'. In all of the interviews with judges, it was stated that delays are mainly due to the legality discussion, which is primarily focused on the right to a fair trial. Some interviewees mention that once the legality discussion is cleared up, evidence from decrypted devices can expedite processing times. While another interviewed judge claims that even when clear legal frameworks exist regarding the legality of this evidence, encryption still causes delays in the criminal justice chain (Jansen et al., 2023). One interviewee noted that 'encryption does not make it more difficult or easier; we have always had discussions about illegitimacy. The only difference is that there are a lot of data.'

The legality discussion is particularly relevant in the context of cryptophones. In criminal cases where cryptophone data are used as evidence, interviews with judges (Jansen et al., 2023) reveal that lawyers, especially in cases involving EncroChat and Sky ECC data, collaborate internationally to prove that collecting the data from these cryptophones was unlawful. These lawyers maintain contact and share plea notes and documents. In a case involving 10 suspects, one lawyer presented a plea on the legality of EncroChat evidence on behalf of all attorneys, according to one of the judges interviewed.

In 2022, over a hundred criminal defence lawyers voiced concerns about new criminal investigation methods in an urgent appeal (NOS, 2022). They allege that the PPS lacks transparency in its approach to seizing, wiretapping and hacking encrypted communication services. Given the increasing number of seized servers and compromised communication services in the Netherlands, legal scholars continue to emphasise the importance of defence access and insight when dealing with digital evidence originating from extensive datasets (Boeser, 2021). This consideration becomes particularly crucial in the context of modernising criminal procedures.

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

The defence particularly seeks to effectively exercise its right to defend within the framework of data-driven investigations and access to large datasets (e.g. EncroChat). Galič (2021) argues that the rise of extensive datasets in criminal cases complicates the position of the defence. She asserts that the defence has a legitimate interest in accessing both the complete and secondary datasets collected in a criminal case to extract relevant information. The complete dataset includes all data collected in a particular case and the secondary dataset is the result of initial searches conducted by the PPS on the complete dataset. Galič illustrates the difference between these datasets using the Ennetcom-Tandem case. The complete dataset contained 3.5 million data points from 19,000 individuals, seized from the Ennetcom server. The PPS performed three searches within this dataset using specific search terms such as names of suspects, email addresses and PIN numbers. These searches resulted in the secondary dataset (Tandem dataset), which the PPS could then freely search to find evidence for the case. A smaller selection from the secondary dataset was used as evidence in the case, which is the so-called tertiary dataset. She argues that the defence generally has no access to the complete or secondary dataset and must have the opportunity to independently search for exculpatory evidence. She also suggests that the defence should at least have the opportunity to be involved in determining the search terms used to explore a dataset.

Martijn Egberts, a Dutch public prosecutor and an expert in digital investigation, explains that when digital evidence is gathered, it is common to secure information that does not directly involve the suspect but pertains to others, including entirely irrelevant data (Egberts, 2022). For instance, this could include personal data such as intimate photos of victims. In such cases, granting unlimited and unregulated access to the suspect and their lawyer is not immediately apparent. Moreover, in criminal cases involving data from crypto services such as EncroChat, it is evident beforehand that the vast majority of the complete dataset is entirely irrelevant to the suspects in specific cases. This is because these clients or suspects often have no connection whatsoever and may not even come from the same country or speak the same language. Egberts adds that in the *Tandem II* case (ECLI:NL:RBAMS:2018:2504), an investigative team submitted a request to an EM to investigate Ennetcom data. Such a request must be well substantiated. In this case, email addresses were known, and various devices were seized. After obtaining permission, a subset was generated based on the criteria deemed relevant by the EM. Egberts refers to this subset as the secondary subset, in line with Galič's description. Consequently, the investigators and prosecutors of *Tandem II* did not have access to the entire primary dataset from Ennetcom. Thus, by requesting access to the primary and secondary dataset, the defence aimed to gain greater access to the Ennetcom data than the PPS and the court.

The European Court of Human Rights (ECtHR) equates insufficiently justified requests for access to the complete primary dataset with a 'fishing expedition' (ECLI:CE:ECHR:2019:0604JUD003975715, in Egberts, 2022). Moreover, the ECtHR asserts that the defence should generally have access to the secondary dataset. Indirect

access, where the defence provides search terms, is also recognised as a possibility for conducting a search for potentially exculpatory evidence. Outcomes of data can be influenced by entering a combination of search terms into the database. For the reliability of evidence, it is essential that the evidence is verifiable and reproducible, according to one of the judges interviewed. The assessment of the value of the evidence involves understanding how certain results in the case file are presented as incriminating. The evaluation of the evidence depends on the justification provided in the case file.

Therefore, additional conditions have been established for searching EncroChat data (26Lemont investigation). According to Article 126dd CCP, the public prosecutor is allowed to share information with a colleague after a review by the EM. The EM then assesses whether the authority to intercept telecommunications could have been deployed and whether there is manipulative searching. All discovered data must be stored in a way that allows for reproduction and verification.

Another point Galič (2021) raises is that the value of digital evidence depends on the reliability of the technological tools used and the defence's ability to authenticate them. She proposes a critical examination of the reliability of digital evidence produced by advanced search engines, such as Hansken, and advocates for enabling the defence to adequately assess it. Hansken is an advanced forensic search engine built by the NFI to search, manage and analyse large datasets.

A thorough examination of the defence's ability to oversee the filtering of information from Ennetcom data in the *Tandem II* case (ECLI:NL:RBAMS:2018:2504) took place in 2018, which was the first time this was performed. During this case, the defence was allowed to visit the NFI twice to utilise Hansken, providing an opportunity for counter-expertise by searching and possibly finding exculpatory evidence within the Tandem dataset. However, based on the verdict, it is apparent that the defence concentrated on assessing the functionality of the search engine Hansken itself, and the reliability of the search outcomes and overall forensic reliability, instead of searching for and possibly finding exculpatory material in the dataset (Egberts, 2022). Egberts emphasises that the opportunity to visit the NFI and use Hansken has also been offered to the defence in other criminal cases. However, this opportunity for further searches and to familiarise themselves with the secondary dataset has not been widely utilised in practice.

Since 2023, defence attorneys have been granted remote access to specific subsets of Hansken (Openbaar Ministerie, 2023b). They can only access Hansken data that are relevant to their case, and the data cannot be downloaded or copied. Additionally, any search terms used by the defence are not logged, ensuring the confidentiality of attorney-client communications.

Our previous study concluded that decrypted data is highly valued by study participants (Jansen et al., 2023). It is generally seen as more reliable than witness statements. According to interviewees, this information is less likely to have been altered by third parties. The open communication of suspects – who feel safe behind encryption – is valuable. Interviewees further assert that decryption aids in forming

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

a more comprehensive understanding of criminal collaborations, surpassing the fragmented insights available prior to or without decrypted data. Additionally, upon accessing encrypted data during the decryption phase, investigators potentially gain access to a wealth of information beneficial to the investigation.

Sunde (2022) delves into the reliability of digital evidence, emphasising that it is often mistakenly viewed as a credible and value-neutral representation of the truth. This misconception, known as the techno-fallacy, assumes that technology is neutral and that ‘facts’ speak for themselves. However, when digital evidence is assumed to be value-neutral, objective and a credible factual representation of the truth, it might be falsely assumed that digital evidence is free from technical and human error. Consequently, there may be insufficient scrutiny and quality control. Sunde illustrates the interpretative flexibility of digital traces and, therefore, the *evidence elasticity* of digital proof as knowledge. Elasticity means ‘the level of ambiguity associated with a piece of information, which leaves room for subjective interpretations’. The human factor greatly influences the construction of digital evidence. She stresses the importance of having a more comprehensive understanding of the potential limitations and misleading aspects of digital evidence.

Another concern arising from the analysis of large datasets (including decrypting crypto communication services) is the assurance of confidentiality between client and lawyers (Boeser, 2021). With the interception of hundreds of millions of encrypted messages from users of encrypted networks, maintaining confidentiality is challenging when using cryptophones. Often, it is not evident that a lawyer is participating in the communication. In cases involving Ennetcom data, this has resulted in the exclusion of evidence (ECLI:NL:RBAMS:2018:2504). The Netherlands Bar Association has warned lawyers about the use of cryptophones and advised them to make extensive use of confidential phone numbers (Nederlandse Orde van Advocaten, 2021).

To date, the utilisation of datasets from cryptophones and online messaging services in criminal cases has been deemed lawful. In 2023, questions regarding the legality of EncroChat and Sky ECC evidence were presented to the Dutch Supreme Court. The Supreme Court responded by affirming that the principle of trust between states applies (ECLI:NL:HR:2023:913). This implies that in Dutch criminal cases, the judge must adhere to the decision made by foreign authorities who conducted investigations abroad. Therefore, it is presumed that these foreign authorities conducted their investigation lawfully. The Dutch judge is obliged to scrutinise the reliability of the results only if specific indications suggest otherwise (ECLI:NL:HR:2023:913). The legality of obtaining decrypted data is further supported by jurisprudence, such as *Flamenco* (EncroChat), *Sartell* (PGPSafe and EncroChat) and *Ennetcom*. It is important to note that the aforementioned parties may have employed the strategy of ‘jurisdiction shopping’, which refers to the practice of selecting the jurisdiction that will have the most favourable outcome for their position.

Neither from the case law of the ECtHR nor from national case law can it be inferred that the ‘equality of arms’ (Article 6. European Convention on Human Rights (ECHR)) means that the defence must also have access to the same software or search engines as those used by police (Egberts, 2022). The principle of ‘equality of arms’ refers to the notion that both the prosecution and the defence should have equal access to and ability to analyse (digital) evidence and data. This ensures a fair and balanced legal process where both sides have the necessary resources to present their case effectively. Egberts concludes that the rights of the defence ‘to acquaint himself, for the purposes of preparing his defence, with the results of investigations carried out throughout the proceedings’ are not unlimited and differ from the possibilities available to the police, as the roles of the parties differ (ECLI:CE:ECHR:2009:0331JUD002102204, pp. 42-43, in Egberts, 2022).

### 6.3.3.2 *Judicial role*

According to interviewees, the role of the judiciary in cases involving encryption is not necessarily more or less difficult compared to cases without encryption. They explain that the judiciary must examine whether the case file is reliable and balanced and whether fundamental rights, such as Article 6 ECHR (equality of arms), have (not) been violated. Moreover, the judiciary’s role is to determine whether the subject is guilty or not. An EM assesses whether the (digital) investigation has been conducted in accordance with the law.

Interviewed judges and EMs note that the presence of encryption in cases is not unique to their work, except the sheer amount of data. This can lead to capacity issues. When there is a lot of information available, for example in cases involving Sky ECC data, the process is prolonged due to legality defences and procedural decisions. Another interviewee indicates that there is insufficient capacity to properly conclude all cases within the police, judiciary and court system. The shortage of judges, in particular, is confirmed by a parliamentary letter dated 27 June 2023 (House of Representatives, document no. 29279-799, 2023). The causes of the capacity shortage are multiple, including the increasing complexity of cases and legislation, the guidance of judges and trainee judges, and primarily the growing outflow of judges due to retirement since 2017.

One EM stated that the judiciary requires individuals with basic technical knowledge. The use of encryption in criminal cases raises questions such as: ‘Is the data accurate and unaltered (by the decryption process)?’ and ‘Can the public prosecutor prove that received data is unaltered?’. For judges it is impossible to keep up with the latest developments in all forensic areas of expertise, nor can they sufficiently reduce or close the knowledge gap themselves by attending courses or acquiring experience (Meeuwissen et al., 2023).

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

### 6.3.3.3 *Judicial resolution*

The mere *use* of sophisticated encrypted services can provide valuable indications regarding the professionalism and intentions of a suspect (Jansen et al., 2023). If an individual has taken measures to professionally shield their information using cryptophones, this does not indicate a one-time criminal activity, but rather enduring connections with criminal activity. However, the mere suspicion of additional encrypted incriminating material does not result in harsher penalties.

Van Toor (2022) states that the mere use of cryptophones (which is not necessarily illegal) by suspects can be relevant for two procedural concepts: reasonable suspicion of guilt and risk of recidivism. When the use of a cryptophone is sufficient to establish reasonable suspicion of guilt, it may lead to subsequent forms of investigative strategies, such as seizing a phone to try to gain access to encrypted data. The use of these services implies a preference for communicating covertly through specialised crypto communication service providers rather than regular applications, indicating financial capacity for encrypted communication and a preference for encrypted communication within a closed network. Therefore, the use of cryptophones can indicate a risk of recidivism and reasonable suspicion of guilt.

The aforementioned discussion and unclarity on the legality of crypto communication evidence has led to several procedural agreements, according to interviewees. These are agreements between the PPS and the defence, and possibly the judge, regarding the form of proceedings (Peters, 2019). A specific form is the judgment agreement, whereby the defendant generally agrees to confess to the charges in exchange for a reduced sentence. Interviewees mention that often it is enforced that one cannot appeal. It is within the judge's authority to decide to what extent these agreements can be accepted.

One interviewee highlighted that procedural agreements are being discussed at the national level, because some courts find them acceptable, while others do not. An example is the *Cymbal* case (ECLI:NL:RBOVE:2019:3103 and ECLI:NL:RBOVE:2019:3124). In the first trial, procedural agreements were rejected and the sentence was much higher than requested by the PPS, which led to the suspects feeling deceived. Consequently, both parties filed an appeal, which was granted. The process in the *Cymbal* case clearly demonstrated that legal practice is searching for how to deal with procedural and verdict agreements. There is a lack of a clear assessment framework for the judiciary, and there is also much uncertainty for the PPS and the defence (Peters, 2019).

These procedural agreements can result in a significant increase in efficiency, while the outcome (in terms of sentence length) is usually comparable to what the sentence would be after years of litigation (Peters, 2019). In a study by Davidse (2022), a public prosecutor specifically argued in favour of choosing procedural agreements due to the workload stemming from the many Sky ECC and EncroChat cases. A research request of 125 pages was the direct reason for making procedural agreements for this public prosecutor. According to this public prosecutor, submitting numerous research

requests to get a lower sentence is already common in cases stemming from EncroChat and Sky ECC investigations.

#### 6.4 CONCLUSION

The purpose of this chapter is to answer the main research question: what is the role of encryption in criminal cases? This question was broken down into three sub-questions: (1) What is the nature of encryption in criminal cases? (2) What is the role of encryption in evidence gathering in criminal cases? (3) What is the role of encryption in the criminal prosecution and judicial resolution of these cases?

*Nature of encryption.* In the limited set of legal rulings related to predominantly serious crimes, there appears to be an upward trend in the presence of forms of encryption. In particular, encrypted communication applications such as WhatsApp, Snapchat and Telegram are widespread. These applications play a significant role in securing private conversations. The impact of encryption of these applications might be different, as it is highly probable that the digital evidence from these applications might be frequently available in an unencrypted manner with an unlocked smartphone. Additionally, there is a notable rise in the utilisation of decrypted data obtained from platforms such as Ennetcom, EncroChat and Sky ECC in criminal cases. Furthermore, encrypted devices, particularly smartphones, are increasingly prevalent in judicial rulings. We could even go as far as what an interviewee mentioned: ‘There are no cases with encryption or without encryption; encryption is everywhere.’

*Evidence gathering.* There are broadly three ways to access encrypted data: technical cracking (i.e. brute forcing), bypassing encryption and alternative strategies. Bypassing can be done by finding, guessing or forcing the key, exploiting encryption software vulnerabilities, accessing the plain text when the device is used, or locating a copy of the plain text. Alternative strategies entail interrogations or observation of a suspect and house searches. Less frequently utilised measures are applying the hacking power or the decryption order. In recent years, there have been several cases where LEAs have explored creative ways to access encrypted data.

On the one hand, encryption makes it more difficult for investigative agencies to find relevant information. On the other hand, once data is decrypted, it generally contributes positively to successful prosecution. The opportunities presented by encryption in criminal cases lie in the ability to obtain evidence that would otherwise not exist through the decryption of digital devices. Specifically in the Netherlands, this type of evidence has aided in the criminal prosecution of organised crime because it provided unique insights into international organised crime.

*Criminal prosecution and judicial resolution.* The judiciary faces significant challenges in navigating the complexities of cases where encryption plays a part. The discussion revolves around the legitimacy of evidence, the lawful acquisition of

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

data and the need for technical expertise to ensure the reliability of information. It is necessary to gain a comprehensive understanding of the reliability of digital and previously encrypted evidence.

In the context of encryption, it is essential to recognise that this field engages with both theoretical and practical aspects across various domains of mathematics, including number theory and statistics among others, as well as cryptography, encompassing encryption and authentication methods, and techniques for breaking these methods. Legal professionals, including lawyers, often approach encryption with scepticism, yet their understanding may lack the epistemological foundations necessary to grasp the complexities and detailed aspects of encryption and decryption processes. Societal interpretations of encryption tend to lag behind scientific and technological advancements, resulting in a labour-intensive effort to bridge these gaps.

*The role of encryption in criminal cases.* Although issues of encryption related to investigation are not new (e.g. Henseler, 2010), they remain highly relevant and have become more prominent due to recent technological developments. Encryption seems to be increasingly present in criminal cases and judicial rulings of (serious) crimes. It poses limitations by complicating access to relevant data. However, LEAs have various methods to gain access to this potentially relevant data. Decrypted data is viewed as more reliable, although techno-fallacies might play a role. Encryption in criminal cases leads to delays, mostly due to the legality discussion in the context of cryptophones. Legislation does not align well with the digitalisation of crime, leading to creative means to access data and thereby pushing the boundaries of the law. In the Netherlands, the Innovation Act seems promising to explore legislation that provides more flexibility for prosecutors and judges to address the latest challenges.

## 6.5 LIMITATIONS

In our study, we have chosen a specific categorisation based on practical considerations and research focus. However, we recognise that alternative categorisations exist, and different perspectives can be equally valuable. By maintaining an open-minded approach, we allow room for other valid approaches and encourage further exploration in the field of encryption research. This chapter focuses specifically on encryption within law enforcement investigations and does not delve into other police strategies such as disruption. It deliberately does not address the broader societal benefits of digitisation and encryption, nor the benefits of encryption for the information security of organisations of LEAs. This study seeks to explore both the positive and negative aspects of encryption's role within the criminal justice system. The researchers have deliberately chosen the term 'role' instead of more charged terms such as 'impact' or 'effect', given the politically sensitive nature of the topic. A limitation of this research is its reliance on a small sample of judges, EMs and prosecutors. It is possible that they may

not have a comprehensive understanding of encryption in the criminal justice chain, thereby hindering a complete portrayal of this topic. Another limitation of this study is that we focused on the prevalence of encryption strategies in judicial outcomes and did not analyse the role of encryption in these cases.

*Implications and further recommendations.* The insights in this chapter aim to inform and stimulate debate about the role of encryption in the criminal justice chain, including debates about legal frameworks and investigative powers. It is crucial to define clearly what is considered encryption and what is not in this debate, as perceptions of encryption vary widely among individuals. For instance, some view encryption as deliberately making information inaccessible, while others see encryption as something that works as shielding in general, such as authentication on a mobile phone. Criminal law enforcement is becoming increasingly data-driven, as crime in a digitised society leaves traces in the form of data, including encrypted data. It is therefore essential to have clear legal frameworks for handling encryption appropriately during evidence gathering and criminal prosecution. Balancing privacy and data protection is crucial. Additionally, establishing requirements for digital investigative tools in law enforcement investigations is necessary. The Innovation Act, a pilot aiming to modernise the CCP, and its evaluation should be closely monitored (the evaluation is expected in October 2024) (Knapp, Grootelaar & Folmer, 2021).

Further analysis of the legal outcomes, including the context and implications of encryption, would be necessary to gain a comprehensive understanding of its impact on these cases. Exploring how LEAs secure, store and analyse data would provide valuable insights. Specifically, the (perceived) reliability of decrypted evidence and its correct interpretation in courts requires further research and a continuation of discussion. Since 2020, the Dutch judiciary has recognised forensic advisors as an asset, aiming to enhance the evaluation of forensic reports (Meeuwissen et al., 2023). They work as generalists for courts, assisting judges and paralegals in complex criminal cases in their understanding and logically correct interpretation of forensic reports and related documents. They advise the judge and EM in the investigative and adjudicative stage, but do not advise on the probative value of the evidence. It is not clear to the authors of this chapter if these forensic advisors also advise on decrypted evidence. Therefore, it would be interesting to explore the role of forensic advisors in aiding the comprehension of decrypted data in criminal cases.

While describing the current situation, we must also consider future developments, such as the impact of quantum computing. Quantum technology continues to develop in the coming years. With quantum photonics, it is possible to perform many calculations simultaneously. Once this technology becomes practical on a large scale, current encryption methods can be cracked at lightning speed, rendering certain encryption methods insecure. Since encryption is essential for securing networks and information systems, this poses risks to the digital society (Rijksinspectie Digitale Infrastructuur, 2023). In this context, post-quantum cryptography, which includes

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

all forms of cryptography that remain secure after the advent of quantum computers, become crucial (National Cyber Security Centre, 2023). Furthermore, new digital investigation techniques are a vital component for effective law enforcement operations, and other methods for facilitating investigations are likely to emerge. Law enforcement must closely monitor these developments to leverage any relevant new opportunities (Europol, 2023).

Anticipation is also needed for challenges related to accessing investigation-relevant data due to digital advancements such as AI. AI has the potential to significantly reduce the time and resources needed to break encryption algorithms, which could undermine the security of sensitive data. However, AI can also enhance cryptography by developing more secure encryption algorithms. Therefore, it is crucial to acknowledge the potential risks and benefits of AI in cryptography and develop strategies to mitigate the risks while leveraging the benefits (Chethiya, 2023).

To conclude, it is difficult to pinpoint the exact role of encryption in the criminal justice system. The complexity of investigations, shaped by a mix of facts, chance and circumstances, makes it impossible to quantify unresolved or additionally solved cases or calculate lost or saved time. Our study presents a balanced perspective on how encryption affects the criminal justice system, highlighting both its advantages and obstacles.

## REFERENCES

- Boeser, J.S. (2021). Cybersecurity en ‘datagedreven’opsporing: stand van zaken met betrekking tot de interceptie van versleutelde cryptocommunicatie [Cybersecurity and ‘data-driven’ investigation: current status regarding the interception of encrypted crypto-communication]. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 7(5), 351-356. <https://doi.org/10.5553/TBSenH/229567002021007005008>.
- Chethiya, P. (2023). How Artificial Intelligence become a threat to cryptography – A systematic literature review. <https://doi.org/10.13140/RG.2.2.14344.60167>.
- Davidse, J. (2022). Pionieren met procesafspraken [Pioneering with procedural agreements]. *Opportuun*, 2. <https://magazines.openbaarministerie.nl/opportuun/2022/02/pionieren-met-procesafspraken>
- Driessen, C. (2021, 8 June). Internationale coalitie tapte achttien maanden lang criminelen af via ‘niet-kraakbare’ app [International coalition intercepted criminals for eighteen months via ‘unhackable’ app]. *NRC*. <https://www.nrc.nl/nieuws/2021/06/08/internationale-coalitie-tapte-achttien-maanden-lang-criminelen-af-via-niet-kraakbare-app-a4046442>
- Driessen, C., & Meeus, J. (2021, 9 March). Encryptie is niet meer weg te denken uit het criminele milieu [Encryption has become indispensable in the criminal underworld].

- NRC. <https://www.nrc.nl/nieuws/2021/03/09/encryptie-niet-meer-weg-te-denken-uit-criminele-milieu-a4034876>
- Egberts, M. M. (2022). De reikwijdte van het inzagerecht en 'equality of arms' in het licht van grote datasets, Hansken en toekomstige ontwikkelingen [The scope of the right to access and 'equality of arms' in light of large datasets, Hansken, and future developments]. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 2(6), 119-129. <https://doi.org/10.5553/TBSenH/229567002022008002007>.
- Europol & Eurojust Public Information (2018). *Common challenges in combating cyber-crime*. <https://www.europol.europa.eu/publications-events/publications/common-challenges-incombating-cybercrime>
- Europol (2023). The Second Quantum Revolution: The impact of quantum computing and quantum technologies on law enforcement. <https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement>
- Galič, M. (2021). De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding [The rights of the defense in the context of extensive datasets and advances search engines in criminal cases: a suggestion for expansion]. *Boom Strafblad*, 2(2), 41-49.
- Galič, M., Stevens, L., & Koops, B.J. (2023). Editorial: A triologue on regulating data-driven criminal procedure. *New Journal of European Criminal Law*, 14(4), 423-433. <https://doi.org/10.1177/20322844231213484>.
- Groothoff, B., & Jansen, R. (2022). Cyberzaken bij het gerechtshof Den Haag [Cyber cases at the Court of Appeal in The Hague]. *Ars Aequi*, 2022(3), 224-231.
- Groothoff, B. (2023). Gekraakte Cryptocommunicatie als bewijs in strafzaken [Decrypted cryptocommunication as evidence in criminal cases]. *Ars Aequi*, 2023(6), 395-395.
- Hartel, P., & van Wegberg, R. (2023). Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. *Crime Science*, 12, 5. <https://doi.org/10.1186/s40163-023-00185-4>.
- Henseler, H., (2010). *Opzoek naar de digitale waarheid* [Searching for the digital truth]. HvA Publicaties.
- Jacobs, R. (2022). De innovatiewet Strafvordering: meeliften op een hype? [The Innovation Act on Criminal Procedure: Riding the Wave of a Hype?]. *Tijdschrift Modernisering Strafvordering*, 2022(1), 31-37. <https://doi.org/10.5553/PMSv/258950952022002>.
- Jansen, J., Westers, S., Schreurs, W., Berkenpas, M., Alpár, G., & Stol, W. (2023). *De rol van encryptie in de opsporing. Belemmeringen en mogelijkheden* [The role of encryption in law enforcement: obstacles and opportunities]. WODC.
- Kerr, O.S., & Schneier, B. (2017). Encryption workarounds. *Georgetown Law Journal*, 106(4), 989-1019. <http://dx.doi.org/10.2139/ssrn.2938033>.
- Knapp, M., Grootelaar, H., & Folmer, T. (2021). *Pilots Innovatiewet Strafvordering* [Pilot innovation act on criminal procedure]. WODC.

S. WESTERS, M. BERKENPAS, J. JANSEN, W. SCHREURS, G. ALPAR AND K. BLUHM

- Laumans, W., Vugts, P. (2023, 3 February). Recherchechef Andy Kraag: ‘We pakken ze bij hun achilleshiel: communicatie’ [Detective chief Andy Kraag: ‘We hit them in their Achilles’ heel: communication’]. *Het Parool*. <https://www.parool.nl/misdaad/recherchechef-andy-kraag-we-pakken-ze-bij-hun-achilleshiel-communicatie~b91ce2ee/>
- Meeuwissen, J., de Roo, R., Kruithof-van Esch, J., van der Heijden, S., Claushuis, M., van Blijswijk-Kieftenbeld, L., & Remijn, W. (2023). Forensic advisers working for all district courts and courts of appeal in the Netherlands: An overview and discussion. *Journal of Forensic Sciences*, 69(1), 182-188. <https://doi.org/10.1111/1556-4029.15385>
- Nederlandse Orde van Advocaten (2021, 20 May). Geheimhoudingsplicht niet goed te waarborgen met cryptotelefoons [The obligation of confidentiality cannot be properly ensured with cryptophones]. <https://www.advocatenorde.nl/nieuws/geheimhoudingsplicht-niet-goed-te-waarborgen-met-cryptotelefoons>
- NOS (2021, 31 May). Raad voor de Rechtspraak wil driekwart van de vonnissen online publiceren [The council for the judiciary aims to publish three-quarters of judgments online]. <https://nos.nl/artikel/2382964-raad-voor-de-rechtspraak-wil-driekwart-van-de-vonnissen-online-publiceren>
- NOS (2022, 25 October). Brandbrief advocaten over opsporingsmethoden, ‘eerlijk proces op het spel’ [Urgent letter from lawyers regarding investigative methods, ‘fair trial at stake’]. <https://nos.nl/artikel/2449687-brandbrief-advocaten-over-opsporingsmethoden-eerlijk-proces-op-het-spel>
- National Cyber Security Centre (2023). Factsheet Post-quantum cryptography. <https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-post-quantum-cryptography>
- Oerlemans, J.J. (2019, 27 December). Cybercrime jurisprudentieoverzicht – december 2019 [Cybercrime jurisprudence overview]. <https://jjoerlemans.com/tag/bulletproof-hosting/>
- Oerlemans, J.J. (2020). Cybercriminaliteit en opsporing [Cybercrime and law enforcement]. In W. van der Wagen & M. Weulen Kranenbarg (Eds.), *Basisboek cybercriminaliteit* (pp. 195-258). Boom Criminologie.
- Openbaar Ministerie (2023a, 3 February). Politie leest opnieuw mee met criminelen: cryptocommunicatiedienst Exclu ontmanteld [Police eavesdrops on criminal again: cryptocommunication service Exclu dismantled]. <https://www.om.nl/actueel/nieuws/2023/02/03/politie-leest-opnieuw-mee-met-criminelen-crypto-communicatiedienst-exclu-ontmanteld>
- Openbaar Ministerie (2023b, 20 March). Digitaal bewijsmateriaal via Hansken nu raadpleegbaar voor advocaten vanaf werkplek [Digital evidence via Hansken is now accessible for attorneys from their workplace]. <https://www.om.nl/actueel/nieuws/2023/03/20/digitaal-bewijsmateriaal-via-hansken-nu-raadpleegbaar-voor-advocaten-vanaf-werkplek>

- Rijksinspectie Digitale Infrastructuur (2023). Trendradar: een kijkje in de digitale toekomst [Trend radar: a closer look in the digital future]. <https://www.rdi.nl/actueel/nieuws/2023/04/12/trendradar-een-kijkje-in-de-digitale-toekomst>
- Peters, L.J.J. (2019). Cymbal en de alternatieve afdoening van ondermijningsdossiers: Een bespreking van 's lands eerste procesafpraak [Cymbal and the alternative resolution of undermining cases: a discussion of the nation's first procedural agreement]. *Strafblad: tijdschrift voor wetenschap en praktijk*, 17(5), 7-13, Article 42.
- Peters, L. (2022). Procesafspraken in strafzaken: Bespreking van actuele experimenten en in het bijzonder de vonnissen uit Limburg en Rotterdam [Procedural agreements in criminal cases: Discussion of current experiments and particularly the judgments from Limburg and Rotterdam]. *Nederlands Tijdschrift voor Strafrecht*, 2022(2), 59-70. [NTS 2022/21]. <https://doi.org/10.5553/NTS/266665532022003002003>
- Sunde, N. (2022). Unpacking the evidence elasticity of digital traces. *Cogent Social Sciences*, 8(1), 2103946. <https://doi.org/10.1080/23311886.2022.2103946>.
- Uden, A. van, & Eeden, C.A.J. van den (2022). *De hackbevoegdheid in de praktijk: Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)* [The hacking authority in practice: an empirical study on the implementation of the hacking authority (articles 126nba, 126uba, 126zpa CCP)]. WODC.
- Van Toor, D.A.G. (2022). Het enkele gebruik van cryptophones als basis voor procesrechtelijke concepten [The mere use of cryptophones as a basis for procedural concepts]. *Tijdschrift Voor Bijzonder Strafrecht & Handhaving*, 8(2), 77-81. <https://doi.org/10.5553/TBSenH/229567002022008002001>.



## 7 WHEN DOES POLICE PROCESSING OF PERSONAL DATA FALL WITHIN THE MATERIAL SCOPE OF THE LAW ENFORCEMENT DIRECTIVE?

*An assessment of the material scope of the Directive using Denmark as a case study*

*Tanja Kammergaard Christensen*

### **Abstract**

*This chapter focuses on the scope of the Law Enforcement Directive (LED). The LED sets the framework for the processing of personal data by the police, but according to Article 1(1) only when the police process personal data for the purpose of prevention, investigation or detection of criminal offences or the protection against or prevention of threats to public security. Thus, not all processing of personal data by the police falls within the scope of the Directive. The chapter assesses what is meant by criminal offences and public security under EU law and whether these concepts have a common meaning in the EU, which is necessary if the scope of the LED is to be the same in all countries. It then examines the tasks of the Danish police and the related processing of personal data in relation to the scope of the LED and Danish law.*

*The chapter concludes that there is no common understanding of all the terms in Article 1(1) in the EU, which is why the scope of the LED is not yet clearly defined, and that a large margin of discretion is left to the Member States. In addition, Denmark has chosen a pragmatic solution when implementing the LED, which is why practically all police processing of personal data in Denmark will be covered by the Danish LED.*

### 7.1 INTRODUCTION

The Law Enforcement Directive<sup>1</sup> (LED) is the first legally binding instrument at EU level that sets out rules for both national and cross-border processing of personal data by law enforcement authorities. The LED is a minimum harmonisation directive

---

1 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

(Article 1(3)), which allows Member States to set higher standards than those laid down in the Directive. This means that although the Directive is intended to help ensure a more coherent framework in the Union, individual Member States may have higher protection than that set out in the Directive. This might lead to unequal protection in different Member States.

It is central to the interpretation of the Directive that the Directive was adopted on the basis of Article 16 of the Lisbon Treaty. The choice of Article 16 TFEU supports the overall purpose of the Directive, which is to ensure the protection of natural persons in connection with the processing of personal data. When interpreting the LED, the protection of personal data must therefore be prioritised. Article 16(2) TFEU in the Lisbon Treaty gave the EU a specific legal basis to also adopt rules on the protection of personal data applicable to judicial cooperation in criminal matters and police cooperation. The LED was adopted in the context of the European Commission's comprehensive reform of the previous data protection rules in the EU.<sup>2</sup> The Intergovernmental Conference that adopted the Lisbon Treaty recognised the need for specific data protection rules for judicial cooperation in criminal matters and police cooperation, due to the specific nature of these areas (recitals 10 and 11 LED).

According to Article 1(1) LED, the Directive applies only when competent authorities, such as the police, process personal data for the prevention, investigation, detection or prosecution of criminal offences. This chapter will focus solely on the processing of personal data by the police, which is why the processing of personal data by other competent authorities is not assessed here.

If the police process personal data for other purposes, the General Data Protection Regulation (GDPR) will, in general, apply to this processing of personal data. However, there are several instances where it is unclear whether the GDPR or the LED applies to the police's processing of personal data, as there are several words in Article 1 LED that are not clear from a word-for-word interpretation. For instance, it is unclear whether the processing of personal data is part of the prevention, investigation, detection or prosecution of criminal offences, and how the EU defines a criminal offence, just as it is not clear what is meant by public safety.

The assessment of whether data is processed under the GDPR or LED is relevant, for example, when the police use the collected data in their big data systems or when the police use personal data to improve their systems. Under the GDPR, there are several lawful bases for processing personal data (Article 6 GDPR), whereas the LED only allows for one lawful basis for processing personal data, namely that the processing is based on EU or national law (Article 8 LED). If the police want to use personal data for the

---

2 European Commission Press Release, 'Commission proposes comprehensive reform of data protection rules to increase users' control over their data and reduce costs for business', IP/12/46, 25 January 2012, and MEMO/12/41 'Data protection reform: Frequently asked questions'.

purposes described in Article 1 LED, the police therefore require a legal basis to carry out the processing in their big data systems, whereas the processing of personal data for the purpose of improving systems will fall outside the scope of the LED and therefore requires a legal basis in Article 6 GDPR. In addition, the LED sets out a number of requirements for the storage of personal data; for example, the police must, as far as possible, distinguish between different categories of data subjects in their systems, and a distinction must be made between data based on facts and personal data based on personal assessments (Articles 6 and 7 LED). The criteria for further use of personal data also depend on whether data is collected under the GDPR or the LED, as the GDPR requires, among other things, when assessing whether data can be used for other purposes, the controller to assess the possible consequences of the processing for the data subjects (Article 6(4)(d) GDPR), whereas the LED primarily requires authorisation and proportionality (Article 4(2) LED).

Against this background, the chapter will assess the scope of application of the LED in relation to the police, with particular focus on the understanding of the concepts of criminal offence and public security. Can a uniform understanding of the concepts be derived at EU level? This is followed by an assessment of Denmark's implementation of the Directive and its scope. Which of the tasks of the Danish police and the processing of personal data in relation to them will fall within the scope of the Directive, and is there a clear separation of the scope of the LED or GDPR in relation to the police in Denmark?

## 7.2 METHODOLOGY

To derive the material scope of the LED, the doctrinal methodology is used. This means that the aim in the chapter is to identify, analyse and synthesise the content of the law<sup>3</sup>.

The analysis of the scope of application of the LED is based on the legislative preparatory work in connection with the adoption of the LED at EU level, as well as the literature on the subject. This is to assess whether the scope of application of the LED is currently clear to the Member States. In addition, case law from the European Court of Justice is included for the cases where the European Court of Justice has taken a position on the scope of application of the LED.

This is followed by an assessment of the Danish implementation of the LED, based on the Danish preparatory works to the law. These are compared with the tasks currently assigned to the police by law. This is to assess whether the Danish implementation of the Directive is in accordance with EU law.

---

3 Burton, Dawn Watkins and Mandy, *Research methods in law*, Routledge, 2013, p. 9.

TANJA KAMMERSGAARD CHRISTENSEN

The assessment of the Danish implementation of the LED and its scope in relation to the role of the police is considered to be of relevance to the other Scandinavian countries, as the police in these countries have largely the same portfolio of tasks as in Denmark.

### 7.3 THE SCOPE OF THE LED

According to Article 2 LED, the Directive is applicable to the processing of personal data by competent authorities for the material scope outlined in Article 1(1). This implies that the directive comes into play when competent authorities process personal data for ‘the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’ (Article 1(1) LED).

In this chapter, the focus will only be on the material scope of the LED, as the chapter is limited to the processing of personal data by the police in connection with the fulfilment of their tasks, and therefore the personal scope is already fulfilled.<sup>4</sup> The material scope can be divided into two situations: (1) prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; and (2) safeguarding against or preventing threats to public security.<sup>5</sup>

The processing of personal data following the material scope is further elaborated in recital 34 LED, which states that the purposes mentioned in Article 1

should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction.

With the words ‘such as’, it is given that the recital does not cite an exhaustive list, but only mentions examples of processing that can be done by the competent authorities, both in the initial stage of an investigation and later on in the police systems used for data linking, processing, etc.

In recital 12 it is clarified that the LED also applies to:

---

4 The material scope of the law defines what kind of personal data processing the law applies to, while the personal scope defines which authorities the law applies to

5 Since the execution of criminal penalties is not a police task, but a task for the public prosecutor, this element will not be discussed further in this chapter.

police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence.

However, this does not explicitly help to determine the scope of use of the LED.

The GDPR,<sup>6</sup> too, cannot help in the interpretation of the scope of the LED, as the GDPR merely clarifies that it does not apply when competent authorities process personal data for LED purposes (Article 2(2)(d)). In recital 19 of the preamble, the GDPR states that if competent authorities are given tasks that are not intended to process personal data that fulfil the purpose in Article 1(1) LED, then the GDPR applies to this processing. At the same time, however, it points out that if competent authorities are given tasks where personal data must be processed for GDPR purposes, then Member States should maintain or introduce more specific provisions to adapt the application of the rules to the GDPR. Such provisions can more precisely define specific requirements for the processing of personal data by these competent authorities (recital 19 GDPR).

The answer to a more precise interpretation of the scope of application of the LED cannot be found in the case law of the Court of Justice of the European Union (CJEU) on the LED either. To date, the CJEU has ruled in three cases concerning the LED: C-180/21 *Inspektor v Inspektorata kam Visshia sadeben savet*, C-205/21 *V.S.* and C-118/22 *N.G.* The last two judgments deal mainly with data minimisation and storage limitation and therefore do not say much about the scope of the LED.

The first judgment, Case C-180/21, deals to some extent with the scope of the LED, but more with the different types of processing that personal data are subject to, including prevention, detection and investigation, and that this should be considered as processing for different purposes.

During the adoption of the LED, its material scope was problematised by the Member States in the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, and at several meetings questions were asked about the scope of the LED. At the third meeting of the expert group, the group stated that the *Engel* criteria (see further below) should be applied when assessing whether the LED applies. Some Member States emphasised that their national systems recognise misdemeanours as part of criminal law and therefore considered that such misdemeanours also qualify

---

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

TANJA KAMMERSGAARD CHRISTENSEN

as criminal offences according to the *Engel* criteria (Minutes of the third meeting of the Commission expert group, para. 1). The discussions on the scope of the LED continued at several meetings, especially in relation to the personal scope (Minutes of the fifth and seventh meetings of the Commission expert group, para. 1). At the ninth meeting of the expert group, the scope of the LED was finalised and the group concluded that

Member States [...] cannot label a situation as a criminal offence only for the specific purpose of including it in the scope of the Directive. Where national legal systems do not provide for a (clear) notion of criminal offence, Member States have the option to decide on the basis of objective criteria (e.g. use of criminal procedure or application of typical criminal sanctions such as imprisonment), where to draw the line between administrative and criminal offences. (Minutes for the ninth meeting of the Commission expert group, para. 1)

Some Member States informed the expert group that they would apply the GDPR to all types of administrative procedures (regardless of whether such procedures may ultimately become criminal proceedings), while others announced that they would apply the LED to all offences that qualify as criminal under their national law, including minor offences (Minutes for the ninth meeting of the Commission expert group, para. 1, and Sajfert & Quintel, 2017, p. 4).

In the first report on the application and functionality of the LED (Communication from the Commission to the European Parliament and the Council), the Commission also states that the material scope of the LED gives rise to doubts, as Member States interpret the LED differently. Several Member States do not distinguish between criminal and administrative offences, and thus some national implementing laws refer to purposes for processing personal data that are not listed in Article 1 LED (e.g. threats to public policy or public security). However, the report does not address either the consequences or the solution to this, but merely points out that there are several cases pending before the CJEU that may help determine the scope of application of the LED provisions to align the application of the rules with the GDPR. Such provisions can more precisely define specific requirements for the processing of personal data by the competent authorities (Communication from the Commission to the European Parliament and the Council, p. 10).

The fact that Member States will apply the LED depending on the content of their national legislation means that the scope of the LED will not be the same in all Member States, but that the scope will depend on the concrete implementation of the Directive in each Member State. This was problematised in the assessment of the implementation of the Law Enforcement Directive (Vogiatzoglou & Marquenie, 2022) as a lack of harmonisation leading to legal uncertainty. Therefore, the authors point out that there is a need for a more uniform understanding of what constitutes a criminal offence and

what constitutes national security, as there is currently no EU legal definition of this (Vogiatzoglou & Marquenie, 2022, p. 17). This leads to an uneven application of the LED and legal uncertainty, which is contrary to the intention of the Directive (Kosta & Boehm, 2023, p. 57).

### 7.3.1 *Criminal offence*

The notion of a ‘criminal offence’ in Article 1(1) is of central importance when determining whether the processing of personal data done by the police falls within the scope of the LED. In recital 13 it is noted that ‘criminal offence’ within the meaning of the LED should be an autonomous concept of Union law as interpreted by the CJEU.

The uniform understanding of the concept of a criminal offence must therefore be sought in case law from the CJEU. It follows that if an offence is to have the character of a criminal offence, it must meet three criteria. These criteria are initially derived from the judgment of the European Court of Human Rights (ECtHR) of 8 June 1976, *Engel and others v. the Netherlands* (*Engel*). They are presented for the first time in para. 82 of that case, but have since been repeated in the case law of the CJEU (see e.g. Opinion of Advocate General Emiliou of 4 May 2023 in Case C-683/21, para. 74 and the Opinion of Advocate General M. Szpunar of 17 December 2020 in Case C-439/19, para. 87).

The three criteria that are relevant for assessing whether an offence has the character of a criminal offence are: (1) the legal qualification of the offence under national law; (2) the nature of the offence; and (3) the nature and severity of the sanction that the offender risks having imposed on them (*Engel*, para. 82). The last two criteria are not cumulative, but alternative, and it is thus sufficient that the offence, by its nature, is to be considered criminal or that the offence has resulted in a penalty which, by its nature and severity, falls within the criminal sphere (*Ezeh and Connors v. the United Kingdom*, para. 86). Central to the assessment of whether an offence is a criminal offence is therefore especially point (2), concerning the nature of the offence.

At this point in time, the case law of the CJEU cannot contribute much to an interpretation of the concept of a criminal offence. However, the CJEU points out in Case C-439/19, para. 88, that infringements that are not classified as criminal offences under national law may nevertheless be criminal offences if this follows from the nature of the infringement and the severity of the sanctions that it may entail. Thus, it is not decisive how the act is defined in national law, as the *Engel* criteria must be considered in order to assess whether it is a criminal offence. In Case C-439/19, the CJEU then examines whether traffic offences can be categorised as a criminal offence. The CJEU concludes that given that traffic offences are subject to sanctions for both preventive and repressive purposes, and that these sanctions can be severe, traffic offences can have the character of a criminal offence (Case C-439/19, para. 91). In addition, the Advocate General’s Opinion in Case C-548/21 clarifies that:

TANJA KAMMERSGAARD CHRISTENSEN

Directive 2016/680 only covers the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences. That is, all types of criminal offences and not only serious criminal offences. (Opinion of Advocate General Campos Sánchez-Bordona of 20 April 2023 in Case C-548/21, para. 67)

When assessing whether the LED or GDPR applies to the roles of the police relating to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, it must therefore be taken into account whether the processing of personal data takes place in connection with a task that falls within the concept of a criminal offence according to the *Engel* criteria, regardless of the assessment in national law or whether it concerns tasks that are considered to be of a disciplinary or administrative nature.

However, as mentioned above, several Member States consider that the LED should also apply to minor offences if the offences are regulated by criminal law (Minutes of the ninth meeting of the Commission expert group, para. 1), which is why the EU's desire for a uniform understanding of the concept of 'criminal offence' is not currently fulfilled (see also Kosta & Boehm, 2023, p. 59).

### 7.3.2 *Public security*

The notion of 'including the safeguarding against and the prevention of threats to public security' in Article 1 LED was not a part of the original draft of the LED. It was added by the Council, but it is unclear from the preparatory work what the reason for this was.<sup>7</sup>

In relation to the role of the police related to the safeguarding and prevention of threats to public security and the related processing of personal data, the scope of the LED is very imprecise, but also very broad, as pointed out by, among others, the European Data Protection Supervisor (EDPS) in the context of the adoption of the Directive., as the term threats to public security is not clear and does not provide a clear delimitation of the scope. This is why the EDPS recommended that the scope of the LED should be limited to activities in the field of criminal law enforcement by the police (EDPS Opinion 6/2015, pp. 5-6). The notion of safeguarding and prevention of threats to public security seems to expand the broadly formulated scope of the LED, and gives the Member States an even bigger opportunity to interpret the scope of the Directive (Brewczyńska, 2022, p. 112).

As mentioned above, recital 12 states that the activities to which LED applies can also be:

<sup>7</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST\\_13523\\_2015\\_ADD\\_1](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13523_2015_ADD_1).

exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence.

However, this does not provide a more precise indication of what, according to the LED, is to be understood by public security. However, it also follows from recital 14 that national security is not included in the scope of application of the LED, which also follows from Article 4(1) TEU. This means that when interpreting the scope of application of the LED, a distinction must be made between national security and public security. However, the exact difference between these two concepts is not clear-cut in EU law (for more details see Vogiatzoglou & Fantin, 2019, and Vogiatzoglou & Marquenie, 2022, p. 24).

There is case law from the CJEU in which the concepts of both national security and public security are used, but as the concepts are very broad, the precise definition has not yet been established, in part because there may be some overlap between the concepts and their application (Vogiatzoglou & Marquenie, 2022, p. 23).

National security has been used as a concept in Case C-511/18, para. 135, where the CJEU states that:

In that regard, it should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.

According to this case law, the concept of national security must be interpreted restrictively (Case C-439/19, para. 62), and the concept seems to be understood as linked to the core, sovereignty and democratic nature of a state (Vogiatzoglou & Fantin, 2019, p. 28). Therefore, when understanding the concept of public security and the tasks of the police in relation to it, and the scope of application of the LED, tasks relating to protection against terrorism must not be included, unless the Member States have provided otherwise in their implementation.

The concept of public security in relation to EU law has been used in Case C-145/09, para. 44, where the CJEU reiterates:

TANJA KAMMERSGAARD CHRISTENSEN

a threat to the functioning of the institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security.

Although these threats are not threats to national security, they are, however, increasingly serious threats that must be recognised as being capable of affecting public security.

In line with this, the EU legislator, in adopting Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, defined public security in recital 19 as follows:

The concept of ‘public security’, within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests.

Also, according to this definition of public security, the concept must include more serious threats to public security, not minor offences.

As mentioned above, for the LED to apply, both the material and the personal scope must be fulfilled, which means that if the police are given tasks that are not for one of the purposes specified in Article 1(1), then the GDPR will apply to the processing of personal data in connection with these activities. The Member States’ regulation of the police and the tasks the police have in each Member State will therefore have an impact on whether the LED or GDPR applies to the processing of personal data done by the police.

### 7.3.3 *Summarising the scope of application*

In order for the LED to apply, both the material and the personal scope must be fulfilled. For the police, the personal scope is already fulfilled, whereas it must be assessed whether the material scope is fulfilled for the police’s processing of personal data to fall within the scope of the LED. This means that if the police are given tasks that are not

for the purposes specified in Article 1(1), then the GDPR will apply to the processing of personal data in connection with these activities.

The LED will, as illustrated above, apply to the processing of personal data by the police if the processing is for a purpose regulated in Article 1(1). For it to be a ‘criminal offence’, according to the wording and interpretation of the LED, it is a requirement that it is a criminal offence that meets the *Engel* criteria. Likewise, ‘threats to public safety’ must be more serious threats to safety and not minor offences.

Following an interpretation of the scope of the LED, the LED will thus only apply to police processing of personal data if it concerns the prevention, investigation, detection or prosecution of more serious crime and thus, as a starting point, not minor offences.

As described, determining whether police processing of personal data falls within the scope of the LED or the GDPR can be a complex assessment, and it can be difficult to assess what impact this has on the police’s ability to process personal data.

In the following, the role of the police in Denmark and the implementation of the Directive will be described to clarify to which parts of the role of the police the LED or GDPR apply. As Norwegian and Swedish legislation regulating the role of the police is very similar to the Danish regulation, this chapter will be relevant for understanding the scope of the LED in these countries as well.

#### 7.4 THE ROLE OF THE POLICE IN DENMARK

According to the Danish Police Act § 2, the Danish police have the following tasks:

- 1 prevent criminal offences, disturbance of the public peace and order and danger to individuals and public safety,
- 2 avert danger of disturbance of public peace and order and danger to individuals and public safety,
- 3 put an end to criminal activity and to investigate and prosecute criminal offences,
- 4 provide assistance to citizens in other situations of danger,
- 5 perform control and supervisory tasks in accordance with applicable law,
- 6 provide assistance to other authorities in accordance with applicable law; and
- 7 perform other tasks that follow from applicable law or otherwise have a natural connection to police activities.<sup>8</sup>

Similar provisions are to be found in Swedish and Norwegian law, see *Polislag* § 2 and *politiloven* § 2.

This list of police tasks in Denmark is, in theory, considered to be an exhaustive list, which is why the police cannot be assigned other tasks than those mentioned in

---

<sup>8</sup> Author’s own translation into English.

TANJA KAMMERSGAARD CHRISTENSEN

the provision and should not take on other tasks than those listed therein (Legislative proposal L 159 Forslag til lov om politiets virksomhed, column 5913; Henricson, 2022, p. 149 and Henricson, 2020, p. 29). The tasks of the police under Danish law are of a very different nature and include matters that fall directly within the scope of the LED, including the tasks in the Police Act § 2, nos. 1-3. The remaining tasks in the Police Act cannot, on a direct reading, be said to fall within the scope of the LED. Whether the processing of personal data in connection with all the tasks imposed on the police falls within the scope of the LED or whether the processing of personal data in connection with some of the tasks instead falls under the GDPR is determined by the purpose of the specific processing. This means that tasks carried out by the police where personal data is processed, but where the role of the police do not relate to the investigation, prevention, etc. of criminal offences, will generally not be covered by the scope of the LED.

In Denmark, the tasks of the police are traditionally divided into tasks within and outside the criminal justice system (Police Commission, 2002, p. 29, and Henricson, 2019, p. 3). The tasks within the criminal justice system will probably in most cases fall under the concept of criminal offences according to EU practice, and the processing of personal data in connection with this will thus be regulated by the LED. These tasks will (see below) typically be related to tasks where the police investigate or uncover criminal offences and are in the Danish context regulated in detail in the Danish Administration of Justice Act (Legislative proposal L 159, column. 5879).

The tasks that fall outside the criminal justice system, and the processing of personal data that takes place in this context, may be regulated by both the GDPR and LED, depending on the purpose of the processing and the national implementation of the LED. Especially for tasks more related to preventive efforts, the processing of personal data in connection with this could be covered by both the LED and GDPR, which depends, among other things, on how concrete the risk of a criminal offence being committed is in each individual case (Kosta & Boehm, 2023, p. 61).

This means that many of the personal data included in police systems and the processing of them that takes place may need to be regulated by two different pieces of legislation, and that the LED requires a specific assessment of the task to determine whether the relationship should be regulated by the LED or GDPR. However, when implementing the LED, this has been solved in several countries by the legislator deciding which EU regulation the police processing of personal data should be regulated by (Kosta & Boehm, 2023, p. 43).

Below is a review of the police's tasks within and outside the criminal justice system in Danish law, where it is considered whether the processing of personal data that takes place in connection with this will have to be regulated by the LED or the GDPR, based on both the wording of the LED and the implementation of the LED in Danish law.

#### 7.4.1 *The role of the police within the criminal justice system in Denmark*

The police's tasks within the criminal justice system can, according to Danish law, be summarised as: 'the police shall put an end to criminal activity and investigate and prosecute violations of criminal provisions to the extent that the offence is subject to public prosecution' (Police Commission, 2002, p. 30). The powers that the police have to fulfil their role within criminal procedure are thus particularly linked to the investigation and prosecution of criminal offences. These are mainly regulated in the Danish Administration of Justice Act, Chapter 61 "The scope of criminal procedure", according to which the police in Chapter 72 "Intrusion" are authorised to carry out several specified criminal procedural interventions, such as interference with the secrecy of communications, searches, personal investigations, etc. Processing of personal data in relation to interventions regulated in the Administration of Justice Act will fall within the scope of the LED. The criminal offences that the police are authorised to investigate or uncover under the Administration of Justice Act will be regulated by criminal law rules. This means that the nature of the offence and the nature and severity of the sanction that the offender risks incurring, as well as the penalty under special legislation, will be so high that the offence meets the *Engel* criteria and will thus be covered by the LED.

However, the criminal offences that the police must bring to an end, etc. are found not only in criminal law, but also in special legislation (Police Commission, 2002, p. 30, and Legislative proposal L 159, column. 5882), which means that it is not clear whether all the criminal offences that the police must investigate or bring to an end will meet the *Engel* criteria and thus fall within the scope of the LED.

It becomes more problematic to determine whether the processing of personal data should be regulated by the LED or the GDPR in cases where the police are obliged to assist in the investigation of criminal offences in special legislation. In these cases, the police can assist with other authorities' control tasks, for example when food authorities inspect restaurants, and the owner of the restaurant does not want to open the door. In these cases, the food authority may not do so by force, but must call the police and obtain police assistance (Police Act § 2, no. 6). Police assistance may therefore concern other authorities' inspection tasks (outside the criminal procedure, as there will be no criminal offence in the first place) and criminal offences (within the criminal procedure) if the inspection authority is certain that there is something criminal to find. Even if these tasks fall within the criminal justice system, it is not certain that they are criminal offences according to the understanding of the *Engel* criteria, which is why the processing of personal data in these situations will not always be regulated by the GDPR. For the LED to be applied uniformly in the Member States, it will therefore generally be required to assess in specific situations whether the *Engel* criteria are met, which may be done according to the approach of the CJEU in Case C-439/19 *B. v. Latvijas*.

TANJA KAMMERSGAARD CHRISTENSEN

The Danish police also have several public order and security tasks, whereby they must ensure public order, peace and safety. In Denmark, these tasks regulated in the Police Act §§ 7-13 and are also specifically regulated in the Danish Public Order Regulation, according to which the police are tasked with ensuring public order and averting danger to the safety of individuals. The Danish Public Order Regulation further determines, among other things, when fines can be issued to citizens for violation of the public order. Although the title of the Danish Public Order Regulation also states that it regulates the police's safeguarding of public security, and the processing of personal data in connection with the fulfilment of the tasks under the Danish Public Order Regulation is thus directly regulated by the LED, it is a question of whether the understanding of public security under EU law and under Danish law is the same.

The Public Order Regulation governs several less serious matters to ensure public order. Among other things, it is stipulated in § 3 that 'fighting, screaming, shouting or other noisy, violent, insulting or similar behaviour that is likely to disturb public order must not take place', in § 10 that 'Young children should be properly supervised by parents or others in their care when travelling on roads', and in § 12 that 'it is forbidden to use firearms, bows, slingshots or the like, to light fires, or to throw stones, snowballs, water or anything else if this may cause danger or inconvenience to passers-by.' These are all examples of offences that do not immediately meet the *Engel* criteria, but which in more serious cases could be covered by the Criminal Code, e.g. a fight can develop into violence under § 244 of the Criminal Code. If the offence develops into a more serious case, it would then meet the *Engel* criteria.. If the situation does not meet the *Engel* criteria, the processing of personal data in relation to the fulfilment of tasks in the Public Order Regulation may still meet the scope of the LED if the purpose is to protect against or prevent threats to public safety. However, as mentioned above, for there to be a case of public safety according to the LED, there must be more serious circumstances, which, as a starting point, is hardly the case with the circumstances regulated in the Danish Public Order Regulation.

However, in many cases where the Public Order Regulation applies, the offence could also have been regulated in the Criminal Code and thus potentially fall under the rules of the criminal process, in only slightly more serious situations (Henricson, 2022, p. 172). This means that the police employees in the specific situations must assess whether the offence should be regulated by the criminal procedure and whether the offence should result in a fine or a prison sentence, and thus the processing of personal data in connection with this will be regulated by the LED.

When the police employee in the specific situation must decide whether the offence should be regulated by the criminal procedure rather than the Public Order Regulation, it is crucial:

- 1 whether the matter can be attributed to a punishable offence under criminal law or a special law;
- 2 whether, specifically and according to practice, a charge will be brought; and
- 3 whether the purpose of the intervention has been to prevent further criminal offences or to uncover a suspected criminal offence (Henricson, 2022, p. 33).

As mentioned, all the above factors argue in favour of the matter being regulated after the criminal proceedings, and thus any processing of personal data in connection with the performance of the task will also fall under the LED after the implementation of the LED in Danish law.

In those cases where the offence is not serious enough to fall under the Criminal Code and thus the criminal justice system, the question is whether any processing of personal data will still fall within the scope of the LED.

When implementing the LED in Danish law, the legislator decided, in accordance with the debate in the expert group around the adoption of the LED, that the offences that can lead to a fine or imprisonment in the Danish context constitute ‘criminal offences’ in the sense of the LED. This was because the prosecution of such offences is also handled in the criminal procedural system by general legal provisions, and failure to pay a fine may result in a commuted sentence in the form of imprisonment (see § 53 of the Danish Criminal Code; Legislative proposal L 168, p. 19).

The Danish legislator has thus chosen a pragmatic solution, so that the police do not have to decide whether their tasks are of a criminal nature according to the *Engel* criteria, but that as soon as the task falls under the criminal procedure, or that an offence may result in punishment in the form of a fine or imprisonment, the processing of personal data in connection with this will be regulated by the LED, which is implemented in the Law Enforcement Act in Denmark. This also applies to those activities that take place without prior knowledge of whether an offence constitutes a criminal offence. This means that the processing of personal data in connection with an investigation does not switch from the GDPR to the LED if it turns out during the investigation that the offence constitutes a criminal offence. It also means that many of the police’s tasks within the criminal justice system will be regulated by the LED.

As violation of the Public Order Regulation may result in a penalty in the form of a fine (§ 18), the processing of personal data in connection with the solution of these tasks will thus be covered by the LED.

Nevertheless, the legislator points out in the proposal for the adoption of the implementation that:

The question of the scope the directive in relation to the police’s tasks related to the maintenance of law and order will, however, have to be determined in practice, as the competent authorities’ performance of their tasks does not in all cases clearly fall within or outside this area. However, it must be

TANJA KAMMERSGAARD CHRISTENSEN

assumed that those parts of the police's maintenance of law and order that take place through the use of coercive measures and which otherwise have the direct aim of preventing or preventing threats to public order are covered by the Directive. Furthermore, police actions related to the maintenance of public order – which generally must be assumed to take place without prior knowledge of whether an act constitutes a criminal offence or not – will also be considered to be covered by the scope of the Directive.<sup>9</sup> (Legislative proposal L 168, p. 20)

The legislator recognises that the scope of the LED will have to be determined in practice, including practice from the CJEU, but for now chooses to include the tasks found in the Public Order Regulation within the scope of the LED. The fact that the legislator points out that the Public Order Regulation is covered, even though the Public Order Regulation is punishable by a fine, perhaps indicates that the scope of the LED is not entirely clear under Danish law either, which fits with the criticism of the LED discussed above.

#### 7.4.2 *The role of the police outside the criminal justice system*

For the role of the police outside the criminal justice system, it is no clearer when the LED and GDPR apply to the processing of personal data that takes place in connection with the police performing their tasks. The processing of personal data in connection with these tasks must either constitute a criminal offence or be related to the maintenance of public security to be regulated by the LED. It must therefore be assessed whether the tasks given to the police outside the criminal justice system are intended to put an end to potential criminal offences or whether the tasks are intended to ensure public safety.

According to § 2, nos. 1, 2 and 4-7 of the Police Act, the police have several tasks that are of a preventive, assisting or supervisory nature. These tasks are an extension of the police's primary tasks and include, for example, teaching and counselling, cordoning off a dangerous area, searching for the public, helping the sick and helpless, assisting with taking people home in connection with traffic accidents or drunk drivers, assisting supervisory authorities with their inspections, and much more. Many of these tasks, if personal data is processed in connection with their fulfilment, will be regulated by the GDPR. The police thus have tasks that are not regulated in the criminal justice system, and where it is obvious that the processing of personal data in connection with this will not be regulated by the LED.

---

<sup>9</sup> Author's own translation into English.

When implementing the LED, the Danish legislator also found that there were matters that would not fall within the scope of the LED, including complaints about police actions, which are regulated by administrative law rules or police visits and inspections of specific companies that carry out activities under specific licences, for example martial arts competitions. In addition, there are administrative cases, including cases concerning licences for offices or the processing of personal data in connection with employment, where it is assessed that the LED does not apply.

In summary, the scope of the LED in Danish law, as illustrated above, and at European level, is still not clear and, as mentioned, must be determined by the legislator in practice. However, at present, the Danish implementation of the LED stipulates that if an offence may result in a penalty in the form of a fine or imprisonment, the processing of personal data in connection with the prosecution thereof will be regulated by the LED, regardless of whether the offence meets the *Engel* criteria or whether it is a matter of 'public security'.

## 7.5 CONCLUSION

As stated in the introduction, the focus in this chapter was to assess the scope of application of the LED in relation to the police, with particular focus on the understanding of the concepts of criminal offence and public security. And the question was whether there could be derived a uniform understanding of the concepts at EU level.

As noted in the chapter, the material scope of the LED is not entirely clear, as was pointed out during the drafting of the LED and again during the evaluation of the LED. For the LED to apply, there must be a 'criminal offence' or 'public security', two concepts whose content is not yet clearly defined.

With regard to the concept of a criminal offence, the case law of the ECtHR and the CJEU has established some criteria for assessing whether an act can be considered a criminal offence. However, these criteria are still very open and may lead to different interpretations in different Member States, as the application of the criteria to determine whether the role of the police falls within the scope of the LED depends on a concrete assessment, which may differ from one Member State to another. This means that Member States may choose a solution, as in Denmark, where all offences punishable by a fine are covered by the LED, even if not all of these offences necessarily meet the *Engel* criteria.

The interpretation becomes even more open when it comes to the definition of public safety. Here, the CJEU has not yet provided a concrete interpretation of the concept, which leads to even greater uncertainty for Member States when assessing which roles of the police are covered by the LED.

The lack of a concrete definition of the concept is a problem in EU law, as the purpose of legislation at EU level is also to ensure uniform protection throughout the EU. If the

TANJA KAMMERSGAARD CHRISTENSEN

concepts are open to interpretation and left to the individual Member States, this could even lead to the entire scope of the LED being different in each Member State. It must therefore be crucial for the EU to define a more concrete scope of the LED in order to ensure that EU citizens receive the same protection of their personal data in the police sector in all Member States.

To illustrate the problem of lack of conceptual clarification, the chapter uses Denmark as a case study. In Denmark, the police have a number of tasks that were established long before the adoption of the LED. This means that it is not always easy to assess whether these tasks, and the associated processing of personal data, fall within or outside the scope of the LED. This issue was raised in the context of the preparatory legislative work for the implementation of the LED in Denmark. Here, the legislator decided that at present it must be the case that if a criminal offence investigated, detected or prevented by the police can result in a fine, then the processing of personal data in connection with that offence must be regulated by the LED. Denmark has thus chosen a pragmatic solution, which means that the LED will apply to a large part of police work.

If the LED applies to police work, it means that the area is regulated by EU law and therefore the Charter of Fundamental Rights will also apply. Whether or not the LED applies to the processing of personal data can therefore be of great importance in an area where Denmark otherwise has a legal reservation.

The conclusion must be that there are no clear guidelines as to when the LED applies to police work in Denmark. Even though the Danish transposition has established a broad scope for the LED, there may still be borderline cases where it must be specifically assessed whether the matter falls under the LED.

In order to get a clear understanding of the material application area for the LED, we currently have to wait for the CJEU to take a more concrete position on this. The current three cases that have been raised with the CJEU regarding the LED have not addressed this issue. Whether the EU legislator could have chosen a more precise wording to avoid interpretation problems is difficult to say, as the tasks of the police in the different EU Member States are different.

## REFERENCES

- Brewczyńska, M. (2022). A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation. In *Research handbook on EU data protection law, Elgar Online*, Edited by Eleni Kosta, Ronald Leenes, and Irene Kamara, 2022.
- Burton, D.W. (2013). *Research methods in law*. Routledge.
- Communication from the Commission to the European Parliament and the Council. First report on application and functioning of the Data Protection Law Enforcement

- Directive (EU) 2016/680 ('LED'). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0364>.
- European Data Protection Supervisor (EDPS), 'Opinion 6/2015 A further step towards comprehensive EU data protection: EDPS recommendations on the Directive for data protection in the police and justice sectors', 28 October 2015. [https://edps.europa.eu/sites/edp/files/publication/15-10-28\\_directive\\_recommendations\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/15-10-28_directive_recommendations_en.pdf).
- Henricson, I. (2019). *Politiloven – en status*. Tfk2019.297.
- Henricson, I. (2020). *Politiloven med kommentarer* (5th ed.). Jurist- og økonomforbundets forlag.
- Henricson, I. (2022). *Politiret* (7th ed.). Jurist- og økonomforbundets forlag.
- Kosta, E., & Boehm, F. (Eds.) (2023). *The EU Law Enforcement Directive – A Commentary*. Oxford University Press.
- Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 7 November 2016. <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3461&fromMeetings=true&meetingId=25283>.
- Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 18 January 2017. <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3461&fromMeetings=true&meetingId=25283>.
- Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 7 March 2017. <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3461&fromMeetings=true&meetingId=25283>.
- Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 4 May 2017. <https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3461&fromMeetings=true&meetingId=25283>.
- Sajfert, J., & Quintel, T. (2017). *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*. Available at SSRN: <https://ssrn.com/abstract=3285873>.
- Vogiatzoglou, P., & Fantin, S. (2019). National and Public Security Within and Beyond the Police Directive. In A. Vedder, J. Schroers, C. Ducuing & P. Valcke (Eds.), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Intersentia. Available at SSRN: <https://ssrn.com/abstract=3466821>.
- Vogiatzoglou, P., & Marquenie, T. (2022). *Assessment of the implementation of the Law Enforcement Directive*. Policy Department for Citizens' Rights and Constitutional

TANJA KAMMERSGAARD CHRISTENSEN

Affairs. [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL\\_STU\(2022\)740209\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf).

### *ECtHR case law*

European Court of Human Rights, 8 June 1976, *Engel and others v. the Netherlands* <https://hudoc.echr.coe.int/tur#%22itemid%22:%22001-57479%22>}}

European Court of Human Rights, 9 October 2003, *Ezeh and Connors v. the United Kingdom* <https://hudoc.echr.coe.int/eng#%22itemid%22:%22001-61333%22>}}.

### *CJEU case law*

Opinion of Advocate General Emiliou of 4 May 2023, Case C-683/21.

Opinion of Advocate General M. Campos Sánchez-Bordona of 20 April 2023, Case C-548/21.

*B. v. Latvijas Republikas Saeima*, C-439/19, Judgment of the Court (Grand Chamber), 22 June 2021.

*La Quadrature du Net*, C-511/18 and C-512/18, Judgment of the Court (Grand Chamber), 6 October 2020.

*Panagiotis Tsakouridis*, C-145/09, Judgment of the Court (Grand Chamber), 23 November 2010.

### *Law and orders*

Police Act: Lovbekendtgørelse 2019-11-29 nr. 1270 om politiets virksomhed. <https://www.retsinformation.dk/eli/lta/2019/1270>

Public Order Regulation: BEK nr. 511 af 20/06/2005 om politiets sikring af den offentlige orden og beskyttelse af enkeltpersoners og den offentlige sikkerhed mv., samt politiets adgang til at iværksætte midlertidige foranstaltninger. <https://www.retsinformation.dk/eli/lta/2005/511>

LED: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of

7 *WHEN DOES POLICE PROCESSING OF PERSONAL DATA*

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

Politikommisionens betækning om politilovgivning (Police Commission) (1410/2002). <https://www.betænkninger.dk/wp-content/uploads/2021/02/1410.pdf>

Lovforslag nr. L 168 (Legislative proposal L 168) Forslag til lov om retshåndhævende myndigheders behandling af personoplysninger, Folketinget 2016-17, [https://www.ft.dk/ripdf/samling/20161/lovforslag/l168/20161\\_l168\\_som\\_fremsat.pdf](https://www.ft.dk/ripdf/samling/20161/lovforslag/l168/20161_l168_som_fremsat.pdf)

Lovforslag nr. L 159 (Legislative proposal L 159) Forslag til lov om politiets virksomhed, Foketinget 2003-04, [https://www.folketingstidende.dk/samling/20031/lovforslag/L159/20031\\_L159\\_som\\_fremsat.pdf](https://www.folketingstidende.dk/samling/20031/lovforslag/L159/20031_L159_som_fremsat.pdf).



## 8 'FISHING' IN LARGE DATA LAKES

### *The Law Enforcement Directive in the context of Danish and Norwegian criminal procedure*

*Inger Marie Sunde, Tanja Kammersgaard Christensen and Lene Wachter Lentz*

#### **Abstract**

*Law enforcement authorities collect large amounts of data in the investigation of crimes. From a crime prevention point of view, such data could be stored and reused for other purposes; however, data protection considerations require that data are only gathered for specified purposes and not reused in a manner incompatible with those purposes. This chapter analyses to what extent law enforcement can reuse excess data, based on three different practical scenarios. First the EU Law Enforcement Directive as a framework is analysed, then two national legislations, Danish and Norwegian, are investigated. The conclusion is that there is a severe risk of establishing large data lakes for reuse for other purposes, and not yet adequate EU or national safeguards in place to ensure privacy, personal data and the fundamental right to be left alone.*

#### **8.1 INTRODUCTION**

In the investigation of crime, law enforcement authorities collect large amounts of digital data to be analysed in search of evidence. Usually, the data are collected under coercive powers, for example search and seizure, production orders, interception and computer monitoring.

Often only a small portion of the collected data is used as evidence in the original case (the case that gave cause for collecting the data). For example, in the *Einarsson* case less than 1% of the secured data were used.<sup>1</sup> However, the huge volume of data not assessed in the forensic analysis of the original case is a resource that could potentially be useful for other purposes. Change of purpose raises the question of the right of reuse of the data, a question addressed herein in the context of combating crime.

Data collected in criminal investigations are predominantly personal data, hence any processing must have clear legal basis, have a legitimate aim, respect the essence of those rights, and be necessary and not disproportionate in relation to the aim sought to

---

<sup>1</sup> *Sigurður Einarsson and others v. Iceland*, 39757/15, 4 June 2019. Of 20 million emails, 6,300 were used as evidence, i.e. 0.03 %.

be achieved (Articles 8 and 52 European Charter of Fundamental Rights,<sup>2</sup> and Article 8 European Human Rights Convention (ECHR)).<sup>3</sup> The protection of the right to respect for private life in Article 8 ECHR also covers the protection of personal data, i.e. areas such as data protection, data collection, right of access to personal information, data sharing, police surveillance, etc.<sup>4</sup> In a European context, the legal basis for reuse must be established in national legislation, subject to the conditions of the Law Enforcement Directive (LED).<sup>5</sup> The core requirements are Article 4(1)(b), stating that personal data must be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes, and Article(2)(b), stating that the processing for another purpose than that for which the personal data are collected shall be permitted insofar as the processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

The right of reuse by law enforcement authorities has been extensively analysed by König (2020),<sup>6</sup> Fedorova et al. (2022)<sup>7</sup> and Jasserand (2017; 2018),<sup>8</sup> with a focus on the conditions of non-incompatibility and necessity/proportionality set out in Article 4(1)(b) and (2) LED. The scholars seem to agree that the provisions are inadequate to impose any meaningful limitation on the national legislator. The present chapter shifts the focus to the matter of the term ‘collected’, as Article 4(1) and (2) refer to personal data ‘collected’ by the law enforcement authority, in conjunction with the proportionality condition. For Article 4(2) to be an effective limitation on reuse of data, we posit that ‘collected’ could be interpreted to take into account the forensic analysis performed after the data are secured by the law enforcement authority. Thus, the data available for reuse are those that were assessed by the forensic examiner in the lawfully conducted analysis, whereby they came to the examiner’s knowledge. In contrast, the data not assessed (‘excess data’) are not available for reuse.

The interpretation rests on the premise that personal data may only be secured and analysed by the law enforcement authority for a specific purpose, which in a criminal investigation should be defined by the suspicion the case is about. Ideally no more data than those relevant to this suspicion should be secured. Still, more data are secured,

2 Charter of Fundamental Rights of the European Union (2010/C 83/02).

3 Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005), 4 November 1950, with later amendments.

4 *Jacobs, White and Ovey: The European Convention on Human Rights* (8th ed. by Bernadette Rainey, Pamela McCormick and Clare Ovey), 2021, pp. 424-428.

5 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

6 M.E. König, *The purpose and limitations of purpose limitation*, PhD thesis, Radboud University, 2020.

7 M.I. Fedorova et al., *Strafvordelijken gegevensverwerking*, Radboud University Press, 2022.

8 C. Jasserand, ‘Law enforcement access to personal data originally collected by private parties: Missing data subjects’ safeguards in Directive 2016/680?’, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2017, 154-165; C. Jasserand, ‘Subsequent use of GDPR data for a law enforcement purpose: the forgotten principle of purpose limitation?’, *European Data Protection Law Review*, 2018, 2, 152-167.

due to the large amounts residing on the digital sources criminal investigators are faced with (e.g. cloud servers, multiple mobile phones, user accounts, etc.). Inevitably this leads to large amounts of data being secured as collateral to the evidence needed for the case. A forensic analysis might have to go through stages of data reduction, as illustrated in *Einarsson*, which describes how – in the forensic analysis – the ‘full collection of data’ was firstly reduced to ‘tagged documents’, subsequently to ‘documents that might have relevance to the case’, and finally to ‘evidence’ incorporated in the ‘investigation file’ (para. 16). Through the forensic procedure the examiner may thus – inevitably – get more knowledge about the data than is needed for the case. These assessed data should be deemed to be ‘collected’ and available for reuse, provided the conditions of Article 4(2) are fulfilled.

The excess data that were not transformed into knowledge seem to be in the custody of the law enforcement authority only because it was not possible to filter them out at the time when the data were secured. This makes it reasonable to exclude them from reuse as per a narrow interpretation of ‘collected’ in Article 4(2) LED. In this chapter we analyse this interpretation further both on the level of the LED and in the national law of Denmark and Norway. The topic thus concerns *law enforcement authorities’ right to reuse excess data*.

## 8.2 METHOD, THEORETICAL BACKGROUND AND RESEARCH QUESTION

The interpretation of Article 4(2) LED set out above was first suggested by Sunde (2023),<sup>9</sup> whose point is that the interpretation logically follows from the limitations and conditions laid down in the fundamental right to privacy as operationalised in criminal procedural law. Building on her work, the present chapter goes one step further and analyses the interpretation in relation to three practical scenarios, both on the level of the LED and in the context of Danish and Norwegian criminal procedural law and data protection law.

We believe the analysis to be an interesting read to a wider circle than the Scandinavian, as it shows the considerable discrepancy between the legal regulation in the two countries. This is thought-provoking considering that Denmark and Norway have a long-standing history of shared legal culture with many similarities in the ambit of criminal and criminal procedural law, and both have transposed the LED into their national law. It thus shows an important shortcoming of the LED in terms of achieving

---

9 I.M. Sunde, ‘To have or have not: Limiting the data available for subsequent use by the police’, *New Journal of European Criminal Law*, 2023, 14(4), 495-511.

its aim of horizontal harmonisation of data protection with a high level of protection across the EU/EEA family,<sup>10</sup> even between close legal cousins.

The questions concerning limitations of the right of reuse are important and urgent, as technological advancements within law enforcement authorities facilitate the interchange of data for various purposes. Consequently, there exists a natural inclination to refrain from deleting the data, instead opting to store them ‘just in case’. This could lead to the accumulation of vast lakes of personal data within law enforcement organisations, perpetually retained and potentially reused in ‘fishing expeditions’ for data in any criminal case, as well as for intelligence purposes, thereby rendering both rights of data protection and privacy insufficient.

In recent years, high-profile law enforcement operations such as Ennetcom, EncroChat, Sky ECC and Anon, where law enforcement authorities have taken control of communications networks, have attracted much scholarly attention.<sup>11</sup> However, to our knowledge these academic works have not delved into the limitations of the right of reuse as asserted in the present work. There is also an important difference of context, as the high-profile cases seemingly were carried out pursuant to general suspicions that the communications systems were predominantly tools for criminals; even the service providers could be deemed as criminals aiding and abetting the crimes planned, organised and sometimes performed through the communications system. These general suspicions justified law enforcement authorities taking control of communications systems, and securing the private communications data of thousands of individuals. Whether the initial operations whereby the law enforcement authorities gained control of the communications networks were performed as steps in criminal investigations or rather in preliminary stages to collect data that could give reason to open criminal investigations seems a bit unclear, but could have a bearing on the academic analyses.

The present chapter addresses criminal investigation concerned with *a specific suspicion*, for example a concrete situation of homicide, drug trafficking or domestic violence, where data typically are collected from the suspect’s mobile phone, laptop and cloud-based user accounts, or from a company server. As demonstrated by Sunde (2023), principles of purpose limitation and orientation create a framework within which the criminal investigation must be planned and performed, which also could have consequences for the right to reuse excess data.

10 The aim of a high level of protection is stated in recitals 4, 7 and 15 LED.

11 See e.g. J.J. Oerlemans & D.A.G van Toor, ‘Legal Aspects of the EncroChat Operation: A Human Rights Perspective’, *European Journal of Crime, Criminal Law and Criminal Justice* 30 (2022), 309-328, and R. Stoykova, ‘EncroChat: The hacker with a warrant and fair trials?’, *Forensic Science International: Digital Investigation* 46 (2023), 301602.

The research question, namely to what extent can law enforcement authorities reuse excess data, is analysed through three scenarios in which data can be reused for different purposes (Scenarios 1 to 3):

- 1 In a criminal investigation concerning economic crime, the investigator wants to use the digital forensic toolkit also to carry out a routine search for child sexual abuse material without prior suspicion. This scenario raises question about the legality of the access gained to the data extracted in the routine search and whether there are limitations to reuse these data.<sup>12</sup>
- 2 Investigators working on a different case might be interested in the full collection of data secured in the original case, hoping they might supply their investigation with relevant information.
- 3 The full collection of data in the original case could be stored with data collected in other cases. Analysis across different datasets could then enable law enforcement to detect unknown patterns and/or social relations, which is useful for building information positions that could give reasonable ground for initiating new investigations or impose crime preventive measures.

Scenarios 2 and 3 raise the question of whether excess data may be shared, or if only assessed data may be shared. The difference is that Scenario 2 concerns the same objective as the original case (criminal investigation), while the objective of Scenario 3 concerns intelligence/crime prevention. Both Scenarios 2 and 3 give rise to the central question 'When do excess data have to be deleted?', as deletion could be an effective measure for preventing further use and subsequent interference with data protection.

The legal analysis is performed in relation to the LED (section 8.3), and the corresponding regulation in Denmark and Norway (section 8.4). The research question of to what extent can law enforcement authorities reuse excess data is first analysed as a question about how the LED applies to Scenarios 1 to 3, before turning to the respective national legal regimes.

The analysis applies legal doctrinal method.<sup>13</sup> As the problem concerns law enforcement authorities' interference with data protection rights, the concrete wording of the LED and of acts in the national legal system weigh heavily as per the principle of legality. Due to scarcity of legal sources directly related to the present research problem, the interpretation must also seek recourse to principles of legal method concerning purpose orientation and reasonable outcomes.

---

12 The topic of detecting child sexual abuse (CSA) material is both nationally and internationally considered high priority, e.g. one of Europol's priorities, cf. the annual reports of the Internet Organised Crime Threat Assessment (IOCTA). The proposed EU draft regulation on CSA, 2022/0155(COD) would make it mandatory for communication service providers to scan private communications for child sexual abuse material and make the information available to law enforcement authorities.

13 Watkins, D., & Burton, D.W. (Eds.), *Research methods in law*. Routledge (2013) p. 9.

### 8.3 THE LAW ENFORCEMENT DIRECTIVE

#### 8.3.1 Introduction

The LED regulates the processing of personal data by law enforcement authorities, including the police. Its preamble states that the EU legislator was aware of the technological developments that took place in society, and affected police work (see recitals 3 and 4). It was still deliberately decided to keep well-established data protection principles intact and that ‘big data processes’ were to be deemed legitimate only when they conform with these principles.<sup>14</sup> This is important particularly with respect to the purpose limitation principle, which is essential because other principles depend on it.<sup>15</sup>

The research question set out in section 8.2 presupposes, in line with the interpretation suggested by Sunde (2023), a legal differentiation between assessed data and excess data in relation to the right of reuse. While Sunde derives this differentiation from a narrow interpretation of ‘collected’, one may ask whether it also might be derived from the principle of proportionality, a question which is analysed in the next section.

#### 8.3.2 Subsequent processing of personal data: Article 4(2) LED

As explained, subsequent use (or reuse) of ‘collected’ data is regulated in Article 4(2) LED. The provision relates to the principle of purpose specificity set out in Article 4(1)(b), according to which personal data may only be collected ‘for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes’. Importantly, the purpose set out in Article 4(1)(b) must be determined at the time when the data are collected (recital 26), which in a criminal investigation is prior to or at the time when the data are secured, at the latest. Use for any other purpose is deemed as subsequent use, regulated in Article 4(2)(b), which states that such processing must be ‘necessary for and proportionate to that other purpose in accordance with Union or Member State law’. The need for a legal basis in national law is reiterated in Article 9(1) LED. Furthermore, the other purpose must be one of the objectives listed in Article 1(1) LED (cf. Article 4(2)).

The question is whether the proportionality test in Article 4(2) makes it relevant to distinguish between assessed data and excess data. In relation to Scenarios 1 to 3, it is clear that the purposes represented in these scenarios fall within the objectives set out in Article 1(1) LED, thus this condition for subsequent use as per Article 4(2) is fulfilled.

<sup>14</sup> E. Kosta & F. Boehm (Eds.), *The EU Law Enforcement Directive (LED): A commentary*, Oxford 2024, loc. 8643.

<sup>15</sup> *Ibid.*, loc. 8727.

The crucial point is whether subsequent use of the data as set out in Scenarios 1 to 3 is necessary and proportionate (Article 4(2)). In *Inspektor v. Inspektorata kam Visshia sadeben savet*<sup>16</sup> (*Inspektorata*), where the Court of Justice of the European Union (CJEU) ruled among other things on the scope of Article 4(2), the purpose in that case changed from the investigation and detection of a crime, to the prosecution of a person. The CJEU noted that:

the scope of Article 4(2) is not limited to the processing of personal data in connection with the same criminal offence as that warranting the collection of those data. (para. 55)

As the data in question were all assessed, known and registered in the law enforcement system, the case did not raise an issue concerning reuse of excess data. However, the Court noted that when collecting personal data in connection with the investigation or detection of a criminal offence, the law enforcement authority will often be

required to gather any data that are potentially relevant to the determination of the acts constituting the criminal offence at issue at a stage where those acts have not yet been established. (para. 53)

The CJEU thus acknowledges that more data than ultimately necessary in the specific case may be collected. A consequence is that the law enforcement authority must also assess more data than ultimately proves to be necessary for the case.<sup>17</sup> The CJEU points out in paragraph 55 that data may be processed for a purpose other than that for which they were originally collected, *namely* for a better understanding of criminal offences, as mentioned in recital 27. It is not clear whether the word 'namely' is to be understood in the sense that the CJEU opens a wider application of subsequent use, as mentioned in Scenario 2 (*Inspektorata*, para. 55). However, as discussed immediately below, some conditions still apply for the subsequent use of data.

As regards subsequent use for intelligence purposes (Scenario 3), recital 27 LED offers some guidance, stating that it may be necessary for the law enforcement authority to use personal data collected for specific criminal offences in a broader context in order *to gain an understanding of criminal offences* and to link different criminal offences that have been detected' (emphasis added).

Obviously, assessed data may lawfully be used for this purpose. The preamble is silent on the issue of whether excess data should be treated differently from assessed

<sup>16</sup> CJEU, Case C-180/21, *Inspektor v. Inspektorata kam Visshia sadeben savet*.

<sup>17</sup> See Bonetto, G., 'The judgment of the CJEU in *Inspektor* (Purposes of the processing of personal data – criminal investigations) of 8 December 2022 and the concept of further processing under the Law Enforcement Directive', *New Journal of European Criminal Law* 2024 15(1), 58-71.

data in relation to subsequent use, and the issue seems not to have been brought before the CJEU. The interpretation of the word ‘collected’, i.e. whether it should be understood literally or be interpreted narrowly only to encompass assessed data, is still an open question. A narrow interpretation is reasonable, because in hindsight the excess data were evidently not necessary and ideally should not have been secured in the first place.<sup>18</sup> The interpretation could have support in the proportionality condition set out in Article 4(2)(b), as preventing excess data from being put to subsequent use would reinforce the principle of data minimisation. There is no doubt in the literature that the data minimisation principle sets limits on the use of personal data for new purposes. For example, as De Hert and Sajfert (2021, p. 14) put it:

the LED facilitates law enforcement data collection and subsequent processing immanent to the intelligence-led, big data policing. At the same time, it prevents law enforcement authorities from mass surveillance-type of collecting and processing personal data ‘just in case’.<sup>19</sup>

The authors of the assessment of the implementation of the LED<sup>20</sup> came to the same conclusion, stating that:

Suitability and effective contribution to the fight against crime alone cannot lead to a mentality of maximisation of information which would seriously interfere with fundamental rights.<sup>21</sup>

This means that the national law of the Member States may not permit law enforcement authorities to collect, process or store personal data ‘just in case’, but must ensure that the principle of data minimisation is respected. One way to achieve this is to apply a narrow interpretation of ‘collected’, as explained earlier. This would reinforce the principles of both proportionality and purpose limitation, as well as the principle of data minimisation.

Case law of the CJEU on data retention could provide further guidance for the proportionality assessment. The case law is relevant as retained data and excess data have in common that their necessity and relevance for the stated (future) purpose are

---

18 I.M. Sunde, ‘To have or have not: Limiting the data available for subsequent use by the police’, *New Journal of European Criminal Law*, 2023, 14(4), 495-511.

19 De Hert, P., & Sajfert, J., ‘The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680’ (16 December 2021), p. 14.

20 European Parliament, Directorate-General for Internal Policies of the Union, Vogiatzoglou, P., Marquenie, T., *Assessment of the implementation of the Law Enforcement Directive*, European Parliament, 2022.

21 European Parliament, Directorate-General for Internal Policies of the Union, Vogiatzoglou, P., Marquenie, T., *Assessment of the implementation of the Law Enforcement Directive*, European Parliament, 2022 p. 38.

unknown when they are stored. Concerning data retention, the CJEU has assessed whether personal data collected for national security purposes may be used also to combat serious crime, and vice versa. In *La Quadrature du Net and others*,<sup>22</sup> the Court thus held that access to data retained in the interest of safeguarding national security may not be made available for the purpose of prosecuting and punishing an ordinary criminal offence. On the other hand, data retained for the purpose of combating serious crime may be made available for safeguarding national security (para. 166).

The interpretation was further clarified in *G.D.*:<sup>23</sup>

Where those data have exceptionally been retained in a general and indiscriminate way for the purpose of the safeguarding of national security [...], the national authorities competent to undertake criminal investigations cannot access those data in the context of criminal proceedings, without depriving of any effectiveness the prohibition on such retention for the purpose of combating serious crime. (para. 100)

This indicates for Scenarios 1 to 2 that although the LED permits subsequent processing (analysis) of excess data collected in the investigation of a criminal offence, this may be done only when the other offence is at least as serious as the original offence. In relation to Scenario 1, this means that national law may authorise law enforcement authorities routinely to search for incriminating evidence, provided the search concerns an offence at least as serious as the original offence.

This does not solve the question of whether the LED permits subsequent use of excess data for intelligence purpose, as in Scenario 3. Fedorova et al. (2022)<sup>24</sup> and De Hert and Sajfert (2021)<sup>25</sup> assert that this cannot be the case, as it renders data protection almost illusory. Hence it must be contrary to proportionality as well as to the principle of data minimisation. Currently, the law on this issue must be regarded as unclear and contentious.

---

22 CJEU, C-511/18, *La Quadrature du Net and others*.

23 CJEU, C-140/20, *G.D. v. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*.

24 Chapter 3.2.1.

25 De Hert, P. & Sajfert, J., 'The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680' (16 December 2021).

### 8.3.3 *Deletion: Article 5 LED*

Data deletion or anonymisation may protect personal data from being put to subsequent use. The question is when obligations to delete or anonymise data become activated as per the LED. It follows from Article 5 LED that Member States must set appropriate time limits for the erasure of personal data, or for a periodic review of the further need for data storage.<sup>26</sup> The appropriateness of time limits in national law must be evaluated in light of Article 4(1)(c) and (e) LED, according to which erasure or anonymisation must be performed if the data are no longer necessary for the purposes for which they were processed.

In *Direktor na Glavna direktsia 'Natsionalna politisia'*,<sup>27</sup> it was pointed out that the LED does not require national law to set absolute time limits for the storage and deletion of personal data; rather, it ensures that this is limited to what is necessary for the purpose of storing the data. The case concerned storage of personal data in a Bulgarian police register, and it was pointed out that the data controller is obliged to periodically review whether further storage is necessary for the purpose (para. 72). National law must also specifically determine when the rights of the data subject require the deletion of the data (para. 52). In the judgment, the CJEU recognises that a time limit for erasure may be, for example, the death of the offender. However, the CJEU points out that such a time limit cannot be applied generally and indiscriminately but must be 'appropriate' to the specific circumstances (paras. 68-69). In other words, Member States cannot choose to retain all personal data collected until the death of the offender.

In the context of criminal investigation and prosecution, the storage time may be long, as the data might be needed until the investigation is finalised and the case conclusively resolved in court. This may take years. Until then, excess data are available to the original case, and from the discussion in the previous section it follows that they are also available to other cases provided they concern offences at least as serious as the original offence.

In relation to Scenario 3, it seems that assessed data may be registered and stored, while excess data must be anonymised. Excess data may thus primarily be used to deduce crime patterns (see recital 27 LED cited above).

<sup>26</sup> For an analysis of the Member States' different deletion deadlines see European Parliament, Directorate-General for Internal Policies of the Union, Vogiatzoglou, P., Marquenie, T., *Assessment of the implementation of the Law Enforcement Directive*, European Parliament, 2022, p. 38 with further references

<sup>27</sup> CJEU, C-118/22, *N.G. v. Direktor na Glavna direktsia 'Natsionalna politisia'*.

### 8.3.4 *Summary on the LED*

The LED does not directly address the issue in Scenario 1. The CJEU recognises that when the police collect personal data, they do not know what information is relevant and therefore more data than is necessary may be collected. These data may be analysed to assess their relevance to the original case. So far, the CJEU has not been asked to decide whether the data may also be used routinely to search for other incriminating material, nor does the LED contain any condition requiring that data processing must be suspicion-based. However, as a routine analysis will concern a different suspicion than the one that gave reason for securing the data, it must be deemed to be subsequent use, and the use of the information must be proportionate as per Article 4(2) LED. Cases handed down by the CJEU suggest that such subsequent use (analysis) must concern a crime at least as serious as the one that gave reason for securing the data in the first place. It means that national law regulating analysis of secured data as a routine, alongside the specific analysis performed in relation to the original purpose, must include a corresponding condition concerning the seriousness of the (other) crime, to comply with Article 4(2) LED.

The same assessment applies to Scenario 2. Here, the scenario is directly in line with Article 4(2) LED and therefore the criteria must be met in order for the police to have access to information from other cases. Again, it is particularly important that it is considered proportionate for the police to have this access.

Scenario 3 is further regulated in recital 27, which allows police to 'develop an understanding of criminal activities and to make links between different criminal offences detected.' Thus, if the police want to detect patterns, etc., this is permitted under recital 27 LED.

## 8.4 NATIONAL LAW IN DENMARK AND NORWAY

### 8.4.1 *Introduction*

In this section we address the national implementation of the LED in connection with national criminal procedural law to explore how the considerations for both crime prevention and prosecution are balanced with the individual's right to protection of personal data. Specifically, we will elaborate on how Scenarios 1 to 3 are treated in two different jurisdictions: Denmark and Norway. Despite both of these Nordic countries traditionally being inspired by similar regulations within criminal law and criminal procedure, significant differences in regulation occur.

#### 8.4.2 Denmark

##### 8.4.2.1 Law Enforcement Act

Denmark has implemented the LED in the Law Enforcement Act (LEA).<sup>28</sup> The LEA sets the framework for the processing of personal data by the Danish police and must be read in conjunction with the Danish Procedural Code (DPC). Based on the principle of the primacy of EU law, the LED and thus the LEA takes precedence over the DPC (Case C-6/64, *Costa v. ENEL*). Although the DPC, as illustrated below, allows for the collection of large amounts of data, if the data are personal, they must be processed – including used and stored – in accordance with the rules of the LEA, regardless of any rules in the DPC.

When implementing the LED in Danish law, Denmark chose to follow the wording of the LED closely. This was done in order to avoid any doubt about the implementation of the Directive's provisions.<sup>29</sup> This means that the wording of the Danish LEA is largely identical to that of the LED and that there are no further interpretative contributions to the understanding of the LEA in Danish law.<sup>30</sup>

The question of whether personal data can be processed for purposes other than those for which they were collected, must be answered based on sections 4 and 5 LEA, where section 4 contains the general rules for data processing, including the requirements for data minimisation, proportionality and accuracy, while section 5 sets out the conditions for further use.

In relation to Scenario 1 the question is whether the police may routinely search the secured data for child abuse, grooming, etc. This will initially require that this search is not incompatible with the original purpose (see section 4(3)), that there is a legal basis, and that the processing is necessary and proportionate in relation to the subsequent purpose (see section 5). In the legislative proposal for the LEA, it is assumed that section 5 provides a relatively broad scope for processing personal data for new purposes.<sup>31</sup>

The LEA thus provides that for a routine search of personal data collected for other purposes to be lawful, it must be authorised by law and be necessary and proportionate. The legal basis is thus not to be found in the LEA, and must be found in the DPC or other national legislation.<sup>32</sup> In cases where the search is made to combat more serious crime

<sup>28</sup> Law no. 410 of 27 April 2017.

<sup>29</sup> 2016/1 LSF 168 Proposal for the law on the processing of personal data by law enforcement authorities, p. 14.

<sup>30</sup> As the LEA is an implementation of the LED, there will naturally be overlap between the introductory section on LED and the answers to the questions below, also because there is currently no Danish case law that can help to understand the Danish interpretation of the area.

<sup>31</sup> 2016/1 LSF 168 Proposal for the law, p. 100.

<sup>32</sup> In Denmark, the police use a police system called POL-INTEL. POL-INTEL allows the police to perform transversal information analyses based on data from the police's various registers. The authorisation in the

than what the data was originally collected for, the search will probably be considered proportional (cf. section 8.3.2 about the LED). This means, that if it was considered proportional by a judge to collect the information for a less serious offence, then it will probably be proportional to reuse the information to solve a more serious offence.

It follows from section 7 LEA that appropriate deadlines must be set for deletion or regular review of the need for storage. A statutory routine search will thus have to take place in immediate connection with the collection of the computer, otherwise the information risks being deleted because it was not necessary for the original purpose. However, no immediate deadlines for deletion are established, apart from the deadlines laid down in the Notice regarding the Danish Criminal Register.<sup>33</sup> According to the Notice, the Danish Criminal Register contains one section for decisions on criminal matters (judgments, etc.) and another section for investigations, 'where information of significance can be recorded' (see section 6). Registration in both sections is subject to automated deletion processes, meaning that if not deleted earlier, information about a registered individual shall be deleted no later than two years after the physical person's death (section 10 of the Notice). The extensive storage period is most likely not compliant with the CJEU practice (see above Case C-118/22 in section 8.3.3).

The above must also apply to answering Scenario 2, if it is a specific case and there is an explicit purpose for using the personal data for this new purpose. This means that in cases where section 5 LEA is fulfilled, the data may be used in another case, with reservations for the DPC, as described below.

Regarding Scenario 3, it should be recalled that recital 27 LED acknowledges that the police may process personal data collected in connection with specific criminal offences, in a broader context in order to gain an understanding of criminal offences and link different criminal offences that have been detected. This must also apply to the LEA even though this is not specifically addressed in the Act.

#### 8.4.2.2 *Danish Procedural Code*

The Danish Procedural Code (DPC) regulates police interference in private life, freedom, communication, etc. Different requirements apply, depending on the severity of the crime; however, as a general rule, police interference requires a prior court order.<sup>34</sup>

The search of a suspect's mobile phone, computers, servers, systems or devices is regulated in sections 793-798 DPC. However, if the search is carried out secretly, stricter conditions apply in section 799. Regarding seizure, this is regulated in sections

---

POL-INTEL order (see in particular sections 4 and 5), is very broad, and the order will probably therefore also allow a routine search of personal data as mentioned in Scenarios 1 and 2. However, the final scope of the police's cross-cutting analyses of personal data in POL-INTEL is beyond the scope of this contribution.

<sup>33</sup> Notice no. 1860 of 23 September 2021 on processing of personal data in the Central Criminal Register.

<sup>34</sup> Interference in communication according to sections 780-788 DPC, and computer monitoring in Section 791 b, which are also important for collection of data, are left out in the following.

801-803(a). The regulation primarily aims at the physical deprivation of objects or the seizure of assets, with the purpose of securing evidence or assets relevant for the confiscation of proceeds from a criminal act or to cover the public authority's claim for legal costs.

In Danish criminal procedure, there is no consideration as to the specific time when data is searched and seized. In Denmark, when a computer, server, system, etc., is searched and seized, typically a mirror copy will be made, or data will be copied and secured on police servers, and only the physical objects will be confiscated in connection to the trial or returned to the owner. No particular regulation in the DPC applies to when the secured copy of the large amount of data will be deleted. During the investigation, there will be no restrictions on police searching data or securing a copy of the data, such as a requirement of a concrete suspicion. There is no Danish default model that large amounts of data can only be analysed based on search terms agreed upon in the particular case.<sup>35</sup> Hence, the Danish default is that Danish police can analyse all data they find, and in the case of large amounts of data, the method will most likely involve sorting the files in an inventory. The requirements in the LED that reuse of data be authorised by law and be proportional are thus not fulfilled by the DPC.

The only limitation to the reuse of data concerns the situation where findings related to a completely new criminal offence are to be used as evidence in court. This situation is known as 'incidental findings', not to be confused with the term 'illegal evidence', where the legal requirements for the initial search have not been fulfilled.<sup>36</sup> With incidental findings, the Danish police have carried out a legal search, and just happen to additionally or alternatively find evidence of other crimes – for instance, in a search no drugs were found as expected; instead, stolen goods were found. Danish regulation seeks to balance two considerations here. On one hand, the police must apply for a court order for the specific relevant crime and not try to gain a court order on a hidden agenda to investigate a less serious crime. On the other hand, evidence of a crime and criminal intent has been found, and the overall purpose of criminal procedure and investigation is to prosecute the suspects. According to section 800 DPC, first it must be established if the newly found evidence is related to a crime severe enough that it could have formed the basis for the interference itself. If so, then there will be no problem in the new case to use the evidence in court. If the new crime is not severe enough, the main rule is that such information can only be used in the investigation, for instance in relation to gaining other evidence. In relation to a secret search, the court may permit such evidence in court if the new crime investigated meets the conditions of the

---

35 As an exception, the court ruled a special procedure based on specific search terms out of consideration for journalistic source protection, U 2015.1249 H.

36 Section 800 was established by Law no. 411, 10 June 1997, based on the Committee's report 1159/1989, referring to 'incidental findings' in the preparatory work. A similar provision, section 789, established in 1985, covers such findings from interference in communication.

severity of the crime, etc., in section 800(2). No doubt, this regulation is rooted in the traditional situations where the police discover during the search evidence of another crime, and interference in communication where the police overhear communication about crimes. It would be too strict a regulation if the police were required to unsee or unhear what was actually found and clearly would be useful as evidence of crimes. And with good reason, this finding of evidence may be regarded as incidental.

However, the terminology is quite ambiguous when used in relation to search of large amounts of data, if the police routinely carry out data searches for other crimes than the one causing the searching and seizure in the first place. In this situation, it is not a question of unseeing or unhearing evidence already obtained by the police, but a deliberate choice to apply search tools that are relevant for other purposes than the actual crime. Such fishing expeditions cannot terminologically count as 'incidental'. However, 'incidental finding' was the popular term used when discussing and establishing the provision; it is not a term used in the wording of the provision.<sup>37</sup> From the wording of section 800, it would most likely be legal to carry out such fishing expeditions, and use of the evidence will rely on the question of whether the new crime is severe enough that it could, by itself, have formed the basis for the search. The conclusion is that there is no clear limit in the DPC to the police carrying out routine searches in all large volumes of data for, for instance, child sexual abuse material, and such findings may also most likely be used as evidence in court.

From a Danish perspective, based on both the LEA and the DPC, there are no limitations in Scenarios 1 to 3 regarding reuse of data from these data lakes. Firstly, there is no specific time limit after which data must be deleted, and secondly, there are no restrictions on how police can reuse such data for other purposes. The only limitation in place is, according to the DPC, if the new crime is not severe enough to justify a coercive measure itself. In such cases, the data cannot be used as evidence in court; it can only be utilised for further investigation, thereby revealing new evidence that can be used as evidence in court proceedings.

### 8.4.3 *Norway*

#### 8.4.3.1 *Introduction*

The LED is implemented in Norwegian law in the Police Databases Act (PDA),<sup>38</sup> applicable to data processing by 'the police and public prosecuting authority' (hereafter collectively referred to as 'the police') for the purpose of combating crime (section 3, first para.). In the context of a criminal investigation, the PDA is supplemented with rules

---

<sup>37</sup> See 1996/98 Proposal for a law and the Committee's report 1159/1989.

<sup>38</sup> Act of 28 May 2010 no. 16.

laid down in the Criminal Procedural Code (CPC),<sup>39</sup> and pursuant to section 225 CPC criminal investigation is the sole responsibility of the police.

Previously in this chapter, Scenarios 1 to 3 were analysed in relation to the principle of purpose specificity (Article 4(1)(b) and (2) LED) and storage limitation (Article 5 LED). It was also noted that the LED applies solely to the processing of personal data.

A first point to be made is that the material scope of the PDA is broader than that of the LED, as it encompasses all electronic data in the custody of the police, not only ‘personal data’. This is possibly in recognition of the wide-reaching scope of the notion ‘personal data’. By making the Act generally applicable to data, the practitioner does not have to determine whether data are personal or not in the concrete case. There is one material exception to this, i.e. section 7 PDA (special categories of data), which is obviously limited to covering personal data (defined in section 2 no. 1 PDA, corresponding to Article 3(1) LED).

#### 8.4.3.2 Purpose limitation

The principle of purpose limitation is laid down in section 4 PDA, which states that data may be processed for the purpose ‘for which they are collected and for other police purposes’. The expression ‘police purposes’ is a defined notion that corresponds to the objectives of the LED set out in Article 1(1) (section 2 no. 13 PDA). Literally, section 4 PDA says that data for instance originally collected for the purpose of investigating a crime (case A), may also be processed for the purpose of preventing crime (intelligence), or be used in a different criminal investigation (case B). However, the provision makes an exception when the right of reuse is limited by ‘statute or in pursuance of statute’.

At first glance, section 4 PDA seems quite straightforward, effectively providing for unhindered use of data across cases and purposes within police organisations, insofar as the objective is to combat crime. One should notice that section 4 PDA, in contrast to Article 4(1)(b) LED, does not apply the condition of non-incompatibility, thus taking for granted that the purposes encompassed by ‘police purposes’ always are compatible. Nor does it invite a discussion about the relationship between ‘purposes’ and ‘objectives’ such as for Article 4(1)(b) LED in relation to Article 1 LED (see e.g. Fedorova et al., 2022, section 3.2.1.2).

In relation to section 4 PDA, a question may be raised about the meaning of the word ‘data’ (the Norwegian authoritative text uses the word ‘*opplysninger*’, i.e. the plural of ‘*opplysning*’). Does ‘data’ mean *all the data initially collected*, or *the part of the data* that came to the knowledge of the police when the data were analysed for the original purpose, i.e. ‘assessed data’? As noted, in the age of big data, ‘assessed data’ may be a significantly smaller entity than ‘collected data’. If the correct interpretation is that the right to further use only applies to assessed data, a legal limitation flows directly

<sup>39</sup> Act of 22 May 1981 no. 25.

from section 4 PDA. Currently this is still an open question, but a discussion of the interpretative problem follows below.

Assuming the size of a dataset matters to the potential for relevant findings, the interpretation of 'data' in section 4 PDA is relevant to Scenarios 2 and 3. For instance, in relation to Scenario 2, the assessed data relevant as evidence in case A may not be directly relevant to case B, yet the *full dataset* may be of interest, for instance because it was collected from a person who is involved in both cases. As for Scenario 3 where the aim is to build an information position, the logic may be 'the more data available, the better'. There is a drive to equip the police technologically, especially after sharp criticism from the national Auditor General in 2023, asserting that Norwegian police had not adequately invested in high-tech capabilities.<sup>40</sup> It is also telling that the Police IT unit (PIT) is steadily being furnished with more resources to provide a 'digital foundation wall' (*digital grunnmur*) for seamless data processing across police districts, cases and purposes.<sup>41</sup>

#### 8.4.3.3 *Data collected in real time*

As noted, section 4 PDA includes the proviso that the right of further use may be limited by 'statute'. Such statute is laid down in section 216 i CPC, concerning data captured in real time in a criminal investigation by secret interception or computer monitoring. Section 216 i CPC states that 'everyone has an obligation of secrecy' in relation to data collected by these methods, though making exceptions for specific purposes set out in paragraphs a to k. Among the purposes included in the list are use of the data in the *investigation* of a case, and as *evidence* for an offence. These alternatives are treated differently.

Intercepted data may be used in any criminal investigation *to move the investigation forward* (section 216 i (a) CPC). To this end, there is no condition concerning the seriousness of the offence. The data may thus be used in the investigation of the original case and any other case, for instance to prepare interviews of suspects and witnesses. When the issue concerns use of the data as *evidence*, stricter conditions apply. The provision permits use of the data as evidence for the offence that gave reason for collecting the data (the original offence) (section 216 i (b)), and for any other offence sufficiently serious to give reason for use of interception or computer monitoring

40 Investigation by the Auditor General, report 3:5 (2020-2021), 'Undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT', sections 2.1.3 and 3.

41 Klepper, K.B. et al. (2021), Report 21/02532 of the Norwegian Defence Research Establishment, Recommendation #4: create 'a digital foundation wall' in the police. From 2021 to September 2023 the staff of PIT has been increased by more than 100 positions (Auditor General, report 3:7 (2023-2024), Appendix 2), and the police receives more funds from the national budget for ICT investments (Revised National Budget 2024, chapter 440, pp. 61-62).

(section 216 i (c)). This requires a statutory level of punishment of at least 10 years (Sections 216 a and 216 o).

The conditions related to use of the data as evidence are thus in alignment with the interpretation of the LED, where the conclusion was that further use of the data was permissible when the other offence was at least as serious as the original offence.

Section 216 i (d) CPC represents a deviation, as it permits real-time data to also be used as evidence for offences for which interception/computer monitoring *could not be used*, provided it is not deemed to be disproportionate according to a concrete assessment of the circumstances of the case. In addition, it must be shown that the investigation of the case would otherwise be substantially impaired. The reach of this provision is hard to determine given the lack of any authoritative decision,<sup>42</sup> a weakness recently recognised by the Attorney General in Criminal Matters.<sup>43</sup>

Finally, section 216 i CPC does not permit further use of real-time data collected in a criminal investigation for pure intelligence activities or crime preventive purposes, except when necessary for averting a crime (section 216 i (f)). Real-time data may thus not be used for the purpose mentioned in Scenario 3.

The Norwegian text of section 216 i CPC uses the word '*opplysninger*', i.e. the same as is used in section 4 PDA. The literal meaning of '*opplysning*' is to shed light on something, which implies that an '*opplysning*' must have come to the recipient's knowledge. Interception is historically a method whereby the police listen in to (and record) electronic communication. This could namely enable the police to act swiftly and descend upon the perpetrators *in flagrante*. By implication, '*opplysninger*' in section 216 i are presumed to be known to the police from the time when they are collected. To preserve equality of arms and the right of contradiction, the suspect is ensured a right of access to communication 'used' by the police, and to the intercepted communication as a whole from the time of issuance of an indictment (section 264 CPC and Supreme Court decision HR-2005-1489-A).

It sometimes happens that the police lack capacity to listen in on a running basis, hence the material accumulates to be analysed sometimes later. However, from the time of the indictment the right of access prevails irrespective of whether the content of the intercepted communication is analysed by the police or not (Supreme Court decisions HR-2005-1489-A; 2008-508-U). The law thus treats these 'data' as 'assessed'. This

---

42 Use of intercepted data was rejected by the Court of Appeal in a decision of 14 April 2023 (LB-2023-30228). Originally the criminal charge concerned corruption by a prison officer who allegedly smuggled smartphones to prisoners. This merited interception. The criminal charge was later reduced to concern negligence regarding a duty to prevent and report prisoners' use of drugs, an offence that could not merit interception. The Court of Appeal denied use of the evidence, a decision accepted by the public prosecutor.

43 Letter from the Attorney General to the Senior Public Prosecutors dated 1 March 2024, available on the Attorney General's webpage.

follows from the characteristics of the coercive method as such; whether the police in a concrete case actually did listen in is not relevant.

The CPC sets out an obligation to delete or bar data from further use once the original case is conclusively finalised (section 216 g CPC, in conjunction with section 50, third para. PDA). This prevents storage of data *in case they could become useful* in a future criminal investigation. Thus, for other criminal investigations to benefit from the intercepted/monitored data in the original case, they must be active when the original case is active.

Finally, a note on Scenario 1: this alternative is not relevant to data collected in real time, as the method of interception presumes that the material is disclosed forthwith.

#### 8.4.3.4 *Historical (stored) data (collected by search, seizure and production order)*

Historical (stored) data may be secured and used under the powers of search, seizure and production orders. The CPC does not provide a provision corresponding to Section 216 i for stored data, meaning that subsequent use is regulated by section 4 PDA. In consequence, the interpretation of 'data' (*'opplysninger'*) in section 4 PDA becomes crucial: *either* all data secured in a criminal investigation may be reused, *or* only data assessed in the original case.

The interpretative problem is not addressed in the preparatory works, there is no case law on the issue, nor is it addressed in academic works, save for Sunde (2023), who takes the view that the data not extracted in the forensic analysis (excess data) are not available for further use. As the argument goes, excess data – not being relevant to the case – should ideally not be secured in the first place, and practical difficulties in avoiding to secure it do not alter the fact that the data *in principle* should not be in the custody of the police. Legally, an obligation to delete data becomes effective once the data are not necessary to the case (section 6, first para., no. 3/section 50 PDA), hence excess data should be deleted. When the obligation is not complied with (for forensic reasons), the data must still legally be deemed inaccessible to the police. Thus, only data assessed in the original case may be used for the purposes mentioned in Scenarios 2 and 3.

With respect to Scenario 3, the outcome differs from the one concerning real-time data. This is due to the lack of a statutory limitation for reuse of seized data for intelligence purposes. However, for the processing, the conditions of section 5 no. 2 PDA apply, compelling the police to make a concrete assessment of the necessity of each '*opplysning*' in the seized data. This excludes the possibility of indiscriminate storage of the volume of information in its entirety.

#### 8.4.3.5 *Scenario 1: Purpose specificity*

Scenario 1 requires a closer look in the context of historical data. It concerns a situation that may be addressed in terms of both purpose specificity and the conditions for initiating a criminal investigation and use of coercive measures. The first perspective

concerns data protection; the other privacy (home and correspondence). To apply the principle of purpose specificity within the scope of one and the same case is unusual, yet has scholarly support: the Commentary to the LED states that ‘every purpose of processing should be detailed.’<sup>44</sup> This translates well into the procedural concept of a ‘criminal matter’ (in Norwegian: *‘straffbart forhold’*), which serves to *individualise* the crime. As demonstrated in relation to real-time data, section 216 i (c) and (d) CPC permit use of data as evidence for a different offence. Whether the offence is committed by the suspect in the original case or a different person is not relevant; what matters is the individualisation of the offence. Therefore, what is important is not whether ‘criminal matters’ are administratively organised by the police in one or more investigations; purpose specificity also applies across different criminal matters within a criminal investigation.

Norwegian procedural law does not deem historical data secured in the police’s storage media as by default seized. Seizure occurs first when data are assessed and deemed relevant to the case (section 203 CPC), and the public prosecutor *has declared* the data as seized (Section 205, first para. CPC). This is settled case law (Supreme Court decision HR-2018-1901-U, para. 17, with reference to cases back to 2011). The analysis performed to identify data to be seized is legally categorised as a ‘continued search’ (section 192 CPC; Supreme Court decision HR-2018-1901-U, para. 16), so named to reflect that it is performed in extension of the search that enabled the police to secure the data. The data analysis per se is therefore a coercive measure that must fulfil the conditions for search (section 192 CPC) and comply with the limitations specified by the judge authorising it (section 197 CPC).

The question is whether historical *excess data* may be analysed for evidence concerning other criminal matters (within the same investigation) than the one that justified the search. If the question is to be solved by resorting to section 4 PDA, the answer is negative, provided that ‘data’ is interpreted only to encompass assessed data. This conclusion *de lege lata* is uncertain.

However, if the question is to be resolved by resorting to aspects of privacy, other factors become relevant. Firstly, a criminal investigation shall be suspicion-based. This is expressed in section 224 CPC, which requires ‘reasonable ground’ to investigate whether a crime has been committed. The condition serves to protect citizens against arbitrary investigations. Secondly, section 226 CPC requires the investigation to be ‘purpose oriented’ and be limited to shedding light on the criminal matter at issue. The law thus requires each investigative step to be relevant to the suspicion that justified the opening of the criminal investigation as per section 224. In itself, this excludes the possibility to search excess data for information about criminal matters without prior

---

44 E. Kosta & F. Boehm (Eds.), *The EU Law Enforcement Directive (LED): A commentary*, Oxford 2024, loc. 8746.

suspicion. Thirdly, as the analysis of secured data is a continued search, 'probable cause for suspicion' (in Norwegian: '*skjellig grunn til mistanke*') is required, which implies that there must be at least a 50% likelihood of the criminal matter (section 192 CPC). This condition conclusively excludes the option of searching excess data 'just because it is possible'.

To stay within the limits of the law, the continued search (analysis) must be performed in a manner suitable for extracting information relevant to the suspicion that gave probable cause for the search. Should the investigator come across information indicating other criminal matters than the original ('incidental findings'), the prosecutor may decide to expand the investigation to also include these criminal matters. The Attorney General of Criminal Prosecution has emphasised that a continued search for evidence for this purpose requires not only 'probable cause' but also that the new criminal matter is of sufficient gravity to fulfil the legal conditions for search (section 192 CPC).<sup>45</sup> As the material conditions for performing a search are not very demanding, in practice there is wide scope for searching secured data within the ambit of one and the same investigation once probable cause is established.

Currently, Norwegian procedural law does not provide a legal basis for performing routine analysis in data absent a concrete suspicion.

## 8.5 COMPARATIVE CONCLUSION

Both Denmark and Norway have transposed the LED with no specific additional national features. As regards the right of reuse, both implement Article 4(2) LED. However, Norwegian procedural law distinguishes between data collected in real time (interception, computer monitoring) and data secured from devices with stored data. As regards real-time data, Norwegian procedural law specifies the purposes for which data may be reused and adheres to the principle of the LED that the other purpose must concern a crime at least as serious as the original. There is not a corresponding regulation for reuse of historical data, though an important limitation follows from the view that the forensic analysis is deemed to be a search, and hence must comply with the limitations applicable to the original purpose. This excludes the possibility of routine search for a different purpose (Scenario 1). The law permits the sharing (reuse) of historical data with another investigation (Scenario 2) and for intelligence purposes (Scenario 3), while at the same time imposing an obligation to delete data not necessary for the original case. This is a conflict that needs to be resolved by the legislator. Finally, as a forensic analysis

---

<sup>45</sup> Attorney General of Criminal Prosecution, 'The Legality Control with Coercive Measures – Relevant investigation purpose and proportionality – special comments related to search in drugs investigation.' *Open letter to Agder police district*, 9 April 2021. <https://www.riksadvokaten.no/document/patalemyndighetens-legalitetskontroll-med-tvangsmiddelbruk/> (visited 3 June 2024).

INGER MARIE SUNDE, TANJA KAMMERSGAARD CHRISTENSEN AND LENE WACHER LENTZ

is a search, Scenario 2 may only be performed if the conditions for search are fulfilled in the other case. As regards Scenario 3, although the data may be shared, there is a provision in the PDA that requires that all data registered for intelligence purposes must be assessed for their relevance and necessity beforehand. This excludes the possibility of bulk storage of excess data for intelligence purposes.

As for Denmark, the provisions on deletion of data are very broad and would most likely not fulfil the requirements laid out in recent CJEU practice, leading to a significant possibility of creating large data lakes. Furthermore, the unrestricted access for searching these data lakes for new purposes does not align well with LEA requirements, which presuppose a legal basis for data reuse and require proportionality. The restrictions in the DPC only refer to the reuse of data as evidence in court. The combination of large data lakes and a lenient framework for access with new purposes will result in the risk of actual fishing expeditions in the data lakes, as laid out in Scenarios 1 to 3.

## 8.6 SUMMARY AND FUTURE CHALLENGES

With the LED, the EU has aimed to balance considerations for crime prevention and prosecution with those of individual privacy and personal data. The question arises whether the EU has succeeded in constructing a ‘stronger and more coherent framework for the protection of personal data in the Union, backed by strong enforcement’, as intended according to recital 4 LED.

Traditionally, criminal law and criminal procedure have been core national domains, with Member States responsible for criminalisation and prosecution. However, in recent years, the EU has increasingly intervened in this legislative area. The LED should be viewed in this context, with the EU establishing fundamental principles for data protection within law enforcement authorities.

Recent EU judgments, such as those regarding the storage of personal data until the person’s death, which was found to be non-compliant with the LED and Articles 7 and 8 of the European Charter of Fundamental Rights, signal new directions in this field. More judgments are anticipated, as it is acknowledged that Member States’ national laws often lack robust protection of personal data within law enforcement authorities.

Illustrating with two jurisdictions, Denmark and Norway, we find that the storage of data in large lakes for future investigative purposes is feasible to a significant extent, particularly in Danish law. In comparison, Norwegian law has taken more significant steps toward data minimisation within criminal procedure. Nevertheless, the risk of establishing large data lakes is immediate and real. Both national and EU laws should do more to safeguard privacy, personal data and the fundamental right to be left alone.

## 9 ASSESSING INTERFERENCE

### *Disrupting computer-enabled crime under Articles 8 and 10 of the European Convention on Human Rights*

Carlos José Calleja

#### **Abstract**

*This chapter explores how disrupting computer-enabled crime would interfere with the rights to respect for private and family life and freedom of expression under Articles 8(1) and 10(1) of the European Convention on Human Rights. By conceptualising the aims and methods of disruption alongside the case law of the European Court of Human Rights, it identifies key questions and arguments pertinent to assessing potential interferences. The chapter observes that disruptive operations with the effect of blocking access to internet services used to transmit information might interfere with the right to impart and receive information under Article 10(1). It also notes that operations involving the structured interception and collection of information over which individuals have a reasonable expectation of privacy might interfere with the right to respect for private life and correspondence under Article 8(1). Furthermore, disruption targeting cognitive processes might impact the right to personal development and to establish relationships under Article 8(1), provided they reach a certain severity threshold and that the disruptive operation is not a foreseeable consequence of the misconduct. These findings represent an early effort to reflect on the implications for fundamental rights of adopting disruption as a method to counter computer-enabled crime.*

#### 9.1 INTRODUCTION

A number of countries in Western Europe are pivoting toward ‘disrupting’ computer-enabled crime in their latest strategies.<sup>1</sup> In the Dutch strategy for cybersecurity for 2022-2028, the ‘disruption (*verstoren*) of cybercriminals’ features alongside efforts to investigate and prosecute (National Coordinator for Counterterrorism and Security, 2022, p. 19). In the United Kingdom, ‘having the most disruptive effect on criminal activity’ is both part of the approach to deterring cybercrime and a measure of success (Government of the United Kingdom, 2016, pp. 48-49 at 6.2.5 and 6.2.6). The Cybersecurity Strategy

---

<sup>1</sup> This chapter employs a working definition of computer-enabled crime as criminal conduct, as defined by substantive law, whose execution relays on information and communication technologies (ICTs) (cf. World Bank & United Nations, 2017, pp. 76-77).

CARLOS JOSÉ CALLEJA

Belgium 2.0 – 2021-2025 makes ‘disrupting criminal cyberinfrastructure’ a strategic objective (Centre for Cybersecurity Belgium, 2021, pp. 27-28). The Danish National Strategy for Cyber and Information Security 2022-2024 establishes as a strategic objective to strengthen the police’s capabilities to ‘investigate and disrupt’ cybercrime (Danish Government, 2021, p. 21).

A similar trend can be observed in regional organs such as the European Union Agency for Law Enforcement Cooperation (Europol) (see e.g. 2021b; 2024), as well as international organisations such as the World Economic Forum (WEF) and the International Criminal Police Organization (Interpol). For instance, the WEF describes disrupting ‘cybercriminal ecosystems’ as a ‘more direct approach’ to deter perpetrators of computer-enabled crimes (World Economic Forum, 2020, p. 18). Similarity, leading, supporting and coordinating Member States to ‘effectively prevent, detect, investigate and disrupt cybercrime’ features as one of the objectives of Interpol’s Cybercrime Global Strategy (2022-2025) (emphasis added) (Interpol, 2022, pp. 1-2).

It seems evident that ‘disrupting’ is becoming a common way of defining how law enforcement agencies (LEAs) are expected to handle computer-enabled crime. That shift towards disruption in fighting computer-enabled crime raises, at the same time, the question of whether and to what extent disrupting *interferes* with fundamental rights established in the European Convention on Human Rights (the Convention) – particularly, the rights to respect for private and family life and freedom of expression under Articles 8(1) and 10(1). To the extent that they so interfere, disruptive operations will have to adhere to the criteria outlined in Articles 8(2) and 10(2) of the Convention to be considered as *justified* interferences. They will thus have to pursue one of the legitimate aims established in the Convention, have a basis in foreseeable and accessible laws, and meet the threshold of necessity within a democratic society. Otherwise, the interference will entail a violation of the rights in Articles 8(1) and 10(1) of the Convention.

This chapter is an early attempt at addressing the question of whether disrupting computer-enabled crime poses an interference with the rights in Articles 8(1) and 10(1) of the Convention. These provisions safeguard the rights to respect for private and family life and freedom of expression. I assume that these rights are likely to be interfered with by measures aiming at disrupting computer-enabled crime. However, the nature and extent of that interference remain to be spelt out. The overarching question is thus: *whether and to what extent would disrupting computer-enabled crime interfere with some of the rights in Articles 8(1) and 10(1) of the Convention?* Addressing that question presupposes, in turn, conceptualising the aims and methods of disrupting computer-enabled crime. Hence, the chapter also raises the following question: *which aims and methods characterise disrupting computer-enabled crime?*

In section 9.2 below, I conceptualise the methods of disrupting computer-enabled crime. Subsequently, in section 9.3, I provide an account of the aims of disrupting computer-enabled crime. The first set of interferences is discussed in section 9.4,

which looks at interferences with Article 10(1) of the Convention. Section 9.5, in turn, discusses interferences with Article 8(1) of the Convention. The particular case of interferences that have a cognitive effect on perpetrators is discussed in section 9.6. Section 9.7 concludes.

I answer the chapter's overarching question by interpreting Articles 8(1) and 10(1) of the Convention. I draw on how the European Court of Human Rights (hereinafter the 'Court') has interpreted these provisions in its case law, adapting those interpretations to the specific reality of disrupting computer-enabled crime. When it comes to characterising the reality of disruptive methods, I draw on previous works (see Clough, 2020; Collier et al., 2022; Hutchings & Holt, 2017). I complement these, however, with scholarship on international security (see Borghard & Lonergan, 2017; Kello, 2018; Liff, 2012; Sharp, 2017; Tate & Bates, 2022) and active cyber defence (see Healey, 2019; Healey et al., 2020; Herpig, 2021; Shackelford, 2019). The parallels between the narrative on disrupting computer-enabled crime and approaches to both cybersecurity and military strategy are indeed apparent. That line of scholarship is thus of help in conceptualising the aims and methods of disruption as applied to fighting computer-enabled crime.

This piece adds to the emerging body of literature on disruption as an approach to policing on the internet. As with any conceptualisation, it has the immediate advantage of clarifying our notion of disrupting as an approach to policing and distinguishing it from other phenomena. On the other hand, to the extent of my knowledge, this is among the first attempts at discussing whether and to what extent disrupting computer-enabled crime might pose an interference with fundamental rights in the Convention (cf. Schmitt, 2017 at Rule 35, paras. 2-3, 6-14; Clough, 2020, p. 62).

The assessment conducted here does not claim to be exhaustive, however. Other rights beyond those established in Articles 8(1) and 10(1) may also be implicated, and there are aspects of Articles 8(1) and 10(1) that this chapter does not discuss. The reader should instead expect a discussion of a number of specific issues. Neither is the aim to pass judgment on whether specific operations constitute an interference. The objective is instead to outline the questions and arguments that may arise in assessing whether and to what extent disrupting computer-enabled crime interferes with the rights in Articles 8(1) and 10(1) of the Convention. As a result, several questions will be left open. Overall, the virtue of this chapter should be seen as being an early attempt at pinning down some of the questions – most of them of first impression – and arguments introduced by adopting disruption as LEAs' method for tackling computer-enabled crime.

CARLOS JOSÉ CALLEJA

## 9.2 METHODS OF DISRUPTING COMPUTER-ENABLED CRIME

### 9.2.1 *The narrative around the methods of disrupting computer-enabled crime*

In 2008, a coalition of industry actors and security researchers – later known as the ‘Conficker Working Group’<sup>2</sup>– collaborated to target the Conficker botnet, made up of over 7 million malware-infected computers. Conficker was ‘sinkholed’: the Working Group repeatedly intercepted domain name system (DNS) requests from infected computers attempting to connect to Conficker’s command-and-control servers and rerouted traffic from within the botnet to servers that the Working Group controlled.<sup>2</sup> The effort ultimately prevented actors behind Conficker from transmitting commands to infected computers (see Kaska, 2012, pp. 23-31; for a technical overview of Conficker, see Werner & Leder, 2009).

Policy documents following the sinkholing of Conficker marked a seminal attempt to justify such operations based on their disruptive effects. A report by ICANN’s<sup>3</sup> Security Team measured the Working Group’s success in that it effectively ‘disrupted botnet command and control communications and caused Conficker malware writers to change their behaviour’ (Piscitello, 2010, p. 2). Interviewees in the report of The Rendon Group similarly reported almost unanimously their success in terms of slowing down the dissemination of the infection and creating obstacles to using the botnet that ultimately deterred actors behind Conficker (The Rendon Group, 2011, p. 31).

Ten years later, the WEF would advocate for disruptive methods as a necessary ‘paradigm shift’ in how private actors and LEAs address computer-enabled crime (2020, p. 18). The WEF described the approach as a form of disrupting ‘cybercriminal ecosystems that contain infrastructure and assets’ by focusing on ‘massively disabling malicious technical infrastructure’ (2020, p. 18). Belgium’s latest strategy similarly mentions disrupting the ‘criminal cyberinfrastructure’ (Centre for Cybersecurity Belgium, 2021, p. 28). The United Kingdom uses similar language. The strategy for 2016-2021 mentions dismantling cybercriminals’ ‘infrastructure and facilitation networks’ (Government of the United Kingdom, 2016, p. 47). The 2022 strategy continues this approach, referring to targeting ‘cybercriminal infrastructure’ (Government of the United Kingdom, 2022, p. 104). Europol’s Cybercrime Centre, a year after its launch, similarly reported its orientation towards assisting Member States and partners in ‘fighting’ the ‘facilitating factors of the digital underground economy’, among which it counted: (1) ‘the infrastructure, including market places’; (2) ‘criminal services that

<sup>2</sup> Sinkholing consists of intercepting and redirecting malicious traffic from infected computers to a controlled server (see e.g. Stone-Gross et al., 2009).

<sup>3</sup> ICANN is an acronym for the Internet Corporation for Assigned Names and Numbers.

enhance cybercrime'; (3) 'the anonymous payment systems'; and (4) 'the main criminal networks that operate (in) the underground economy' – all in order 'to address the nature of criminal cooperation' (2014, p. 30).

Disrupting cybercrime thus appears to be some form of targeting or disablement. It has as its object an internet infrastructure loosely categorised as 'malicious' or 'criminal' or as a 'facilitation network'. These narratives beg the question of what methods disruption would cover – terms such as 'disabling' or 'disrupting' are hardly explanatory. Similarly, references to 'cybercriminal ecosystems' or 'criminal cyberinfrastructure' leave open questions about what exactly is being targeted – what makes up the (cyber) infrastructure or ecosystems which LEAs seek to disable or disrupt? Moreover, what makes that infrastructure or ecosystem '*criminal*' or '*malicious*'?

### 9.2.2 *Conceptualising the methods – degrading, disrupting and disabling*

There are notable parallels between the language in the policy documents mentioned above and the terminology employed in cyber defence. For example, the United States' Joint Publication 3-12 on Cyberspace Operations defines a 'Cyberspace Attack' as actions aimed at creating visible 'denial effects' in cyberspace, such as 'degradation, *disruption*, or destruction' (emphasis added) (Chairman of the Joint Chiefs of Staff, 2018, p. IV-7). Sven Herpig offers a similar definition in a policy brief on 'active cyber defence' that he has authored, describing it as the use of 'technical measures' to '*technically neutralise* and/or mitigate the impact' of an 'ongoing malicious cyber operation or campaign' (emphasis added) (Herpig, 2021, p. 11). Similarly, Jason Healey, Neil Jenkins and J.D. Work define 'disruptive counter-cyber operations' as proactive measures to defeat a specific cyber adversary by '*disrupting an adversary's technology*' (emphasis added) (Healey et al., 2020, p. 253). The similarity in language suggests that the approach of disruption as an approach to handle computer-enabled crime borrows methods known in cyber defence and adapts them to address criminal activities.

Given that similarity, the scholarship around cyber defence operations can help conceptualise what 'disrupting' or 'disabling' might mean in the context of addressing computer-enabled crime. That scholarship limits the notion of 'disrupting' to methods that cause some type of *effect* on either data residing in or processed by a computer system, the computer system itself or the network of interconnected computers (Liff, 2012, p. 405 at n. 409; Smeets, 2022, pp. 14-16).<sup>4</sup> These effects are typically *detrimental* to either the data residing in the system or the expected functioning of targeted computers

<sup>4</sup> The notion of networks, computers and data residing in them is in the context of this chapter interchangeable with the notion of information and communication technologies (ICT(s)) (see World Bank & United Nations, 2017, pp. 76-77).

CARLOS JOSÉ CALLEJA

or networks. Disrupting does not seek to improve the security or resilience of systems at risk of being targeted; instead, it seeks to have an adverse effect on the systems, network and data that might be used in committing such crimes (see Healey et al., 2020, p. 254; Herpig, 2021, p. 12). In short, disrupting consists of causing a detrimental effect on the networks, computers and data – or all of them – that perpetrators might employ (Liff, 2012, p. 405 at n. 409; Smeets, 2022, pp. 14-16).

Depending on the intensity of the effects, it is possible to distinguish between three types of disruptive operations. The first is *degradation*, which includes methods that operationally limit a system without completely denying access or preventing it from functioning (Chairman of the Joint Chiefs of Staff, 2018, p. II-7). An example would be changes to the software to slow down a server to hinder certain activities while still allowing some level of operation. Second, *disruption*, strictly speaking, is sometimes reserved in the literature for methods that deny access or prevent a system from functioning *for a period*, after which the system might be returned to its previous functioning (Chairman of the Joint Chiefs of Staff, 2018, p. II-7). For example, LEAs might temporarily disconnect a computer from the internet. The third and most intense form – *disabling* – involves completely and irreparably denying access to a system or infrastructure, rendering it non-operational (Herpig, 2018, p. 19; Chairman of the Joint Chiefs of Staff, 2018, p. II-7).

Closely related to that distinction is the concept of ‘reversibility’ of measures (Herpig, 2018, p. 17). Reversibility refers to the ability to undo the effects of disruptive operations, specifically to restore systems to their pre-operation state. An operation might be more or less reversible depending on whether it can be rolled back or deactivated without causing lasting damage (Deeks, 2020, p. 4; Herpig, 2018, p. 19).

### 9.2.3 *Conceptualising the infrastructure targeted*

Conceptualising the (cyber)infrastructure or ecosystems that law enforcement aims to disable or disrupt requires an additional distinction. It is possible to distinguish between information and communication technologies (ICTs) that are part of perpetrators’ internal infrastructure, on the one hand, and systems on which perpetrators merely rely, which might belong to innocent third parties, on the other (Herpig, 2018, p. 19). The former category includes the perpetrators’ own computer systems and devices, whereas the latter encompasses compromised third-party computers or internet services such as DNS or servers provided by hosting providers.

That distinction allows an understanding that a state’s definition of the (cyber) infrastructure can vary, ranging from narrowly focusing on the ICTs that are part of the perpetrator’s infrastructure to also broadly encompassing systems on which perpetrators rely but do not necessarily own or exclusively operate. For example, a state’s decision to target a botnet might involve assessing whether to disrupt the command-

and-control servers directly operated by the perpetrators or to mitigate the impact by eradicating the malware from compromised third-party systems used in the botnet (see e.g. Threat Intelligence Team, 2021).

Regardless of the scope chosen, any conceptualisation of infrastructure must acknowledge the potential for collateral effects on other ICTs – that is, unintended adverse effects on systems not directly targeted by an operation (Herpig, 2018, p. 28; Shackelford, 2019, pp. 390, 399, 488). Indeed, given the interconnectedness of ICTs, disruptive operations can affect systems beyond the intended targets (see Romanosky & Goldman, 2017). For instance, Sven Herpig discusses the possibility that cyber defence operations using malware-removal software to eradicate malware from infected computers may cause detrimental effects on a number of systems (Herpig, 2018, p. 28). Additionally, there are known cases of sinkholing a botnet that incidentally blocks access to legitimate websites (see Ragan, 2014). Furthermore, disconnecting a server from the internet might also disrupt legitimate services hosted on the same server. Overall, even operations narrowly targeting the perpetrator's internal infrastructure carry the risk of unintendedly affecting other interconnected systems.

#### 9.2.4 *Disrupting computer-enabled crime at a cognitive level*

There is, however, a subset of disruptive operations that do not target the technical infrastructure but operate at what seems to be a cognitive layer. This layer encompasses users' digital representations and the relationships and communities they establish on the internet – such as internet forums and social networks (cf. Chiefs of Staff, 2022, pp. 7-9; Chairman of the Joint Chiefs of Staff, 2018, p. I-4). Operating at this cognitive level involves influencing individual perceptions (see National Cyber Force, 2023, p. 14). LEAs might, for example, seek to instil mistrust among participants in online communities by revealing the agency's presence or control over websites or forums.

Two forms of cognitive interventions can be distinguished based on the literature on policing organised crime. Firstly, LEAs may disseminate information, accurate or otherwise, to cast doubt on the idea that crime can be performed with impunity. Secondly, LEAs may sow suspicion among online community members (Tilley, 2016, pp. 162-165). The Police2Peer initiative is an apposite example of the first approach. Under this initiative, LEAs across Europe will generate files with names that mimic child abuse material and release them on peer-to-peer networks for those seeking such content. Upon downloading one of those files, the individual will instead get a file featuring a police officer from any of the states adopting the initiative. The officer will be holding a placard stating that the individual has connected on the peer-to-peer network to the LEA's computer, that their IP address, username and list of shared terms might be visible, and that the information might be forwarded to their local police force (see Europol, 2021a)

CARLOS JOSÉ CALLEJA

As a third possibility, LEAs might employ influencing tactics to steer potential perpetrators towards specific behaviours (Collier et al., 2022, pp. 117-120). Ben Collier et al. (2022) document a comparable policing strategy aimed at combating the market for denial of service (DoS) attacks. This approach utilises targeted advertising to deliver specific messages to users searching for terms associated with DoS attacks to try to exert influence on their choices (Collier et al., 2022, pp. 117-120). This approach, which has been termed ‘influence policing’, shares similarities with strategies used in countering online radicalisation (Collier et al., 2022, p. 118; cf. Qurashi, 2018).

### 9.3 AIMS OF DISRUPTING COMPUTER-ENABLED CRIME

#### 9.3.1 *Increasing costs and mitigating harm caused to victims*

Disrupting cybercrime seems to have two different aims: first, raising costs and risks of computer-enabled crime while reducing rewards, and second, mitigating harm caused to victims.

The first rationale features a number of strategies. The WEF’s Partnership Against Cybercrime report of 2020 characterises disruption as a particular way of making cybercrime more costly and less attractive (World Economic Forum, 2020, p. 18). Similarly, Belgium’s Cybersecurity Strategy indicates that ‘disrupting’ certain ‘criminal cyberinfrastructure(s) *partially undermines the criminal’s business model*’ (emphasis added) (Centre for Cybersecurity Belgium, 2021, p. 28). The United Kingdom makes parallel claims. The National Cyber Security Strategy for 2016-2020 already established the need to ‘raise the cost, raise the risk, and reduce the reward of cyber criminals’ activity’ (Government of the United Kingdom, 2016, p. 47). The 2022 strategy seems to continue that approach: by 2025, disrupting will make it ‘*more costly and higher risk* for state, criminal and other malicious cyber actors to target the UK’ (emphasis added) (Government of the United Kingdom, 2022, p. 104 at para. 181). How the United Kingdom’s strategy assesses previous efforts sheds further light on the rationale behind disrupting. It indeed establishes that previous efforts ‘have not yet fundamentally altered the risk calculus of attackers who continue to successfully target the UK and its interests’, partly, it seems, a consequence of new capabilities to evade mitigation, easier access to attack infrastructure and higher potential rewards from attacks (Government of the United Kingdom, 2022, p. 100 at para. 169).

In addition to increasing costs, mitigating harm to the victims also appears to be an aim in some strategies. Outside Europe, in the United States, that rationale is indicated with particular clarity. The Department of Justice instructs investigators, attorneys and other agents to ‘consider whether taking such actions (i.e., disruptive measures) could mitigate ongoing harm posed by the actors, such as by changing their risk-reward calculus, by otherwise protecting victims, or by making victims whole after having

suffered an attack' (Department of Justice, 2022, p. 10). Victims are also mentioned in the Netherlands. In her letter to the House of Representatives of November 2022 on an integrated approach to cybercrime, the Minister of Justice and Security established that 'where detecting and/or prosecuting cybercriminals is not feasible or proves insufficiently effective, disrupting criminal processes is an alternative or additional method *to limit damage to citizens and companies*' (Yesilgöz-Zegerius, 2022, p. 5).

### 9.3.2 *The rationale that underpins disrupting computer-enabled crime*

Disrupting cybercrime seems to obtain its rationale from elements of disruption-oriented policing in organised crime. The idea of disruption-oriented policing has its origins in the adoption of an intelligence-led model of policing to fight organised crime (see Ratcliffe, 2016; Tilley, 2016). In a disruption-oriented mode of policing, the object of the intervention is the network, market or organisation, not the offender as an individual (Innes & Sheptycki, 2004, pp. 13-14; Skidmore, 2023, p. 5; Tilley, 2016, p. 159). The type of intervention consists of proactively exploiting vulnerabilities in that network, market or organisation to make it difficult or even impossible for other actors in the network to engage in criminal activities and thereby mitigate harm to victims (Innes & Sheptycki, 2004, p. 17; Tilley, 2016, p. 157).

Analogous to participants in a network, market or organisation, perpetrators are thought of as dependent on a network made of computers interconnected over the internet and data residing in them. Degrading, disrupting or altogether disabling that network is an effective way of making it hard for those perpetrators to act and of reducing the harmful consequences for victims. Similarly, transmitting information, stimulating suspicion among participants or using targeted messages to nudge actors can act as a method to hinder computer-enabled criminal activities.

Others have rightly shed light on the similarities between disruption-oriented policing in dealing with organised crime and disruptive approaches to computer-enabled crime (Clough, 2020; Collier et al., 2022; Hutchings & Holt, 2017). The literature on international security studies could further help add nuance by distinguishing between two aims of exerting force over the internet: *coercion* and *brute force*. An actor might seek to *coerce* an adversary by inflicting a limited amount of damage on the targeted network – combined with the threat of additional harm if demands are not met. Coercion is, in this context, a negotiation in which an actor promises to refrain from inflicting (further) harm if the target agrees to meet the demands made. Alternatively, an actor can exert *brute force* not to compel an adversary into a negotiation but to directly weaken their ability to behave in a specific way (Borghard & Lonergan, 2017, pp. 453-454; Liff, 2012, pp. 404-408; Sharp, 2017, p. 902). In the same way, LEAs can impose costs on computer-enabled perpetrators to the point that it is difficult to participate in the network and thereby engage in criminal activities – that is, they could

CARLOS JOSÉ CALLEJA

aim at coercing them. Alternatively, they could neutralise their capabilities – which would qualify as a form of brute force. While coercion will serve the aim of increasing the costs of computer-enabled crime, the aim of protecting victims seems better served by exerting brute force.

#### 9.4 INTERFERENCE WITH THE RIGHT TO RECEIVE AND IMPART INFORMATION IN ARTICLE 10(1) OF THE CONVENTION

##### 9.4.1 *The Court's case law on the right to receive and impart information in Article 10 of the Convention – blocking means of disseminating and receiving information*

Article 10(1) of the Convention establishes that ‘everyone has the right to freedom of expression’, which includes the ‘freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.’ The Court has consistently held that restricting access to the *means of disseminating information* amounts to an interference with the right under Article 10(1) to receive and impart information. The Court recognises, in particular, the internet as a crucial means for accessing and sharing information, as well as a means for participating in political discussions and engaging with matters of public interest (*Ahmet Yildirim v. Turkey*, para. 54; *Times Newspapers Ltd (Nos. 1 and 2) v. the United Kingdom*, para. 27). Consequently, the Court has ruled that measures blocking access to services on the internet can interfere with the right to receive and impart information.

The Court seems to distinguish in these cases between individuals who actively manage a site or use the internet to disseminate information and those who are mere recipients of information (*Cengiz and others v. Turkey*, para. 50). For the former, measures resulting in blocking access constitute an interference with their Article 10(1) rights. In *Ahmet Yildirim v. Turkey*, the Court found an interference when a measure that blocked all access to Google sites had the incidental effect of blocking access to the specific website the applicant used to publish academic works and views on a range of topics (*Ahmet Yildirim v. Turkey*, para. 55). A measure blocking access to an internet protocol (IP) address that resulted in the inaccessibility of a Russian website sharing the same IP address was also deemed to interfere with the website administrator’s rights under Article 10 (*Vladimir Kharitonov v. Russia*, paras. 33-36). In *Cengiz and others v. Turkey*, the Court held that incidentally preventing access to YouTube interfered with the rights of university professors who relied on the platform to receive *and impart* information (*Cengiz and others v. Turkey*, para. 52).

Conversely, blocking services that individuals use solely to receive information does not automatically constitute interference (*Akdeniz v. Turkey*, paras. 19-27). The Court seems to consider two additional factors in these cases. First, it assesses whether the

information can be ‘easily’ accessed through alternative means (see *Cengiz and others v. Turkey*, para. 51). If alternative means are available, the measure might not interfere with Article 10 rights. For example, in *Akdeniz*, where applicants could access musical works through other means despite website blocks, the Court found no interference (*Akdeniz v. Turkey*, para. 25). Conversely, in *Cengiz* the Court based its conclusion that there was an interference with Article 10(1) on YouTube’s ‘unique characteristics’ as a means for sharing information, and the lack of a comparable alternative (*Cengiz and others v. Turkey*, para. 52). Second, the Court considers whether the measure deprives the applicant of an essential means to participate in public debate (*Akdeniz v. Turkey*, para. 26). Where that is the case, the Court seems inclined to find interference with the right to access information.

In both scenarios, the specific targeting of the blocked service by the measure is immaterial to the Court’s assessment. What matters is whether the measure *effectively results* in preventing access to a service, regardless of whether this effect is incidental (see *Ahmet Yildirim v. Turkey*; *Vladimir Kharitonov v. Russia*).

#### 9.4.2 *Disrupting computer-enabled crime as an interference with the right to receive and impart information in Article 10(1) of the Convention*

The central concern under Article 10(1) is thus whether disrupting computer-enabled crimes results in blocking access to services used for information exchange. This encompasses both intended outcomes and unintended collateral effects. In each case, the consideration is whether the measure ultimately leads to blocking access to a service, irrespective of the intention of the specific LEA.

Consider the following scenarios:

Scenario 1: An agency requests the top-level domain name registrar to alter the resolution settings, intending to sinkhole traffic from botnet-infected computers. This operation inadvertently prevents countless users from accessing websites used to share blogposts for several days.

Scenario 2: An agency discovers that a popular file-sharing website is being used to distribute illegal content. To disrupt this activity, the agency instructs the internet service provider (ISP) to block access to the IP addresses associated with the website. While this action effectively prevents access to illegal content, it also prevents customers of that ISP from accessing the site for file-sharing purposes.

Scenario 3: An agency implements bandwidth throttling on a streaming platform used for illegal content distribution. By significantly reducing the available bandwidth, the agency aims to discourage large-scale piracy activities. While the platform remains accessible, users experience slowdowns and buffering issues, diminishing the quality of service and effectiveness of illegal distribution.

CARLOS JOSÉ CALLEJA

The first question under Article 10(1) is whether the measures result in blocking a means of disseminating information. It could be argued that measures in Scenario 2 effectively block access to the file-sharing website since customers of the ISP implementing the order will be, as a matter of fact, unable to access the website. In contrast, it is debatable whether measures such as those in Scenario 1 entail an interference. These measures impede the resolution of a domain name, preventing the site from being accessed directly through its domain name in a web browser. However, they do not block access to the site. Domain names merely serve to translate specific IP addresses into names that are easy to remember. Therefore, obstructing this translation does not preclude access to the website; users can still access it by entering the IP address directly into a browser. It could be nonetheless argued that the IP address may not be readily known by individual users, the measure thus having in practice an effect analogous to blocking a service. It would not be unreasonable to view this instance as also involving some form of interference.

Less clear are those cases such as the one described in Scenario 3, where disruptive operations do not lead to disabling or disrupting – i.e. blocking – a service but merely *degrade* access by slowing it down. The argumentation above can also be applied in this case. In this sense, there will be an interference only insofar as degrading the service has the effect of *preventing* individuals from accessing a service that is a means of disseminating and receiving information. Since individuals might not be prevented from accessing the service despite its suboptimal functioning, one could argue that the effects fall short of an interference with Article 10(1). In this case, it might nonetheless be helpful to complement the consideration of the ease of access with an assessment of the *reversibility* of the measure. Measures that cannot be easily undone might degrade the functioning of a service for a length of time such that its users are deterred from accessing it. This criterion might thus facilitate determining whether measures such as those described in Scenario 3 have the effect in practice of blocking access to a certain means of disseminating and receiving information.<sup>5</sup>

The second question is whether the effects on internet service have an impact on an individual disseminating information or merely affect individuals who use a service to receive information. There will arguably be an interference where the effects concern an individual's reliance on a service to transmit information. Where it is instead the case that the individual is a mere recipient of information, it might be necessary to consider the two additional questions described above, namely the ease of accessing alternative means of information and the importance of the website for an individual's participation in a general debate. Where both conditions are met, preventing access to

---

<sup>5</sup> A different question is whether and to what extent illegal forms of expression will be protected under Article 10(1) of the Convention, in particular whether they are such that they should be excluded altogether from the scope of the right under Article 17 (see Harris et al., 2023, pp. 608-609).

the service might also interfere with an individual's right to access information over the internet.

## 9.5 INTERFERENCE WITH THE RIGHT TO RESPECT FOR PRIVATE LIFE AND CORRESPONDENCE IN ARTICLE 8(1) OF THE CONVENTION

### 9.5.1 *The Court's case law on the right to receive and impart information in Article 8(1) of the Convention – reasonable expectation of privacy*

This section discusses the extent to which disrupting, disabling or degrading a service interferes with the rights enshrined in Article 8(1) of the Convention. This analysis focuses on the direct impact on ICTs, irrespective of any intelligence collected before or after such disruption. The issue is whether and to what extent effects on the network, computer systems or data residing in them amount to an interference with Article 8 of the Convention.

According to Article 8(1) of the Convention, everyone 'has the right to respect for his private and family life, his home and his correspondence'. The issue of interference can be tackled from the point of view of the notions of 'correspondence' and 'private life'. The Court has read respect for 'correspondence' and 'private life' as covering any type of *private communication*, whatever their form (*Copland v. the United Kingdom*, para. 41; *Podchasov v. Russia*, para. 52). It has further understood the right as covering not just the *content* of communications but also *data related to the exchange* – such is the case of metadata like the addresses from and to which messages were sent or the time at which they were sent (*Copland v. the United Kingdom*, paras. 13, 41).

Additionally, the Court has considered that Article 8 protects 'information derived' from monitoring an individual's internet usage – even if no private exchange occurs. In *Copland*, in particular, the Court held that monitoring the websites an individual visited, along with the times, dates and durations of those visits, without prior warning, constituted an interference under Article 8 (*Copland v. the United Kingdom*, paras. 41-44).

The overarching test can be described in terms of what the Court has defined as the 'reasonable expectation of privacy' (Gómez-Arostegui, 2005, pp. 162-176). The test first appeared in the case of *Halford v. the United Kingdom* (paras. 42-45) and has been particularly elaborated on in *Benedik v. Slovenia*. Given the elaboration and the fact that it also concerns activities on the internet, I will apply this test to the context of disrupting computer-enabled crime.

In *Benedik v. Slovenia*, the Court considered whether an ISP transmitting subscriber information associated with a dynamic IP address to LEAs amounted to an interference with the right to private life under Article 8(1) (*Benedik v. Slovenia*, para. 119). The

CARLOS JOSÉ CALLEJA

Court used the reasonable expectation test, which can be read as involving three different questions.

Firstly, the Court deemed it relevant to consider whether the specific activity engaged information that could be linked to an identifiable individual. There is a reasonable expectation of privacy over information regarding *identifiable* individuals, even if actual identification requires additional steps. In *Benedik*, the Court deemed information about individual internet usage sufficient for authorities to ultimately identify the individual behind the IP address (*Benedik v. Slovenia*, paras. 109, 111-114).

Secondly, the Court considered whether the information was made available to others through internet use, such as making an IP address visible, or whether additional steps were required – such as issuing a request to ISPs – to expose information the user had not revealed. In the former case, there is no expectation of privacy over the information made available to others; in the latter, there is (*Benedik v. Slovenia*, paras. 115-117).

Thirdly, the Court also deemed relevant, though not decisive, the applicable legal and regulatory framework, including the terms of a contract of accessing services online (*Benedik v. Slovenia*, para. 118).

#### 9.5.2 *The Court's case law on the point at which an interference with the rights in Article 8(1) takes place*

After considering the case law on the type of information protected under Article 8(1), the next question is at what point the Court considers that there is an interference with the right to respect for correspondence or private life under Article 8(1). This is relevant to determine what type of effects on ICTs will constitute an interference.

The Court has held in its latest case law that the mere *intercepting and collecting* of information by LEAs suffices for an interference with the rights enshrined in Article 8(1), even if no subsequent access to that information ever takes place. In this sense, in *Podchasov v. Russia* – which concerns a statutory requirement for service providers to store data of internet communications and provide LEAs access upon request – the Court considered that the sole *storage* of ‘data related to the private life of an individual’ sufficed for an interference (*Podchasov v. Russia*, para. 52). In both *Big Brother Watch v. the United Kingdom* and *Centrum för Rättvisa v. Sweden* – concerning bulk interception of communications and traffic data – the Court concluded that *intercepting and retaining* traffic data already amounted to interference, even if that information was immediately discarded or filtered out (*Big Brother Watch and others v. the United Kingdom*, paras. 324, 326, 330; *Centrum för Rättvisa v. Sweden*, paras. 238, 240, 244).

The question remains whether incidental interception of information suffices or if a more structured collection is required. The above-mentioned cases of *Big Brother Watch*, *Centrum för Rättvisa* and *Podchasov* involve some form of structured collection,

suggesting the latter is necessary. This position is also supported by the Court's previous case law. In *P.G. & J.H. v. the United Kingdom* – concerning covert listening devices at a police station – the Court found that an individual's expectation of privacy was engaged despite the measures targeting activities conducted in public. The Court deemed the systematic and permanent collection of information relevant, bringing it within the scope of Article 8(1) (*P.G. and J.H. v. the United Kingdom*, para. 57). Similarly, in *Rotaru v. Romania*, the Court held that public information systematically collected and stored in governmental files fell within the scope of Article 8(1) (*Rotaru v. Romania*, paras. 43-44). Thus, while the availability of information suffices, it should be intercepted through a structured system. Incidental collection appears to be insufficient for an interference.

### 9.5.3 *Disrupting computer-enabled crime as an interference with the right to respect for private life and correspondence in Article 8(1) of the Convention*

Article 8(1) covers the structured interception of information over which individuals have some expectation of privacy. Disrupting, disabling or degrading computer systems or data stored in them does not inherently constitute an interference with Article 8(1). The key questions are: (1) whether information over which an individual holds a reasonable expectation of privacy is concerned; and (2) whether the disrupting of computer-enabled crime results in LEAs collecting that information in a structured manner. Consider the following two scenarios:

Scenario 4: An agency requests a registry that manages a top-level domain name to modify the resolution of a number of specific domain names exploited by a botnet. Instead of allowing infected computers to connect with their designated command-and-control servers, the altered settings redirect communications to servers controlled by the agency. This intervention disrupts the perpetrators' ability to manage and exploit malware-infected computers. As a result, however, infected computers communicate with the agency's servers, transmitting their IP addresses and time of connection. The LEA's server records those IP addresses and the timestamp at which they communicate with the server. The purpose of that recording is to estimate the size of the botnet and the impact of the operation – i.e. how many computers that formerly attempted to communicate with command-and-control servers now communicate with the LEA's server. It might also serve to identify victims of the malware infection – typically with the assistance of ISPs – and inform their owners of the infection so that they can eradicate the malware from their computers.

Scenario 5: LEAs seize servers used to control a botnet. Using their access to these command-and-control servers, LEAs modify the malware code. This altered code is automatically downloaded by the infected computers during a scheduled update. The

CARLOS JOSÉ CALLEJA

new code initiates a ‘clean-up’ routine on a specified date, relocating essential malware files to a quarantine area within each infected computer, effectively rendering the malware inoperative and eradicating the infection.

The first question is whether the information gathered constitutes information over which an individual has a reasonable expectation of privacy. In Scenario 4, redirecting traffic within the botnet means that malware-infected computers, which formerly communicated with command-and-control servers, now transmit their IP addresses and timestamps to LEA-controlled servers. According to the first criterion in the *Benedik* test, such information can likely be linked to an identifiable individual with the assistance of an ISP. Furthermore, although IP addresses are shared through internet use, the sinkhole also reveals the infection status of the computers. Since this information is not publicly available, the second criterion of the *Benedik* test also indicates a reasonable expectation of privacy. In contrast, considering the third condition, relevant regulations, if these prescribe the general possibility of sinkholing, they could be used to defeat any reasonable expectation of privacy of users of computers infected with malware – though the weight of this criterion in the assessment remains unclear (see *Benedik v. Slovenia*, para. 118).

In the case of Scenario 5, the method used to eradicate the malware involves *transmitting code* instructions to the malware installed in compromised computers. Those instructions give LEAs control over the malicious program and, to the degree that such malware controlled infected computers, of those same computers themselves. During the removal process, LEAs are thus in a position that would allow them to monitor private activities on the infected computers, such as communication transmitted and received. It can be argued that those activities can be linked to an identifiable individual (first criterion in *Benedik*) and will arguably concern information that is not publicly available – for instance, activities on a computer that the user does not intend to share (second criterion in *Benedik*). As in the previous case, however, the presence of regulations explicitly authorising authorities to transmit commands through malware installed in infected computers might be used to defeat a general expectation of privacy.

In both cases, it thus seems that individuals hold a reasonable expectation of privacy over the information concerned. The second question is whether the disruptive operation results in LEAs intercepting and collecting that information in a structured manner.

That seems to be the case in Scenario 4, where the LEA-controlled server systematically records and makes this information available. The case of Scenario 5 is more complicated. It can be argued that LEAs are in a position to monitor activities within compromised machines by transmitting commands to malware-infected computers, potentially allowing them to read information or execute commands to transmit information to their servers. Transmitting commands to the malware thus makes the information available for LEAs to monitor. However, making information available does not point

to a structured form of collecting; it instead appears as an incidental possibility of being in a position of control over compromised computers. It thus seems open to dispute that cases such as the one described in Scenario 4 will pose an interference unless the LEA at stake decide to use its position of control to systematically collect information about the computers from which it seeks to remove the malware.

## 9.6 THE PARTICULAR CASE OF COGNITIVE FORMS OF DISRUPTING COMPUTER-ENABLED CRIME

### 9.6.1 *The Court's case law on the protection that Article 8(1) affords to establish relations and personality development*

Cognitive disruption may involve providing information to undermine the perception that crime can be committed with impunity, fostering suspicion among group or network members, or sending targeted messages to potential perpetrators. This section explores whether cognitive forms of disrupting computer-enabled crime might interfere with fundamental rights under the Convention.

Beyond protecting an individual from intrusions into private activities, Article 8(1) also encompasses a 'personal choice' dimension (Gómez-Arostegui, 2005, p. 155). This dimension includes, on the one hand, the right to engage in relationships with others. The right to engage in relationships with others can be traced back to the seminal case of *X. v. Iceland* – concerning regulations prohibiting keeping a dog within a house. There, the European Commission of Human Rights argued that Article 8(1) covered a right to create and cultivate interpersonal relationships, especially in terms of an emotional bond (p. 87; see also Gómez-Arostegui, 2005, p. 161). Later, in *Niemietz v. Germany* – concerning the search of a lawyer's office – the Court adopted the notion that 'respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings' (*Niemietz v. Germany*, para. 29). In *Bărbulescu v. Romania* – concerning the termination of an employment contract as a consequence of monitoring an employee's internet activity – the Court's Grand Chamber further developed the principle that Article 8 includes a right to lead a 'private social life', which includes a right to engage in relations with others and develop a social identity (*Bărbulescu v. Romania*, para. 70). In that particular case, for instance, the Court noted that internet instant messaging was one of the forms of communication enabling that sort of 'private social life' (para. 74). Other cases have addressed this right in various contexts, such as establishing professional relationships or seeking help (*Locatus v. Switzerland*, paras. 56-60; *Özpinar v. Turkey*, para. 45).

The right to pursue personal development and fulfilment is a second aspect of the personal choice dimension of Article 8(1). *Brüggemann & Scheuten v. Germany* marks the seminal case where the Commission extended its understanding of private life to

CARLOS JOSÉ CALLEJA

also encompass the free development of one's personality (*Brüggemann & Scheuten v. Germany*, para. 55). In later cases such as *Pretty v. the United Kingdom* and *Denisov v. Ukraine*, the Court further emphasised that Article 8 covers the right to personal development (*Denisov v. Ukraine*, para. 95; *Pretty v. the United Kingdom*, para. 61). Though vague, the development of an individual's personality appears to cover aspects of psychological integrity, such as emotional disturbance resulting from verbal abuse (*F.O. v. Croatia*, paras. 85-90).

### 9.6.2 Restrictions to the protection of Article 8(1)

The Court relies on the severity of the consequences to limit the number of cases that fall under Article 8(1) based on their impact on the individual's integrity or the ability to engage in social relations. This assessment considers the 'intensity and duration of the nuisance' and its effects on an individual's quality of life and health (*Denisov v. Ukraine*, para. 31). In *Denisov*, the Court deemed it relevant to assess whether: (1) the measure impacted the individual's inner circle; (2) the intervention posed material consequences; or (3) otherwise impacted the individual's ability 'to establish and develop a relationship with others' or (4) their reputation (*Denisov v. Ukraine*, para. 107). For instance, in *Vučina v. Croatia*, the Court determined that the distress caused by mistakenly labelling a picture did not meet the threshold of severity required to constitute an interference with Article 8(1), given in part to the fact that it did not lead to denigrating the individual in the public eye (*Vučina v. Croatia*, paras. 42-51).

The Court has further emphasised that Article 8(1) does not protect individuals against any personal, social, psychological or economic suffering resulting from a criminal conviction, which are foreseeable consequences of committing a criminal offence – this is known as the 'Gillberg exclusionary principle' (*Gillberg v. Sweden*, para. 68). In *Denisov v. Ukraine*, the Court extended this principle to include not only criminal offences but also other misconduct entailing legal responsibility, which would pose foreseeable negative effects on private life (*Denisov v. Ukraine*, para. 98).

Under the 'Gillberg exclusionary principle' (*Denisov v. Ukraine*, para. 121), any negative consequences of unlawful conduct that were foreseeable by the applicant are excluded from the protection of Article 8(1) of the Convention. The principle has been applied to questions such as whether injuries from a traffic accident raise an issue under Article 8. The Court concluded that it would not, partly because the injuries were the foreseeable consequence of the applicant's voluntary actions, not the result of an act of violence intended to cause harm to the applicant (*Nicolae Virgiliu Tănase v. Romania*, para. 130).

### 9.6.3 Cognitive disruption – an interference with Article 8(1)?

Determining whether cognitive disruption methods interfere with Article 8(1) hinges on the severity of the impact on individuals' ability to engage with others or their psychological integrity and whether these impacts were foreseeable consequences of their criminal activities. Since these questions are new and their answers depend on the particular circumstances, this part will only examine the potential arguments that could either back or challenge these stances. Consider the following scenario:

Scenario 6: LEAs identify an online forum frequently used by perpetrators to share child abuse material. To disrupt their operations, the agency implements a strategy to seed mistrust within the forum. Agents create multiple accounts posing as trusted members and begin subtly spreading rumours about certain key members being undercover law enforcement or informants. Additionally, they introduce fake evidence and manipulate screenshots to support these claims. This strategic misinformation campaign gradually sows doubt and suspicion among forum members, leading to infighting, reduced cooperation and a significant decline in the forum's activity and effectiveness.

Since the forum's purpose is to facilitate interaction and cooperation among members, sowing mistrust affects their ability to establish and develop relationships. Regarding the psychological integrity of individuals participating in the forum, the campaign might cause stress and paranoia among members, affecting their mental well-being. One could thus argue that campaigns such as the one in Scenario 6 target the trust dynamics within a forum, directly impacting members' ability to engage with others freely and openly. Their mental integrity seems to also be affected. However, it could also be contended that these effects do not surpass the severity threshold. Concerning the ability to establish relationships with others, the intervention is confined to participation in a specific online forum. It does not impede individuals from forming connections in other forums or the offline world. Whether stress and paranoia constitute an impact of sufficient severity on an individual's integrity can also be discussed. While these emotional responses can cause discomfort and concern, they do not necessarily imply a profound and lasting impact on an individual's mental health. Overall, it is uncertain whether cognitive interventions like the one discussed in Scenario 6 meet the severity threshold required to engage Article 8(1) of the Convention.

The second question concerns whether these effects are a foreseeable consequence of misconduct or criminal activity. Sharing child abuse material falls within criminal prohibitions. Indeed, Article 9(1)(b) and (c) obligates state parties to criminalise 'offering', 'making available', 'distributing' or 'transmitting' child abuse material over the internet. The key issue is whether it is foreseeable LEAs will sow mistrust among participants within the forum as a consequence of such misconduct. One might argue that these consequences are foreseeable because those engaged in sharing child abuse materials online could anticipate a range of tactics aimed at preventing their activities

CARLOS JOSÉ CALLEJA

or mitigating their effects. Participants in the forum should indeed expect that their illicit activities will attract innovative and intrusive methods of disruption from authorities. However, it could be suggested that seeding mistrust is a relatively novel tactic and, therefore, might not be reasonably foreseeable to participants in a forum.

## 9.7 CONCLUSIONS

The chapter has overall served as an initial effort to address some of the questions and arguments that could emerge due to the adoption of disruption as a method for LEAs to tackle computer-enabled crime. It began by acknowledging that various policy documents advocate for disruptive strategies as effective tools for LEAs combating computer-enabled crime. It then discussed whether and to what extent disrupting could be an interference with some of the rights in Articles 8(1) and 10(1) of the Convention.

The first section provided a conceptualisation of the aims and methods of disruptive operations. Distinctions between disabling, degrading and disruptive effects, considerations of collateral damage, the concept of reversibility, and the emergence of cognitive forms of disruption formed the foundation for the subsequent legal analysis.

The central inquiry was then whether and to what extent disruptive operations would interfere with rights enshrined in Articles 8(1) and 10(1) of the Convention. The chapter pointed out that engaging in activities that disrupt access to internet services could interfere with the right to transmit and receive information, as stated in Article 10(1) of the Convention. It also noted that activities involving the structured interception and gathering of information that individuals reasonably expect to be private could pose an interference with the right to privacy and correspondence as outlined in Article 8(1) of the Convention. Additionally, disturbances that affect cognitive processes might impact the right to personal development and forming relationships under Article 8(1) of the Convention, provided they meet a certain level of severity and are not a foreseeable result of misconduct.

## REFERENCES

*Academic writings, commentaries and media reports*

- Borghard, E.D., & Lonergan, S.W. (2017). The Logic of Coercion in Cyberspace. *Security Studies*, 26(3), 452-481. <https://doi.org/10.1080/09636412.2017.1306396>.
- Clough, J. (2020). Between prevention and enforcement: The role of 'disruption' in confronting cybercrime. In D.J. Baker & P.H. Robinson (Eds.), *Artificial Intelligence and the Law: Cybercrime and Criminal Liability* (pp. 49-73) (1st ed.). Routledge.

- Collier, B., Thomas, D.R., Clayton, R., Hutchings, A., & Chua, Y.T. (2022). Influence, infrastructure, and recentring cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, 32(1), 103-124. <https://doi.org/10.1080/10439463.2021.1883608>.
- Deeks, A. (2020). *Defend Forward and Cyber Countermeasures*. Public Law and Legal Theory Paper Series 2020-59, Aegis Series Paper No. 2004.
- Europol (2021a). *Police2Peer*. <https://www.europol.europa.eu/partners-collaboration/police2peer> [Accessed 10 October 2024].
- Europol (2021b, 27 January 2021). *World's most dangerous malware EMOTET disrupted through global action*. <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action> [Accessed 10 October 2024].
- Europol (2024). *Law enforcement disrupt world's biggest ransomware operation*. <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation> [Accessed 10 October 2024].
- Gómez-Arostegui, H.T. (2005). Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations. *California Western International Law Journal*, 35(2).
- Harris, D.J., O'Boyle, M., Bates, E., & Buckley, C.M. (2023). *Law of the European Convention on Human Rights* (5th ed.). Oxford University Press.
- Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), tyz008. <https://doi.org/10.1093/cybsec/tyz008>.
- Healey, J., Jenkins, N., & Work, J.D. (2020). Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations. In L.L.T. Jančárková, M. Signoretti, I. Tolga, G. Visky (Eds.), *2020 12th International Conference on Cyber Conflict* (pp. 251-274). NATO Cooperative Cyber Defence Centre of Excellence.
- Herpig, S. (2018). *A Framework for Government Hacking in Criminal Investigations*. Stiftung Neue Verantwortung.
- Herpig, S. (2021). *Active Cyber Defense Operations: Assessment and Safeguards*. Stiftung Neue Verantwortung.
- Hutchings, A., & Holt, T.J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, 18(1), 11-30. <https://doi.org/10.1080/17440572.2016.1197123>.
- Innes, M., & Sheptycki, J.W.E. (2004). From Detection to Disruption. *International Criminal Justice Review*, 14(1), 1-24. <https://doi.org/10.1177/105756770401400101>.
- Kello, L. (2018). Private Sector Cyber Weapons: An Adequate Response to the Sovereignty Gap? In H. Lin & A. Zegart (Eds.), *Bytes, Bombs, and Spies* (pp. 357-378). Brookings Institution Press. <http://www.jstor.org/stable/10.7864/j.ctv75d8hb.19>.

CARLOS JOSÉ CALLEJA

- Liff, A.P. (2012). Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35(3), 401-428. <https://doi.org/10.1080/01402390.2012.663252>.
- Qurashi, F. (2018). The Prevent strategy and the UK 'war on terror': embedding infrastructures of surveillance in Muslim communities. *Palgrave Communications*, 4(1), 17. <https://doi.org/10.1057/s41599-017-0061-9>.
- Ragan, S. (2014). Takedown of No-IP by Microsoft impacts 1.8M customers. *CSO Online*. <https://www.csoonline.com/about-us/> [Accessed 10 October 2024].
- Ratcliffe, J.H. (2016). *Intelligence-led policing* (2nd ed.). Routledge.
- Romanosky, S., & Goldman, Z. (2017). Understanding Cyber Collateral Damage. *Journal of National Security Law and Policy*, 9, 233-258.
- Shackelford, S.J.C., Danuvasin Waite, T., & Zhang, N. (2019). Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking. *University of Pennsylvania Journal of International Law*, 41, 377-427.
- Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, 40(7), 898-926. <https://doi.org/10.1080/01402390.2017.1307741>.
- Skidmore, M. (2023). *Lifting the Lid on 'Disruption' as an Approach to Controlling Serious and Organised Crime*. Perspectives on Policing: Paper 9. The Police Foundation.
- Smeets, M. (2022). *No shortcuts: why states struggle to develop a military cyber-force*. Oxford University Press.
- Schmitt, M.N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781316822524>.
- Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydowski, M., Kemmerer, R., Kruegel, C., & Vigna, G. (2009). Your botnet is my botnet: analysis of a botnet takeover. *CCS '09: Proceedings of the 16th ACM Conference on Computer and Communications Security*, 9-13 November 2009, Chicago, Illinois. Association for Computing Machinery.
- Tate, R., & Bates, C. (2022). Deterrence Through Transparent Offensive Cyber Persistence. *The Cyber Defense Review*, 7(4), 227-246. <https://www.jstor.org/stable/48703302>.
- Threat Intelligence Team (2021, 29 January). Cleaning up after Emotet: the law enforcement file. *Malware Bytes Labs*. <https://www.malwarebytes.com/blog/news/2021/01/cleaning-up-after-emotet-the-law-enforcement-file#:~:text=Shortly%20after%20the%20Emotet%20takedown,the%20April%2025%202021%20deadline> [Accessed 10 October 2024].
- Tilley, N. (2016). Intelligence-led policing and the disruption of organized crime: motifs, methods and morals. In T. Delpuech & J.E. Ross (Eds.), *Comparing the Democratic Governance of Police Intelligence: New Models of Participation and Expertise in the United States and Europe* (pp. 153-179). Edward Elgar Publishing. <https://doi.org/10.4337/9781785361036.00015>.

Werner, T., & Leder, F. (2009). *Know your enemy: containing conficker. To tame a malware.* The Honeynet Project.

### Case law

*Ahmet Yildirim v. Turkey*, no. 3111/10, European Court of Human Rights (Second Section), 18 December 2012.

*Akdeniz v. Turkey* (dec.), no. 20877/10, European Court of Human Rights (Second Section), 11 March 2014.

*Bărbulescu v. Romania*, no. 61496/08, European Court of Human Rights (Grand Chamber), 5 September 2017.

*Benedik v. Slovenia*, no. 62357/14, European Court of Human Rights (Fourth Section), 24 April 2018.

*Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13 and 2 others, European Court of Human Rights (Grand Chamber), 25 May 2021.

*Brüggemann & Scheuten v. Germany*, no. 6959/75, European Commission of Human Rights (Plenary), decision of 19 May 1976, Decisions and Reports 5.

*Cengiz and others v. Turkey*, nos. 48226/10 and 14027/11, European Court of Human Rights (Second Section), 1 December 2015.

*Centrum för Rättvisa v. Sweden*, no. 35252/08, European Court of Human Rights (Grand Chamber), 25 May 2021.

*Copland v. the United Kingdom*, no. 62617/00, European Court of Human Rights (Fourth Section), 3 April 2007.

*Denisov v. Ukraine*, no. 76639/11, European Court of Human Rights (Grand Chamber), 25 September 2018.

*F.O. v. Croatia*, no. 29555/13, European Court of Human Rights (First Section), 22 April 2021.

*Gillberg v. Sweden*, no. 41723/06, European Court of Human Rights (Grand Chamber), 3 April 2012.

*Halford v. the United Kingdom*, no. 20605/92, European Court of Human Rights, 25 June 1997, Reports 1997-III.

*Locatus v. Switzerland*, no. 14065/15, European Court of Human Rights (Third Section), 19 January 2021.

*Nicolae Virgiliu Tănase v. Romania*, no. 41720/13, European Court of Human Rights (Grand Chamber), 25 June 2019.

*Niemietz v. Germany*, no. 13710/88, European Court of Human Rights (Chamber), 16 December 1992, A251-B.

*Özpinar v. Turkey*, no. 20999/04, European Court of Human Rights (Second Section), 19 October 2010.

CARLOS JOSÉ CALLEJA

- P.G. and J.H. v. the United Kingdom*, no. 44787/98, European Court of Human Rights (Third Section), 25 September 2001, Reports of Judgments and Decisions 2001-IX.
- Podchasov v. Russia*, no. 33696/19, European Court of Human Rights (Third Section), 13 February 2024.
- Pretty v. the United Kingdom*, no. 2346/02, European Court of Human Rights (Fourth Section), 29 April 2002, Reports of Judgments and Decisions 2002-III.
- Rotaru v. Romania*, no. 28341/95, European Court of Human Rights (Grand Chamber), 4 May 2000, Reports of Judgments and Decisions 2000-V.
- Times Newspapers Ltd (Nos. 1 and 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, European Court of Human Rights (Fourth Section), 10 March 2009.
- Vladimir Kharitonov v. Russia*, no. 10795/14, European Court of Human Rights (Third Section), 23 June 2020.
- Vučina v. Croatia* (dec.), no. 58955/13, European Court of Human Rights (First Section), 24 September 2019.
- X v. Iceland*, no. 6825/74, European Commission of Human Rights (Plenary), decision of 18 May 1976, Decisions and Reports 5.

#### *Reports, guidelines and national strategies*

- Centre for Cybersecurity Belgium (2021). *Cybersecurity Strategy Belgium 2.0 – 2021-2025*.
- Chairman of the Joint Chiefs of Staff (2018). *Joint Publication JP 3-12 Cyberspace Operations June 2018*.
- Chiefs of Staff (2022). *Cyber Primer* (3rd ed.). United Kingdom Ministry of Defence.
- Danish Government (2021). *The Danish National Strategy for Cyber and Information Security 2022-2024*.
- Department of Justice (2022). *Comprehensive Cyber Review July 2022*. Office of the Deputy Attorney General.
- European Cybercrime Center (EC3). (2014). *First Year Report*. <https://www.europol.europa.eu/publications-events/publications/european-cybercrime-center-ec3-first-year-report#downloads> [Accessed 10 October 2024].
- Government of the United Kingdom (2016). *National Cyber Security Strategy 2016 to 2021*.
- Government of the United Kingdom (2022). *National Cyber Strategy 2022*.
- Interpol (2022). *Cybercrime Global Strategy 2022-2025*.
- Kaska, K. (2012). *Conficker: Considerations in Law and Legal Policy*. NATO Cooperative Cyber Defence Centre of Excellence.
- National Coordinator for Counterterrorism and Security (2022). *Netherlands Cybersecurity Strategy 2022-2028*.

- National Cyber Force (2023). *The National Cyber Force: Responsible Cyber Power in Practice*.
- Piscitello, D. (2010). *Conficker Summary and Review*. ICANN.
- The Rendon Group (2011). *Conficker Working Group: Lessons Learned*. The Rendon Group.
- World Bank & United Nations (2017). *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*.
- World Economic Forum (2020). *Partnership against Cybercrime Insight Report November 2020*.
- Yesilgöz-Zegerius, D. (2022). *Integrale aanpak cybercrime*. [https://www.tweedekamer.nl/kamerstukken/brieven\\_regering/detail?id=2022D45408&did=2022D45408](https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022D45408&did=2022D45408) [Accessed 10 October 2024].

#### *Treaties and legislation*

- European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, ETS 5, 4 November 1950, (1950).



## 10 DIGITALISATION AND THE POLICE FUNCTION

### *How the playing field is changing and what it demands of the police: a Dutch case study*

Wouter Stol, Jurjen Jansen and Wouter Landman

#### **Abstract**

*This chapter discusses digitalisation and the police function. Digitalisation has brought about changes, significantly altering the playing field for the police function. In particular, actors outside the police function have gained additional opportunities to challenge or contribute to the rule of law. This is due to changes in organisational capacity, information capacity and normative capacity. We provide examples of this by examining the influence of digitalisation on crime and public order. This 'new' reality forces the police to reflect on their role. In this chapter, we offer several possible approaches to fuel further debate on the police function and the role the police can or should play. These approaches include: (1) collaboration with citizens and private organisations, and regulating the field of social control; (2) shifting from detection to crime prevention; and (3) ensuring legal protection by supervising the use of new opportunities by citizens and organisations. These changes require a proactive approach to ensure and strengthen the effectiveness of the police function in the digital age.*

#### 10.1 INTRODUCTION<sup>1</sup>

The question we seek to answer in this chapter is what implications the digitalisation of society has for the police function in the Netherlands and what that means for the Dutch police. By digitalisation, we refer to the trend where automated processes play an increasingly significant role in daily life in various ways and settings (Stol & Strikwerda, 2019). Section 10.2 discusses the terms 'police function' and 'the police', as well as the theoretical perspective in which we situate these terms. We then examine the influence of digitalisation on crime in section 10.3 and its impact on public order in section 10.4. Subsequently, we delve into the importance of these developments for the police function in section 10.5, and in section 10.6 we take a stance on how the police can respond to these challenges.

---

<sup>1</sup> This chapter is based on Stol et al. (2024).

### 10.2 SOCIAL CONTROL AS A THEORETICAL PERSPECTIVE

We position the police function within the theoretical framework of social control (Cachet, 1990; Stol, 1996). Social control involves the application of (positive or negative) sanctions aimed at aligning or bringing the behaviour of others in accordance with the standards prevailing within the group (Stol, 1996). From this perspective, the police function essentially entails the enforcement of collective norms and rules in society. A defining characteristic of the police function is that it involves *formal* social control, which implies that coercion can be exerted based on legal rules to achieve compliance with shared norms and rules (Heijder, 1989). Formal social control contrasts with informal social control, which relies on informal sanctions in everyday life (at home, school, social circles). Therefore, the police function has a broader scope than ‘the police’ but a narrower scope than ‘social control’.

The police function is also understood as ‘a regulatory function consisting of monitoring and enforcing generally accepted norms and rules, and maintaining order within a social environment – if necessary, through the use of coercion and/or compulsion’ (Van Steden et al., 2009, p. 6; see also Van Halderen et al., 2024). However, in this approach, the police function is not linked to a legal basis, which risks losing its relationship with the rule of law, and blurs the distinction between the police function and social control in any form. In our approach, the police function and social control are explicitly not synonymous, precisely because of the legal basis of the former.

The police function is carried out by various parties (Brodeur, 2010) such as the police, special investigation officers, the tax authorities, and mental health institutions for compulsory care. This characteristic is also referred to as ‘plural policing’ (Bijleveld et al., 2021). The police are an organisation for formal social control and in the Netherlands the police are the organisation intended in Article 25, paragraph 1 of the Dutch Police Act 2012 (Pw). The police traditionally hold a unique position within the broader police function, particularly due to the combination of their broad mandate (Article 3 Pw), which they use to work towards the police function, their organisational size, their visibility and their ability to intervene with significant coercive measures in the domain of individual citizens and private organisations.

### 10.3 STUDY DESIGN AND METHODS

This study is designed as a case study and it focuses on the Netherlands. The methodology used can best be described as qualitative participative observation. The authors have been actively participating in the field of digitalisation and policing for, respectively, 30 years (Stol) and more than 10 years (both Jansen and Landman). These time periods give us the opportunity to consider changes over the course of time. Our lens for examining past and present events in Dutch society consists of the total of what we have

heard from others, what we have read in newspapers and in policy documents, and what we have read in professional and academic publications. We distinguish between crime-fighting and public order maintenance and we describe what changes related to the digitalisation of society become visible in these two areas. The term ‘visible’ refers to empirical data from which we conclude that a certain development has occurred. We limit our analysis to the Netherlands and we identify both impactful events (e.g. the Anne Faber case in the field of crime-fighting) and recurring events (e.g. ‘online-induced public order disturbances’ in the field of public order maintenance) that demonstrate the existence of certain trends. These events as well as trends are elaborated below.

#### 10.4 DIGITALISATION AND CRIME

In this section, we delve into the impact of digitalisation on crime. We provide a concise overview where we particularly focus on what digitalisation means for citizens, private organisations and the police.

##### 10.4.1 *Digitalisation and offending behaviour*

Digitalisation has provided citizens and organisations with the opportunity to commit online crimes. We define ‘online crimes’ as criminal activities where the use of automated systems<sup>2</sup> is crucial for the commission of the offence. Due to digitalisation, new forms of crime have emerged (cybercrime), and many traditional crimes have taken on a digital form (digitalised crime). We categorise both forms and their hybrids under the term online crime. Online crime has become an increasingly significant portion of overall criminal activity (CBS, 2022). Additionally, new methods of committing crimes digitally continue to emerge, such as assault by disrupting a pacemaker or brain implant,<sup>3</sup> murder by hacking a moving vehicle (ENISA, 2017), or sexual assault by virtually touching an avatar.<sup>4</sup>

In addition to providing opportunities for new forms of crime, digitalisation also offers a cover for anonymity to perpetrators (Stol, 2003; Van den Berg et al., 2012). People can easily conceal their activities and locations online through encryption

---

2 We align with the concept stated in Article 80sexies of the Dutch Criminal Code, which defines an ‘automated work’ as ‘a device or group of interconnected or interrelated devices, of which one or more automatically process computer data based on a program.’

3 <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update>.

4 <https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta>.

(Jansen et al., 2023). On the so-called dark web, hiding identities and locations (IP addresses) is the norm (Emmen et al., 2023). Moreover, (criminal) financial transactions can be concealed using cryptocurrencies (Europol & Eurojust, 2019). The fact that concealment may not always be sustainable does not negate this overall trend.

Online crime can be carried out irrespective of time and location. Although most online crimes affecting individuals in the Netherlands occur within national borders (Roks & Monshouwer, 2022), some have an international dimension, where perpetrators and victims are located in different jurisdictions, making it challenging to effectively address such crimes. The so-called de-territorialisation of online crime not only involves crossing national borders but can also occur within a country, as criminal activities spread across different regions, cities or neighbourhoods. This ‘domestic de-territorialisation’, while not entirely new, represents a second wave. In the 1960s, police chiefs, in a paper entitled ‘Crime Control in a Changing Society’, noted the first wave, also driven by technology:

Not only so-called professional burglars and swindlers, whose work area is often the entire country, make use of modern traffic and communication means, but also exhibitionists, molesters, bicycle and moped thieves, shoplifters and thieves, et cetera, are motorised and often operate outside their place of residence (Haane & Heijboer, 1965, pp. 61-62).

However, digitalisation exacerbates this phenomenon. Wrongdoers can easily collaborate with each other in changing networks to innovate their attacks (Leukfeldt, 2016; NCTV, 2022), and the ICT infrastructure used for online crime can be located in different countries, for example due to the increasing use of cloud-based storage and services (Europol & Eurojust, 2019). Importantly, digitalisation enables offences to be committed remotely, greatly expanding the possibilities for perpetrators.

While digitalisation provides perpetrators with significant opportunities, it does not offer comparable opportunities for self-protection to citizens and businesses as potential victims. People often struggle to understand and navigate their digital environments, leading to errors and vulnerabilities (Stol, 2020), and consequently victimisation. Additionally, distinguishing between what is real/true and what is fake/false online has become increasingly difficult for individuals (Jansen et al., 2019), making them susceptible to various new forms of fraud. An example of this is ‘voice cloning’, where criminals call a potential victim using the ‘cloned’ voice of a friend or family member, requesting quick money transfers or sharing personal information (see Landman, 2023). Deepfake videos also exemplify this trend.

It is not just citizens and their organisations that are facing challenges. Due to digitalisation, society as a whole has become more reliant on technologically complex systems, making it more susceptible to outages, disruptions and attacks (NCTV, 2022), which can have significant (societal) impacts (Prins et al., 2019). Outages can result

from a targeted attack or a so-called cascade effect, where an individual (criminal) attack affects the rest of a chain or network, or even beyond (Prins et al., 2019).

#### 10.4.2 *Digitalisation and participation in crime control*

Digitalisation not only provides citizens and organisations with new opportunities to commit crimes but also to exercise social control and combat crime. Citizens can organise themselves using digital technology for crime prevention. In the Netherlands, the most widespread example is likely the WhatsApp neighbourhood watch group (WhatsApp-buurtpreventie in Dutch; Lub & de Leeuw, 2019). More specialised initiatives in the Netherlands include Bureau Dupin, which focuses on helping solve unsolved homicide cases. Other examples include the journalist collective Bellingcat, which investigated the downing of flight MH17, and the whistleblower platform WikiLeaks (Higgins, 2021). A milestone in this development in the Netherlands was the digitally organised effort by the Faber family in 2019 to gather information about their missing (and later found murdered) daughter, Anne. This effort surpassed what the police were doing at the time, and subsequently the police were able to benefit from it (Lam & Kop, 2020). Regardless of whether a missing person is a precursor to a crime – it could also involve, for example, running away, accidents or suicide – searching for a missing person is a subject that digitally organised citizens focus on. Dutch examples include the Veterans Search Team (VST) and the Coordination Platform for Missing Persons (CPV),<sup>5</sup> both of which officially collaborate with the police. The VST originated from a one-time initiative in 2017 (VST, 2019), and the CPV was established in 2016 following a single search operation via Facebook.

In addition to gathering information, private parties can also set norms, intervene, enforce sanctions or exert coercion (Svensson & Zouridis, 2004; Stol, 2010). This can range from corrections by a moderator to more extensive measures, such as a financial institution closing a bank account suspected of being used for phishing transactions, a social networking site excluding a user from its services because the content of a post is ‘norm-breaking’, or a provider taking down a website distributing child sexual abuse material. The possibilities for sanctions through teasing, bullying and exclusion have also increased due to digitalisation. However, the sanctioning powers of private parties are not unlimited, as they are limited by the rights of those targeted by the sanctions.

The fact that a significant portion of crime now occurs online means that the parties capable of exercising social control are often private entities (Svensson & Zouridis, 2004; Bijleveld et al., 2021). Much of the ICT infrastructure – including cables, servers, data centres and sensors, as well as platforms, services, etc. – necessary for committing

---

5 See respectively [www.veteranensearchteam.nl](http://www.veteranensearchteam.nl) and [www.cpv-nl.nl](http://www.cpv-nl.nl).

online crime is privately owned. Owners may include tech giants like Meta, Google, Apple, Microsoft and Amazon, insurers, energy companies, or financial institutions. Smaller companies that establish a position through their digital information position (e.g. satellite data, internet monitoring) are also relevant. However, it is primarily the large private entities that possess extensive information about their end users and/or target groups, including interests, preferences and behaviours (comprising norm-deviating behaviour).

Cases where citizens use digital tools for social control are often controversial due to conflicts with the principles of the rule of law. For instance, in 2009, online paedophile hunter Yvonne van H. was convicted of defamation.<sup>6</sup> In 2015, a journalist noted that what started as WhatsApp neighbourhood watch in the municipality of Aalborg quickly turned into a discriminatory ‘witch hunt against people with an Eastern European appearance.’<sup>7</sup> Dutch police chief Oscar Dros stated in 2020 that the police do not need the ‘assistance’ of paedophile hunters because they ‘commit criminal offences and create dangerous situations.’<sup>8</sup> Members of the civilian watch in Ter Apel, where the busiest asylum-seeker centre in the Netherlands is located, maintain contact through a (closed) Facebook page and a WhatsApp group. They patrol and carry out citizen’s arrests, with the latter particularly sparking media debate, especially when violence is involved.<sup>9</sup> ‘Do not take matters into your own hands,’ says the Dutch Ministry of Justice and Security.<sup>10</sup>

#### 10.4.3 *Digitalisation, police and crime-fighting*

Digitalisation demands significant adaptability from the police. Over time, specialised teams have been established to combat online crime, and international collaboration occurs in major cases. However, in generic police work, as conducted by local police units, there remains a significant knowledge gap. This has been a consistent finding since the advent of digitalisation (Stol et al., 1999; Jansen et al., 2020; Ruiters et al., 2023). While initiatives are taken to address this knowledge gap, the catch-up process is, to put it mildly, slow. Currently, the police possess the least knowledge about the most prevalent type of crime, namely online crime. However, merely having ‘more knowledge’ does not solve all the problems posed by digitalisation. For instance, the scale of online crime requires scarce resources, its de-territorial nature necessitates cooperation across

6 NRC, 8 May 2009.

7 Reformatorisch Dagblad, 1 October 2015; NRC, 23 August 2017.

8 [www.gelderlander.nl/binnenland/politie-over-pedo-jagers-dit-zijn-geen-helden-we-zijn-er-klaar-mee--a9664741/](http://www.gelderlander.nl/binnenland/politie-over-pedo-jagers-dit-zijn-geen-helden-we-zijn-er-klaar-mee--a9664741/).

9 [www.facebook.com/groups/950867156083671/](https://www.facebook.com/groups/950867156083671/); [www.groene.nl/artikel/de-burgerwacht-in-ter-apel-nos.nl/nieuwsuur/artikel/2485941-burgerwacht-in-opkomst-hoe-ver-mag-je-gaan](http://www.groene.nl/artikel/de-burgerwacht-in-ter-apel-nos.nl/nieuwsuur/artikel/2485941-burgerwacht-in-opkomst-hoe-ver-mag-je-gaan).

10 [nos.nl/nieuwsuur/artikel/2485941-burgerwacht-in-opkomst-hoe-ver-mag-je-gaan](http://nos.nl/nieuwsuur/artikel/2485941-burgerwacht-in-opkomst-hoe-ver-mag-je-gaan).

different jurisdictions, which is not always straightforward, and online anonymity makes detection challenging across the board (see also Jansen et al., 2023).

Moreover, legal frameworks that provide guidance to the police are under pressure in various areas, leading to uncertainty for the police. For example, the intertwining of humans and machines enables forms of crime for which our current substantive criminal law has no answer (Borwell et al., 2021; Van der Wagen, 2018). We mentioned some examples earlier (see section 10.4.1). Digitalisation also presents new challenges for criminal procedural law. For instance, the formal authority regarding systematic information gathering (Article 126j of the Dutch Code of Criminal Procedure) and that regarding body searches (Article 195 of the Dutch Code of Criminal Procedure) are now strictly separated powers. However, systematic information gathering can transition into research on and even within the body by collecting data from smartwatches (e.g. heart rate, movement, body temperature, fertility cycle, sleep/wake patterns).

Of course, digitalisation also offers the police new opportunities. Examples include hacking powers or the authority to systematically collect personal data from publicly accessible (internet) sources.<sup>11</sup> Police officers also utilise general digital (information) capabilities, such as Google, and they record information in police systems that they can subsequently access. This gives police officers more information about citizens at their fingertips than ever before, often information about norm-deviant behaviour. The police use information from police systems for their operations on the streets or for handling cases, but also for purposes such as predictive policing, which involves analyses to help predict and act upon criminal activity. However, there is no research indicating that the use of databases or predictive policing has led to a reduction in crime (see also Meijer & Wessels, 2019). Nevertheless, the police achieve success through international collaboration in cracking crypto services, such as Ennetcom, EncroChat and Sky ECC (Jansen et al., 2023; Landman, 2023). For instance, the Sky ECC operation yielded around a billion messages from 70,000 devices, resulting in hundreds of investigations in the Netherlands and Belgium alone (Oerlemans & Royer, 2023). Cracking such services also provides the police with knowledge about modus operandi and criminal networks.

### 10.5 DIGITALISATION AND PUBLIC ORDER

In this section, we delve into the impact of digitalisation on public order. Similar to our discussion on crime, this is a broad overview focusing on what digitalisation entails for citizens, private organisations and law enforcement agencies.

---

11 This latter is part of the modernisation of the Dutch Code of Criminal Procedure.

WOUTER STOL, JURJEN JANSEN AND WOUTER LANDMAN

### 10.5.1 *Digitalisation and public order disturbances*

In addition to its impact on crime, digitalisation also influences offline public order. In 1997, hooligans organised a fight in a field near the Dutch city of Beverwijk via SMS, resulting in a fatality. In 2003, the new digital possibilities to gather people were humorously demonstrated in various countries with ‘flash mobs’ (a group of people suddenly assembling in a public place, doing something unusual, and then quickly dispersing). In 2012, a Dutch 15-year-old girl posted a public invitation for her ‘Sweet Sixteen’ party in the Dutch city of Haren on Facebook. Through this invitation, initially directed at her friends, more people were invited by a friend of a friend, and through a snowball effect, thousands of people arrived in a short time. Deleting the original invitation post did not help as new event posts were already created with the recurring name ‘Project X’. Thousands of young people came to the ‘party’ in Haren, which ended in riots, with the riot police called, and the resignation of the mayor (Cohen et al., 2013).

Project X was not fundamentally new but served as a wake-up call and the beginning of a phenomenon called ‘online-induced (public) order disturbances’: physical disruptions of public order initiated or amplified online.<sup>12</sup> In the years following Project X, this phenomenon occurred many more times (Bantema et al., 2020). The most recent example of large-scale online-induced public order disturbances in the Netherlands are the ‘curfew riots’ (*avondklokrellen* in Dutch). In January 2021, the introduction of the curfew (because of the COVID-19 pandemic) led to days of unrest with riots in several municipalities (COT, 2021a; 2021b; Moors et al., 2022). These riots demonstrate that the mobilising role of digital technology has greatly evolved: from one digital platform to many platforms; from a prior invitation to live reporting of riots; from inciting to both inciting and coordinating; from seeking entertainment and sensation to also expressing discontent. An analysis of the curfew riots concludes: ‘Social media played a significant role. As a coordination and incitement tool, which influencers from groups with organisational capacity deliberately use to channel experienced discomfort and anger into protest movements’ (Moors et al., 2022, p.7).

### 10.5.2 *Digitalisation and participation in order maintenance*

Digitalisation also provides citizens with new opportunities to take action in maintaining public order. In January 2021, ‘football supporters’ easily organised themselves using digital means and took to the streets to prevent rioters from vandalising the city during the pandemic. They received praise from a mayor for their civic-mindedness,

---

<sup>12</sup> In addition to online-incited public disturbances, there is also online-incited violence (see also Bartelds et al., 2023). Think of drill rap groups initiating heavy street fights through online channels.

but there was also criticism from a rule-of-law perspective.<sup>13</sup> The police were also not entirely supportive. Such citizen actions to maintain order are not new (as far back as 1970, marines autonomously cleaned up Dam Square in the centre of Amsterdam).<sup>14</sup> However, the ease with which such actions can now be initiated and organised thanks to digitalisation is indeed new.

The frequency with which these ‘citizen-order teams’ emerge, in our estimation, is less than the frequency with which citizens engage in combating crime. There are many local fathers and/or mothers active in various neighbourhoods, keeping an eye in particular on young people to maintain order in the area. However, their formation and operation are less dependent on digital means. Such initiatives typically arise more gradually (idea, discussion, resources, coordination with local authorities), although smartphones and chat apps are undoubtedly used in execution.

### 10.5.3 *Digitalisation, police and order maintenance*

Digitalisation presents the police and their partners in law enforcement with new challenges regarding maintaining public order. Firstly, there are issues concerning capabilities and authorities, particularly with regard to the police investing more in online data gathering in recent years, especially concerning public order and increasing ‘social discontent.’ However, other actors have also begun collecting online data related to social discontent and potential public order disturbances. Dutch municipalities, for instance, have become active in online monitoring to anticipate potential threats to public order. Additionally, organisations such as the Dutch National Coordinator for Counterterrorism and Security (NCTV) have been monitoring citizens on social media using ‘fake accounts’ on a large scale in connection with possible threats to national security.<sup>15</sup> Moreover, efforts are being made by entities like youth groups and the police to be present in and intervene in the online world of young people to prevent online-driven disturbances or violence.

The question arises about who has what capabilities and what is legally permissible and ethically desirable. Consequently, there is much uncertainty about how to proceed in this regard. The development of legal frameworks for online activities in public order enforcement has not kept pace with practice. This discrepancy poses challenges, as legislation and jurisprudence related to physical domains do not seamlessly translate to the digital domain. This issue is evident in efforts to establish a legal basis for what

13 NRC, 26 January 2021; [www.nhnieuws.nl](http://www.nhnieuws.nl), 27 January 2021.

14 NRC, 26 August 1970 (NRC archive: [https://www.nrc.nl/nieuws/1970/08/26/en-minister-president-optreden-van-mariniers-ouist-kb\\_000033265-a2898371](https://www.nrc.nl/nieuws/1970/08/26/en-minister-president-optreden-van-mariniers-ouist-kb_000033265-a2898371)).

15 <https://www.nrc.nl/nieuws/2021/04/09/nctv-volgt-heimelijk-burgers-op-sociale-media>.

WOUTER STOL, JURJEN JANSEN AND WOUTER LANDMAN

is termed an ‘online area ban’. Recent measures have been taken to provide more legal basis for activities such as online monitoring by municipalities and the NCTV.<sup>16</sup>

Apart from the legal and ethical challenges, there is also a collaboration challenge. Within the police force, various departments are increasingly involved in gathering online data and are working towards an optimal distribution of tasks. Collaboration processes are also ongoing between the police and other actors. Additionally, consideration is being given to how government agencies collaborate with online platforms to remove undesirable content related to online-driven disturbances. However, such collaboration raises legal and ethical questions about whether citizens are being monitored and ‘judged’ by a ‘non-democratically controlled entity’ (Bijleveld et al., 2021). Thus, the collaboration challenge is closely linked to legal and ethical issues.

## 10.6 CONCLUSIONS: CHANGED POSITIONS AND THE POLICE FUNCTION

The foregoing illustrates that digitalisation affects social control in three main respects. It affects what we call organisational capacity, information capacity and normative capacity of citizens, private organisations and government entities, including the police. ‘Organisational capacity’ of an individual or collective refers to the potential to coordinate actions towards a particular goal. ‘Information capacity’ pertains to information as capital and as a basis for action. It involves possessing information and being able to use it, for example in order to exercise social control. ‘Normative capacity’ refers to the ability of an individual or organisation to influence the opinions of others and potentially their behaviour as well. Below we will have a closer look at these three capacities.

### 10.6.1 *Digitalisation and organisational capacity*

Digitalisation creates organisational capacity, primarily providing new opportunities for individual citizens who are mutual strangers. Thanks to digital capabilities, they can now organise themselves and then coordinate actions collectively. We have just seen various examples of this. Citizens use digital tools to commit crimes together, organise demonstrations and riots, hunt down alleged criminals, search for missing persons, or intervene against what they perceive as disruptors of order. Not only do citizens have many new opportunities due to their recently acquired organisational capacity, but

---

16 Since October 2023, municipalities have had a guideline for online research in maintaining public order. Regarding the National Coordinator for Counterterrorism and Security (NCTV), the Coordination of Counterterrorism and National Security Act is relevant, which was published on 12 December 2023. This law provides the authority to process personal data, originating from publicly accessible sources, under the responsibility of the Dutch Minister of Justice and Security.

this also comes with great flexibility. Searches for missing persons also demonstrate significant capacity. ‘More than a thousand people searching for missing boy’, reads a headline on 13 January 2024, from NOS.<sup>17</sup> Naturally, digitalisation also provides existing organisations with additional organisational capacity, but this does not constitute a fundamental change. Individuals in organisations were already clearly organised. Existing organisations are often modelled as bureaucracies, including larger commercial entities, and therefore have much less flexibility (but often more continuity and status). For the police, the change mainly involves dealing with citizens who can now organise ad hoc and flexibly to either pose a challenge to or contribute to social control in society according to their own judgement and in a coordinated manner. While they have not become part of the police function (as they lack the formal powers that characterise it), they do place that function in a different perspective. By virtue of their ability to coordinate action, they form a new power bloc alongside it.

#### 10.6.2 *Digitalisation and information capacity*

Digitalisation also creates information capacity, particularly benefiting organised collaborations. Citizens who have organised digitally can then work on the information capacity of their organisation. However, information capacity truly thrives in larger organisations with abundant information.

Information about individuals is fundamental for exercising control over them (Foucault, 1975). Without information and ‘files’, corrective government intervention is not possible. Whoever possesses information about citizens holds a significant resource for the police function. Historically, it was primarily the government, including the police, that had information about citizens. Now, it is primarily the larger private companies that have a wealth of information about the daily activities of citizens (their customers or users) – information that is often relevant to the police function. Although the police sometimes manage to obtain large amounts of information about criminals, we must assume that information capacity in the private sector has increased many times more and faster than in the police and other law enforcement agencies. Private organisations barely had information capacity 30 to 40 years ago and now possess an immeasurable amount of (privacy-sensitive) information about citizens, even considering that communication between users of communication apps such as WhatsApp and Signal is encrypted and inaccessible to the service provider. As a result, these organisations do not enter into the police function, but they have become

---

<sup>17</sup> <https://nos.nl/artikel/2504713-meer-dan-duizend-mensen-zoeken-naar-vermiste-jongen-16-jas-gevonden-in-merwede>.

WOUTER STOL, JURJEN JANSEN AND WOUTER LANDMAN

entities with significant resources for that function and therefore also for police work, regardless of whether the police should be allowed to use that information.

The information capacity of organisations can adversely affect individuals when their rights are infringed upon. Society implements legal measures against this, such as the General Data Protection Regulation (GDPR) at the EU level. However, the protection of individual rights also involves monitoring compliance with such rules. Organisations that possess information capacity not only have information that is useful for law enforcement, they should also be actively supervised by organisations that are part of the police function, with an eye on possible misuse of their information capacity.

### 10.6.3 *Digitalisation and normative capacity*

Digitalisation also impacts the normative capacity of organisations, and individuals to some extent. Organisations or individuals who manage or moderate digital platforms enforce certain norms on the platform and can apply sanctions against those who deviate (too far) from them (Bijleveld et al., 2021). In extreme cases, they can remove someone from the platform. More than 20 years ago, Svensson and Van Wijk (2002) showed that online communities are far from normless. In online student groups, they found that illegal copying is acceptable, but hacking and spamming are taboo, as is the spreading of computer viruses. Today, there is ample discussion about algorithms that confirm and reinforce user preferences. It is mainly about influence and not so much about coercion, although sometimes an example is set, such as when Donald Trump was removed from Twitter (the predecessor of X). Normative capacity traditionally lies with authoritative figures in someone's everyday life, such as caregivers, teachers and peers. Due to digitalisation, others have joined, such as influencers and organisations that manage algorithms (see also Schuilenburg, 2023).

Actors in the police function also play a normative role. The police's task in this regard is to enforce the norms established by law when they are violated, even if necessary with violence based on legal powers. Digitalisation has not fundamentally changed this. However, new behaviours have become illegal (e.g. hacking), making old powers (e.g. arrest) applicable to these behaviours, and new powers have been introduced due to digitalisation (e.g. remotely accessing a computer) (Stol & Strikwerda, 2019). What is new is the normative capacity that individuals and organisations have gained through digitalisation and their ability to enforce it with (threats of) sanctions. Due to digitalisation, a group has emerged between informal norm-setting in people's everyday lives (by parents, teachers, friends) and formal norm-setting by the police function (the state), consisting of individuals and organisations with a normative role and sanctioning capabilities. An example is the Dutch public-private partnership called

'Project Online Content Moderation' (PrOCOM).<sup>18</sup> This partnership enables citizens, public parties and private parties (social media platforms in particular) to take action in the case of harmful online content. Algorithms play an increasingly important role in detecting and moderating harmful online content. From the perspective of the police function, the emergence of this 'middle group' has made the societal fabric of social control more complex.

#### 10.6.4 *Digitalisation: altered social relations*

Although our analysis is concise, it leads to the conclusion that societal relations have changed. Individuals and private organisations have gained new opportunities for deviant behaviour and social control. For individuals, this primarily involves the ability to quickly organise ad hoc. Police officers theoretically have this option as well, but in practice they do not, as they operate in accordance with their organisation. For organisations, the new opportunities are mainly related to information capacity. Although the police keep up with the times, they are no longer the organisation that exclusively possesses sensitive information about citizens. Practically speaking, they no longer have a monopoly on organising enforcement or investigative activities, not even on collecting relevant investigative information. The police function concerns social control and thus the enforcement of norms. Traditionally, the police, as the only organisation allowed to do so, and as a last resort, can use force. However, they do not have a monopoly on negative sanctions, let alone on norm enforcement. Due to digitalisation, the normative capacity of individuals (who then become influencers) and organisations has increased, and the ability of organisations to apply sanctions has grown.

The consequence of the changes in organisational, information and normative capacity is that the police function must be shaped within a different power dynamic (see also Van Halderen et al., 2024). For the police, this means that they need to reassess their position in relation to citizens and companies with their newly acquired capacities. We propose initiating a discussion to address this matter.

---

<sup>18</sup> <https://hetccv.nl/themas/cyberveiligheid/online-aangejaagde-ordeverstoringen/project-online-content-moderatie/>.

WOUTER STOL, JURJEN JANSEN AND WOUTER LANDMAN

## 10.7 DISCUSSION: TASK FOR THE POLICE IN THE CHANGED LANDSCAPE OF THE POLICE FUNCTION

### 10.7.1 *New power blocs in a changed landscape*

The landscape in which the police operate has significantly changed: citizens and private organisations now have capabilities they previously did not possess and are fully utilising them. They have not become part of the police function as such, but they do place the police function in an entirely different environment. Citizens and private organisations, through their ability to coordinate actions, form a new power bloc to which the police function, and thus the police, must relate. Private organisations, with their information capacity, have become a party with crucial resources for the police function and therefore for police work, necessitating the police to engage with these organisations. Between the classic informal social control in everyone's everyday life and the formal social control by the police, a new group for social control has emerged, consisting of moderators, influencers and algorithms. They too constitute a new power bloc in the landscape of the police function. Ignoring these developments is not an option, thus prompting the question of how the police function, and specifically the police, should relate to these new groups and positions. In this concluding discussion, building on what we have presented, we provide some starting points that can serve as material for further debate.

Firstly, regarding the role of the police, they are the organisation entrusted by the government to enforce legal rules, if necessary with force. The police hold the monopoly on the use of force. They conduct (formal) social control based on legal rules. They operate subordinate to the authorities and are accountable to them for their work. Democratically elected representatives can hold the authorities accountable. In other words, the police oversee society, and a representation of that society oversees the police. Essential in police work is the balance between state power and civil rights. The same law that gives the police powers also protects citizens against unwanted violations of their rights. The police should safeguard both law enforcement and legal protection; they ensure the correct balance between the two, which must be continually reassessed. Many others in society continuously work on enforcing legal rules. Seen in this light, the role of the police is limited and often merely supplementary, but – as the final enforcement authority with enforcement power and with attention to the balance between law enforcement and legal protection – no less important.

Even as society changes due to digitalisation, the essential role of the police remains as outlined in the previous paragraph. However, digitalisation has led to a change in the landscape of the police function, requiring the police to respond. Not so much to secure their own position in a power struggle, but to allow the policing role and the relationships within our rule of law to evolve with the times. Three themes primarily demand the attention of the police for this purpose: collaboration, an integrated approach to online crime, and safeguarding legal protection.

### 10.7.2 Collaboration

Collaboration refers, first and foremost, to working together with citizens and organisations due to their increased capabilities in law enforcement (organisational, information and normative capacity). Lam and Kop (2020) advocate, in response to the Anne Faber case (see section 10.4.2), for a collaborative model that encompasses both citizen and police participation. This development is underway. The police are open to collaborations but also have reservations due to principles related to democratic control and decency in law enforcement, and rightfully so, as it is their role. A crucial question here is whether the police should only collaborate ad hoc with individual groups of citizens and organisations or whether they want to regulate the area. The latter may seem somewhat strange in what appears to be a chaotic playing field, but it is certainly partly a realistic option. When the police collaborate with a particular law enforcement initiative, and the initiative thereby becomes structural, it channels similar initiatives that follow. For example, the police collaborate with the two mentioned organisations for citizen search actions in missing person cases (the VST and the CPV), and it seems unlikely that more such permanent organisations will emerge. Both the VST and CPV also call for new citizen initiatives to be reported to them, thus working towards regulation. Therefore, the police must develop policies on whether and how they, from their role, want to regulate the field of and around the police function in response to law enforcement initiatives.

The theme of collaboration is also linked to cooperation with law enforcement organisations from other countries and to national or international collaboration with private organisations with information capacity. For the police, it is first and foremost important to uphold the principles of legal protection. The accusation of jurisdiction (s)hopping should not be possible, and collaboration with private companies must comply with prevailing norms for legal protection.

Finally, regarding collaboration, we note that while the police do collaborate with WhatsApp neighbourhood watch groups which are ubiquitous in society, they typically do not participate in the groups themselves but maintain contact with the group administrators. There are good reasons for this, such as participation in a group suggesting that every message posted in the group is officially brought to the attention of the police. Capacity constraints also play a role. At the same time, there is reason to thoroughly evaluate this policy choice. It is in tension with the principle of knowing and being known. The current system gives the police a face with the administrator, but they remain anonymous to all other participants, and thus to the majority of residents in the neighbourhood.

### 10.7.3 *Integrated approach*

Online crime is prevalent and even, if we could count all online offences, likely the 'most common crime'. Combating online crime by simply handling 'digital cases' is a futile path. Kop (2012) advocates for a shift from conducting criminal investigations to crime-fighting. The latter is a wider concept and explicitly includes addressing the issue at its source. This primarily involves prevention policies where various public and private actors play a significant role. Prevention includes the ability among potential victims to resist crime, both in terms of knowledge and behaviour and in terms of the organisational and technical aspects. Additionally, legislation (e.g. from the EU) addresses this, ensuring that privacy and security are taken into account in the design process of technology.<sup>19</sup>

Fighting crime, alongside prevention, also involves relatively new strategies such as disrupting crime. In the Netherlands the police's Team High Tech Crime (THTC) works with analyses aimed at detecting nodes or crucial services for committing online crime, to then address them – thus not only handling individual cases but also preventing new offences by disrupting the system. For some time now, the THTC has had a Cyber Offender Prevention Squad (COPS). While handling cases has not been abolished, specialists now clearly focus more than before on preventing people from becoming offenders and on disrupting the criminal infrastructure. While these specialists seek different paths, paradoxically districts and local police units are asked to handle more (simple) online crime cases. For the police, it is now essential to develop an integrated approach to online crime – integral in terms of tailored combinations of detection, prevention (including resilience) and disruption, both nationally and at district and basic team levels. Collaborations are crucial in this regard. However, prevention and disruption aimed at law enforcement must always take into account the boundaries set by legal protection and/or by civil rights.

Preventive policy regarding social disorder is more complicated than prevention regarding crime, because with prevention of social disorder tensions arise with legal protection requirements earlier than with crime prevention, for example in relation to protecting the right to privacy, assembly and demonstration. Our plea for an integrated approach does not concern preventing online-driven disorder. However, the police must develop practices, taking legal protection into account and in line with the motto 'know and be known', to anticipate online-driven disorder as effectively as possible. While the police have Teams for Public Order Intelligence (in Dutch: Teams Openbare Orde Inlichtingen or TOOI), they are currently criticised for violating civil rights while

---

19 See, for example, <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>.

collecting information. There appears to be a lack of democratic control over the work of these teams, according to, for example, Amsterdam City Council.<sup>20</sup> To some extent, the police (as well as society and politics) will simply have to accept that disturbances may occur more unexpectedly than before because an all-knowing police force is not an option.

#### 10.7.4 *Safeguarding legal protection*

As the third theme that requires attention from the police, we mentioned safeguarding legal protection i.e. defending human rights, or rather, decent law enforcement. Citizens and organisations that utilise digital means for exercising social control can thereby infringe upon the rights of others and thus cross ethical boundaries themselves. They may even become subjects of corrective actions. According to Bijleveld et al. (2021), concerning offences, alternative (civil-law-based) resolutions seem to be more common. They wonder in this context whether this trend means that some offences are becoming 'de facto unpunished'. Or, as we add, not unpunished, but rather addressed outside the formal criminal justice system.

Stol (2021) emphasises that, especially in relation to digitalisation, it is the police's responsibility to ensure decent law enforcement. We referred to this as safeguarding the balance between law enforcement and legal protection. Given all the initiatives that citizens and organisations, such as tech giants, can take due to digitalisation and their acquired capabilities, more attention is required for safeguarding legal protection. Activities that citizens and organisations can undertake due to their new capabilities are not subject to an authority and democratic control as is customary in criminal justice proceedings. For example, someone who is banned from a social media platform can indeed turn to the courts, and someone deprived of their freedom by a vigilante group can file a complaint. However, a passive stance from the police, merely observing without taking action, seems too reactive. A more proactive approach is preferable because it concerns the essentials of our legal system. The police, therefore, should take the lead in the public discussion on digitalisation, the landscape that is changing as a result in and around the police function, and the legal protection of citizens.

---

<sup>20</sup> NRC, 24 January 2024, p. 8.

## REFERENCES

- Bantema, W., & Buitenhuis, M. (2023). Burgemeester: Sheriff van het internet? [Mayor: Sheriff of the Internet?]. *Het Tijdschrift voor de Politie*, 2, 42-45.
- Bantema, W., Westers, S., & Munneke, S. (2020). *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen*. [Not authorized, yet responsible? Enforcement options for online-incited public disturbances]. Boom bestuurskunde.
- Bantema, W., Westers, S., Hoekstra, M., Herregodts, R., & Munneke, S. (2021). *Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk* [Black box of municipal online monitoring: A shaky foundation under a solid practice]. Sdu Uitgevers.
- Bartelds, A., Vries, S. de, Postma, L., Bantema, W., & Greijdanus, H. (2023). *Preventie van online aangejaagd geweld. Een praktijkverkenning naar de online werkwijze van jongerenwerkers en politie in Amsterdam Zuid-Oost* [Prevention of online-incited violence. An exploration of the online methods of youth workers and police in Amsterdam South-East]. NHL Stenden Hogeschool/Rijksuniversiteit Groningen.
- Bijleveld, C., Salet, R., Damstra, A., & Stéfanovic, D. (2021). *Politiefunctie in een veranderende omgeving* [Police function in a changing environment]. Wetenschappelijke Raad voor het Regeringsbeleid.
- Borwell, J., Jansen, J., & Stol, W.P. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research*, 3(3), 85-110.
- Brodeur, J.-P. (2010). *The policing web*. Oxford University Press.
- Cachet, A. (1990). *Politie en sociale controle* [Police and social control]. Gouda Quint.
- CBS (2022). *Veiligheidsmonitor 2021* [Safety monitor 2021]. Dutch Statistics.
- Cohen, M.J., Brink, G.J.M., Adang, O.M.J., Van Dijk, J.A.G.M., & Boeschoten, T. (2013). *Twee werelden: You Only Live Once* [Two worlds: You Only Live Once]. Commissie 'Project X' Haren.
- Commissie Waarborgen Werken Onder Dekmantel (2023). *Waarborgen voor heimelijk werk: Onderzoek van de commissie Waarborgen Werken Onder Dekmantel* [Guarantees for covert operations: Research by the Commission on Guarantees for Undercover Work]. Pencilpoint.
- COT (2021a). *Ongekende ongeregeldeheden: Leerevaluatie naar aanleiding van de ongeregeldeheden in Eindhoven van 24 januari 2021* [Unprecedented disturbances: Learning evaluation following the disturbances in Eindhoven on 24 January 2021]. COT.
- COT (2021b). *Een machteloos gevoel: Leerevaluatie naar aanleiding van de ongeregeldeheden in Den Bosch op 25 januari 2021* [A feeling of powerlessness: Learning evaluation following the disturbances in Den Bosch on 25 January 2021]. COT.

- De Vries, S., & Bantema, W. (2022). *Aanpak in kaart: Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen* [Approach described: Insight into a regional approach to online-driven public disturbances]. NHL Stenden Hogeschool.
- Emmen, B., De Poot, C.J., & Stol, W.P. (2023). Politieoptreden op het darkweb [Police operations on the dark web]. *Tijdschrift voor de Politie*, 85(2), 32-35.
- ENISA (2017). *Cyber security and resilience of smart cars*. European Union Agency for Cybersecurity.
- Europol & Eurojust (2019). *Common challenges in combating cybercrime*. <https://www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime>.
- Foucault, M. (1979 [1975]). *Discipline and Punish; the Birth of a Prison*. Vintage Books.
- Greijdanus, H., Postmes, T., Bartelds, A., Postma, L., De Vries, S., & Bantema, W. (2023). *Interventies in de cyclus van online aangejaagd geweld: Inzichten uit een literatuurreview* [Interventions in the cycle of online-incited violence: Insights from a literature review]. Rijksuniversiteit Groningen/NHL Stenden Hogeschool.
- Haane, T.H., & Heijboer, H.J. (1965). Criminaliteitsbestrijding in een veranderende maatschappij [Combating crime in a changing society]. *Tijdschrift voor de Politie*, 1965(3), 61-74.
- Heijder, A. (1989). *Management van de politiefunctie* [Management of the police function]. Van den Brink and Gouda Quint.
- Higgins, E. (2021). *Wij zijn Bellingcat. Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden* [We Are Bellingcat. How Ordinary People Became the Investigative Journalists of the Future]. Het Spectrum.
- Jansen, J., Van Valkengoed, T., Veenstra, S. & Stol, W.P. (2020). *Level-Up! Kennis voor politiewerk in een digitale samenleving* [Level-Up! Knowledge for police work in a digital society]. Cybersafety Research Group.
- Jansen, J., Westers, S., Schreurs, W., Berkenpas, M., Alpár, G., & Stol, W.P. (2023). *De rol van encryptie in de opsporing. Belemmeringen en mogelijkheden* [The role of encryption in investigations: Obstacles and opportunities]. Cybersafety Research Group.
- Jansen, J., Westers, S., Twickler, S., & Stol, W.P. (2019). *Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing* [Purchase fraud from abroad: Alternatives for detection]. Sdu Uitgevers.
- Kop, N. (2012). *Van opsporing naar criminaliteitsbeheersing. Vijf strategische implicaties* [From criminal investigation to crime control. Five strategic implications]. Boom Lemma uitgevers.
- Lam, J., & Kop, N. (2020). *Schouder aan schouder: Burger- en politieparticipatie tijdens de vermissing van Anne Faber. Leerpunten uit de samenwerking tussen burgers en politie* [Shoulder to shoulder: Citizen and police participation during the disappearance of Anne Faber. Lessons learned from cooperation between citizens and police]. Politieacademie.

- Landman, W., & S. Groothuis (2022). *Politiewerk op het web: Een verkennend onderzoek naar online gegevensvergaring door de politie* [Policing on the web: An exploratory study of online data collection by the police]. Sdu Uitgevers.
- Landman, W. (2023). *Politiewerk aan de horizon: Technologie, criminaliteit en de toekomst van politiewerk* [Policing on the horizon: Technology, crime and the future of policing]. Sdu Uitgevers.
- Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven International Publishers.
- Lub, V., & De Leeuw, T. (2019). *Politie en actief burgerschap: een veilig verbond? Een onderzoek naar samenwerking, controle en (neven)effecten* [Police and active citizenship: a safe alliance? A study into cooperation, control and (side) effects]. Sdu Uitgevers.
- Meijer, A., & Wessels, M. (2019). Predictive policing: review of benefits and drawbacks. *International Journal of Public Administration*, 42(12), 1031-1039.
- Moors, H., Klarenbeek, L., Berger, E., Dückers, M., Van Duin, M., Kist, G., Luesink, M., Schrijvenaars, T., & Van der Wijngaart, M. (2022). *‘Avondklokrellen’: lokale dynamiek in een mondiale crisis. Analyse van de voedingsbodem van de ordeverstoringen in vier Noord-Brabantse steden* [‘Curfew riots’: local dynamics in a global crisis. Analysis of the breeding ground for the disturbances in four North Brabant cities]. EMMA.
- NCTV (2022). *Cybersecuritybeeld Nederland (CSBN) 2022*. Nationaal Coördinator Terrorismebestrijding en Veiligheid.
- Oerlemans, J.-J., & Royer, S. (2023). The future of data-driven investigations in light of the Sky ECC operation. *New Journal of European Criminal Law*, 14(4), 434-458.
- Prins, J.E.J., Schrijvers, E.K., Passchier, R., & De Visser, M. (2019). *Voorbereiden op digitale ontwrichting* [Preparing for digital disruption]. Wetenschappelijke Raad voor het Regeringsbeleid.
- Roks, R., & Monshouwer, N. (2020). F-gamers die ‘mapsen’, ‘swipen’ en ‘bonken’: Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger [F-gamers who’re ‘mapping’, ‘swiping’ and ‘bonking’: A netnographic study of fraud and scams on Telegram Messenger]. *Justitiële Verkenningen*, 2, 44-58.
- Ruiter, S., Van Leuken, M., Van Ruitenburch, T., Schiks, J., & Leukfeldt, R. (2023). *In- en doorstroom van online criminaliteit in de strafrechtketen* [In- and throughflow of online crime in the criminal justice system]. Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.
- Schuilenburg, M. (2023). Big data policing. Schets van de belangrijke vraagstukken, partijen en nieuwste trends in de praktijk [Big data policing. Outline of important issues, parties and latest trends in practice]. In T. Snaphaan, W. Hardyns, A. van Dijk, R. Spithoven & R. van Brakel (Eds.), *Big data policing* (pp. 53-70). Gompel & Svacina.
- Stol, W.P. (1996). *Politie-optreden en informatietechnologie: Over sociale controle van politiemensen* [Police behavior and information technology: On social control of police officers]. Koninklijke Vermande.

- Stol, W.P. (2003). Sociale controle en technologie. De casus politie en kinderporno op het internet [Social control and technology. The case of police and child pornography on the internet]. *Amsterdams Sociologisch Tijdschrift*, 30(1/2), 162-182.
- Stol, W.P. (2010). *Cybersafety overwogen: Een introductie in twee lezingen* [Cybersafety considered: An introduction in two lectures]. BJu.
- Stol, W.P. (2020). Digitalisering en criminaliteit: Een beknopte inleiding op cybercrime [Digitalisation and crime: A brief introduction to cybercrime]. *Cahier Politiestudies*, 2020(3), 13-22.
- Stol, W.P. (2021). Digitalisering en de rol van de politie: Naar een 'autoriteit fatsoenlijke rechtshandhaving' [Digitalisation and the role of the police: Towards an 'authority for decent law enforcement']. *Panopticon*, 42(2), 161-168.
- Stol, W.P., Van Treeck, R.J., & Van der Ven, A.E.B.M. (1999). *Criminaliteit in cyberspace: Een praktijkonderzoek naar aard, ernst en aanpak in Nederland* [Crime in cyberspace: A practical study into its nature, severity and approach in the Netherlands]. Elsevier.
- Stol, W.P., & Strikwerda, L. (2019). *Law Enforcement in Digital Society*. Eleven International Publishing.
- Stol, W., Jansen, J. & Landman, W. (2024). Digitalisering en de politiefunctie: hoe het speelveld verandert en wat dat van de politie vraagt. [Digitalisation and the police function. How the playing field is changing and what it demands of the police.] *Tijdschrift voor Veiligheid*, 23(1-2), 53-70.
- Svensson J.S., & Van Wijk, A.Ph. (2002). *Informeel sociale normering op het internet* [Informal social norms on the Internet]. IPIT/NPA.
- Svensson, J.S., & Zouridis, S. (Eds.) (2004). *Waarden en normen in de virtuele wereld: Twee verkennende studies met discussie* [Values and norms in the virtual world: Two exploratory studies with discussion]. IPIT.
- Van den Berg, E., Hermans, C., & Quast, J. (2012). *Politiefunctie in perspectief: Instrumenten voor toekomstgericht denken over de maatschappelijke functie van de politie* [Police function in perspective: Instruments for future-oriented thinking about the societal role of the police]. Dutch Ministry of Safety and Justice (Directe Strategie).
- Van den Eeden, C.A.J., Van Berkel, J.J., Lankhaar, C.C., & De Poot, C.J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit* [Detecting, prosecuting, and stopping cybercrime]. Dutch Scientific Research and Document Center (WODC).
- Van der Wagen, W. (2018), *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actornetwork theory*. PhD thesis, Rijksuniversiteit Groningen.
- Van Halderen, R.C., Tjoelker, R. & Spithoven, R. (2024). Met gezag online. Online schadelijk gedrag, publieke waarden en de politiefunctie [With authority online. Online harmful behavior, public values, and the police function]. *Cahiers Politiestudies*, 2024(70), 185-200.

WOUTER STOL, JURJEN JANSEN AND WOUTER LANDMAN

Van Steden, R., Roelofs, M., & Heijnen, M. (2009). *Pluriforme politiefunctie. Inventarisatie van en burgerpercepties over beveiligers, toezichhouders en handhavers* [Pluriform police function. Inventory of and citizen perceptions of security guards, supervisors and enforcers]. Vrije Universiteit Amsterdam.

VST (2019). *Stichting Veteranen Search Team. Jaarverslag 2018* (Annual report 2018). Verkregen via: [www.veteranensearchteam.nl](http://www.veteranensearchteam.nl).

# 11 EFFICACY OF THE DUTCH GENERAL MUNICIPAL BYLAW IN COMBATING ONLINE TROUBLEMAKERS\*

Willem Bantema

## Abstract

*This chapter examines the effectiveness of the Dutch General Municipal Bylaw (Algemene Plaatselijke Verordening, APV) in addressing public disturbances incited online, using administrative law. It focuses on recent developments in the cities of Almelo and Utrecht. The increasing role of social media in promoting public disorder, as witnessed in incidents such as the 2021 curfew riots and COVID-19-related protests, has raised concerns. Almelo's efforts to introduce explicit regulations targeting online behavior pose both legal and practical challenges, particularly in how municipalities can govern virtual spaces under local law. Through case studies, including Utrecht's initiative to impose periodic penalties for inflammatory online statements, this chapter explores the potential and limitations of using the APV to tackle online disruptions. A comparison with Belgium's approach, where Brussels has explicitly extended police regulations to virtual spaces, highlights key differences. The analysis addresses important legal challenges, particularly the potential conflict with freedom of expression under Dutch constitutional law, which limits municipalities' ability to restrict fundamental rights. The chapter concludes by evaluating whether local bylaws can effectively regulate online-incited disturbances and offers specific suggestions for amending the APV to create a legally robust framework for governing online behavior.*

## 11.1 INTRODUCTION

'Almelo now wants to be able to act against online public disorder.' This headline of the Almelo municipality's press release on 1 December 2022 (Wennekes, 2022) reflects the growing concern over online calls for public disorder. The municipality has faced such issues during the farmers' protests and curfew riots at the height of the COVID-19 pandemic. Recognising that social media and other online platforms can

---

\* This chapter has previously been published in Dutch in *Computerrecht* (see Bantema & Twickler, 2023). Permission has been granted to publish in English with a reference.

WILLEM BANTEMA

instigate public disturbances,<sup>1</sup> the mayor aims to take preventive measures. Consequently, Almelo has advocated for the use of administrative powers online and has included an explicit provision in the General Municipal Bylaw (Algemene Plaatselijke Verordening, APV) to criminalise online behaviour that may disturb public peace. This chapter explores the efficacy of the Dutch General Municipal Bylaw in addressing online-incited disturbances through administrative law.

This local perspective on a global issue is unique. Literature shows that authoritarian national regimes such as China, Cuba, Iran, Syria, Turkey and Vietnam take extensive measures to regulate social media by blocking platforms and censoring information online (Tuncay, 2018). Censorship practices vary widely across different countries (Ververis et al., 2019). This chapter focuses on the approach of local governments based on local regulations, with an emphasis on social media users rather than platform regulation. The central question in this chapter is: *To what extent can the municipality use the General Municipal Bylaw to act against online-incited disturbances, and, if possible, how can such an article be designed textually?*

This chapter consists of seven sections. Section 11.2 focuses on the administrative law background in the Netherlands, and section 11.3 outlines the context in which online-incited disturbances occur (with international examples). Section 11.4 provides the background to the studies and methods on which this chapter is based. The results are presented in section 11.5, which discusses a case in Utrecht where the General Municipal Bylaw was deployed. Section 11.6 examines the Belgian method, in which all articles from the General Police Regulations (similar to the Dutch General Municipal Bylaw) are declared applicable to the virtual domain. Section 11.7 translates the insights from Belgium to the Dutch situation and proposes textual suggestions for a new General Municipal Bylaw article in the Netherlands. The chapter concludes in section 11.8 with a brief discussion and conclusion.

## 11.2 LEGAL BACKGROUND

As of 12 June 2024, the Netherlands comprises 342 municipal authorities. These authorities perform many tasks, including registering residents, building roads and footpaths, providing social services, and maintaining law and order. Mayors are generally responsible for maintaining law and order, crisis management and representing their councils at the national and international levels. In emergencies, the mayor leads the crisis team. A mayor is a non-elected administrative authority appointed by the monarch and the Minister of the Interior, so-called the Crown (*de Kroon*), for a period of six years. The rules concerning the governing bodies of municipalities (council, executive and

---

1 Here and hereafter, ‘municipality’ refers to mayor or college of mayors and councillors.

mayor) are defined in the Municipalities Act (Gemeentewet). In contrast to the General Municipal Bylaw, the Municipalities Act is established by the national government. The mayor chairs both the executive board and the legislative council of the municipality and is responsible for safety and public order. On behalf of the municipality, the mayor has many powers to intervene in public disturbances and contribute to the prevention of disturbances.

The General Municipal Bylaw lays down the municipal regulations on public order and safety. Each Dutch municipality has its own General Bylaw, which applies to everyone in the municipality. The rules in the General Bylaw stipulate whether residents require a permit for certain activities (Rijksoverheid, 2024). The General Bylaw describes various rules that apply in the municipality and includes rules on, for example, events, use of fireworks, nuisance and rowdiness. Examples of administrative powers to regulate public order and safety include a periodic penalty (a sum imposed to provide an incentive for undertakings to comply with a decision in a timely manner and to prevent future offences), an area ban (the creator of a nuisance is banned from a specific area for a set period) and an administrative power to take control of houses used for criminal activities such as drug trafficking. At the local level, the police act under the authority of the mayor in matters of public order (administrative law), and where criminal enforcement is concerned, the police act under the authority of the district attorney.

### 11.3 SOCIETAL AND ADMINISTRATIVE BACKGROUND

#### 11.3.1 *Examples of online-incited disturbances*

The example of the municipality of Almelo is not an isolated one. In recent years, Dutch municipalities have regularly faced public order disturbances organised and driven through social media. One of the most widely known examples was the party in Haren that was organised online (Project X) in 2012 (Tweede Kamer der Staten-Generaal, 2013). Haren is a village of 20,000 residents near the town of Groningen (in the northern part of the Netherlands). In September 2012, a 15-year-old girl accidentally posted an open Facebook invitation to her 16th birthday party. Facebook users broadcast the message, and thousands of youths heeded the call. The mayor tried to stop them by spreading a social media message stating in effect that there was no party. However, between 3,000 and 5,000 people assembled, resulting in severe disturbances, including the destruction of shopfronts and robberies. Project X (Haren) was a wake-up call for local authorities regarding the role of social media and their relationship to public order and safety.

In recent years, the relationship between online behaviour and municipal public order has become more apparent. The best-known recent example concerns the curfew riots of January 2021, which took place in many municipalities in the Netherlands and

WILLEM BANTEMA

caused significant damage. These riots were not unique to the Netherlands. Measures were taken worldwide to prevent the spread of COVID-19, and people in other countries also disagreed with their governments' measures, such as school closures, compulsory working from home and restrictions on large gatherings. This culminated in demonstrations and sometimes violence (Wood et al., 2022). Other examples include football hooligans, organised mass fights and social unrest around fake news. One might also consider unrest related to paedophiles in residential areas, unrest related to the potential establishment of asylum centres and the polarisation of population groups on local Facebook pages or X (formerly Twitter).

Currently, several farmer protests and actions are being organised through social media. In the academic literature, most examples involve protests and the use of social media for organising demonstrations and (violent) protests (Briggs, 2012; Treadwell et al., 2013). The legal discussion is different regarding demonstrations and protests, but the line between reasonable demonstration and riots is sometimes thin, as seen in practice and in the British studies mentioned. One can also observe a clear influence from social media influencers on public order and safety. In May 2024, a TikTok influencer named Oracle caused chaos in a park in Zurich by dropping 24,000 Swiss francs (about 25,000 euros) in banknotes from a drone over a crowd. The action resulted in injuries to a young bystander, and the police are now looking for witnesses (De Jager, 2024). In another case, during the Champions League final (football), three pitch invaders stormed the Wembley turf after being promised £300,000 by a controversial Russian influencer (Elson, 2023).

### 11.3.2 *Research and administrative developments*

In 2018, there was still reluctance among mayors to take an active role in preventing online-incited disturbances (Bantema et al., 2018). More recent research, however, even before the COVID-19 pandemic, has shown that increasing numbers of mayors see an active role for themselves. For example, 71% of mayors feel responsible for preventing online-incited disturbances (Bantema et al., 2018). Mayors feel they have a limited repertoire for action, however, as they have no explicit powers to intervene preventively online (Bantema, Westers & Munneke, 2020). At the same time, they can be held administratively responsible for the public order consequences of a disruption (Article 172 of the Municipalities Act). Calls for powers to intervene preventively online seem to be increasing in recent years (NRC, 2023).

In one study (Bantema, Westers & Munneke, 2020), half of the mayors questioned indicated that they would consider imposing a periodic penalty on online comments expected to lead to disorder. The legal analysis in the same study showed that this would not be possible, however, because, among other things, a legal regulation is not being violated (Bantema, Westers & Munneke, 2020). Bantema et al. (2018) also show

that fundamental rights, jurisdictional problems, legislation focusing on the physical (local) domain and an unclear relationship between online comments and public order are among the reasons the mayors cannot apply their powers online.

Because municipalities had relatively little experience with public order disturbances instigated online, the discussion of administrative law powers in the online domain was seen by many as a scholarly or even legal-philosophical discussion. This was the case until 2021, when several municipalities experienced public order disruptions instigated online. Some municipalities seized on these events to experiment with their powers by imposing periodic penalty payments to prevent a repeat of these disturbances. One example is the periodic penalty in the municipality of Utrecht in November 2021, on which the District Court of the central part of the Netherlands (Rechtbank Midden-Nederland) has now ruled (Gemeente Utrecht, 2021; Rechtbank Midden-Nederland, 2023).

The research underlying this chapter started in 2020, before municipalities experimented with applying administrative law powers online (Bantema, de Vries & Twickler, 2022). It is worth noting that, unlike in many other countries, mayors in the Netherlands have many powers to maintain public order. In the study, commissioned by the District Security Consultation IJsselland, various administrative law options for dealing with online-incited disturbances were discussed. This chapter is limited to the possibilities offered by the General Bylaw as a basis for administrative law enforcement online. The question is to what extent it is possible to set out rules with prohibitions and/or restrictions on online conduct at the local community level and what these rules might look like. Scientific knowledge about this topic is still limited, yet its relevance and social urgency are high. The central question is: *To what extent can the municipality use the General Municipal Bylaw to act against online-incited disturbances, and, if possible, how can such an article be designed textually?*

In the Netherlands, the police are under the authority of mayors (for the administrative approach) and the district attorney (for the criminal approach). This chapter deals with the administrative approach, where the police have an executive task by order of the mayor to maintain public order and safety.

#### 11.4 METHODS

The data used in this chapter were collected on behalf of the IJsselland region in the eastern part of the Netherlands, which wanted more insight into the possibilities offered by the General Municipal Bylaw. The study consists of a legal analysis/source study and an empirical part including interviews and focus groups. For the practical exploration (phase 1), five interviews were held with municipalities in the IJsselland region. In these interviews, attention was paid to the municipalities' views on administrative

WILLEM BANTEMA

law enforcement and the possibilities and shortcomings of the General Municipal Bylaw. Additionally, three interviews were held with Dutch municipalities outside the region that have experimented with an administrative law approach to online-incited disturbances. Another in-depth interview was held to gain more insight into the design and considerations of the Brussels ‘virtual’ Bylaw article.

Finally, for the review of phases 1 and 2, an expert meeting was held with three legal experts, and a focus group was held with municipal lawyers (predominantly from the region) to present the legal routes (phase 2) and reflect on their implementation/enforcement (phase 3). The legal source research was based on legislation, case law, annotations and literature. The data collection took place between December 2021 and April 2022.

To paint the most reliable and objective picture possible, legal experts were consulted, and the results of these sessions were incorporated into the report. The practical and legal source research and interviews illuminate the issue from multiple angles, which benefits the independence and validity of the study.<sup>2</sup>

#### 11.5 DESCRIPTION OF THE ADMINISTRATIVE GENERAL BYLAW EXPERIMENT IN THE CITY OF UTRECHT

##### 11.5.1 *Case study description*

The case in the city of Utrecht, described here as an example, was analysed using literature research. The mayor of the municipality of Utrecht imposed a periodic penalty on a resident of the municipality of Zeist. A pamphlet had been distributed with a picture of Canal Street (Kanaalstraat) and the text ‘Utrecht in revolt! Bring your mates and fireworks.’ The person was tracked down and detained, and the periodic penalty was imposed to prevent a repeat of the online sedition. The person had to refrain from posting messages online (on social media) that could lead to disorder. Prohibited messages included calls aimed at disturbing public order in the municipality where the effect of the resident’s digital expression occurred (i.e. in the other municipality). If this individual did not comply with the periodic penalty, he forfeited a fine of €2,500 (Gemeente Utrecht, 2021). This forfeiture did not take place, and the mayor of Utrecht has since withdrawn the measure (RTV Utrecht, 2022).

---

2 For more details see Bantema et al. (2022).

### 11.5.2 *Basis of the measure*

The administrative measure was based on Article 125(3) of the Municipalities Act and Article 5:32(1) of the General Administrative Law Act. From these articles, the mayor derives the power to impose a periodic penalty. In this case, a periodic penalty was imposed on the person concerned, because his provocative behaviour caused disorder (i.e. calling for riots), which is punishable under Article 2.2, paragraph 1(g) of the General Municipal Bylaw 2010 of the municipal authorities. The relevant provision reads as follows:

Without prejudice to the provisions of Articles 424, 426a and 431 of the Penal Code, it is forbidden in or on a public place or in a building accessible to the public, in any way: (a) to disturb order; (b) to behave in a nuisance manner; (c) to harass persons; (d) to fight; (e) to take part in a gathering; (f) to intrude unnecessarily; or (g) to incite disorder by provocative behaviour.

The Utrecht municipality further states that it has no independent power to monitor the online messages of the person concerned. This is instead achieved through the powers of the investigative authorities. According to the municipality, inflammatory messages are traced by the investigative authorities. These authorities can use all powers available to them under the Code of Criminal Procedure. The municipality assumes that, in this way, any future inflammatory statements by the person concerned will come to light and the periodic penalty will be enforced. In this sense, it works no differently from a regular area ban, according to the Utrecht municipality. A person on whom a restraining order is imposed may not enter the designated area. An investigating officer must establish that the person was in the area in question to establish that the area ban has been violated (Gemeente Utrecht, 2021).

### 11.5.3 *Case law and literature*

#### 11.5.3.1 *Limitations on Article 7 by central government legislation*

Direct criticisms of the Utrecht case in the literature include the contention that the provocative behaviour consisted of inciting riots via a computer, and therefore the freedom of expression of Article 7 of the Dutch Constitution is at stake. It has been argued that by applying the mayor's administrative sanction, freedom of expression is unlawfully restricted by taking the General Municipal Bylaw article as the basis for sanctioning the conduct. According to the restriction system of the Dutch Constitution, only the national government is allowed to restrict fundamental rights.

This General Municipal Bylaw article focuses on the concept of challenging behaviour. The question is whether challenging behaviour is a form of expression as

WILLEM BANTEMA

referred to in Article 7 of the Constitution. A Supreme Court judgment of 28 May 2020 (ECLI:NL:HR:2002:AE1494) ruled on this issue. The case concerned the gathering ban in the General Municipal Bylaw of the municipality of Tilburg, in which challenging behaviour was (also) punishable as stated. The case involved participating in riots at a football match. The defendant's counsel invoked Article 12(3) of the International Covenant on Civil and Political Rights (ICCPR) and Article 2(3) of the Fourth Protocol to the European Convention on Human Rights (ECHR), both of which address the fundamental right to freedom of movement. Both articles state that restrictions on this right are not permitted except those which are, among others, 'provided by law and are necessary to protect national security and public order'. Rulings based on these articles have clarified that legal restrictions imposed by municipalities may limit the fundamental rights referred to in these treaty articles, provided they are established by law and necessary to protect public order. As a treaty is of a higher legal order, it supersedes the Dutch Constitution and its limitations on local laws regarding fundamental rights.

The rulings state that neither article requires that the restriction of the fundamental right must be included in a national law, as the Constitution does in certain articles on fundamental rights. It has been argued that when restrictions are contained in an order based on a prohibition provision of the General Municipal Bylaw, the court can assume that the 'provided by law' requirement, as expressed in the above-mentioned international law articles, has been met (Kortman et al., 2016, pp. 401-402), even though it concerns local law. In the above-mentioned Supreme Court ruling, the General Municipal Bylaw article of the municipality of Tilburg was binding. It was also argued in this case that the General Municipal Bylaw article of the municipality of Tilburg was contrary to the aforementioned international law provisions, because it was drafted too broadly and too vaguely. In this judgment, the Supreme Court considered that a certain vagueness in the description of the offence was necessary, because disturbance of public order has a multitude of manifestations (Hoge Raad, 2002).

In summary, prohibiting 'challenging behaviour' is not necessarily an impermissible curtailment of freedom of speech that would only be permitted by a law of the central government, but there is not much case law on this point.

### 11.5.3.2 *Specificity of Utrecht's General Municipal Bylaw article*

The question here is whether Article 2.2 of the General Municipal Bylaw of the municipality of Utrecht and Article 125, paragraph 3 of the Municipalities Act, in conjunction with Article 5:32, paragraph 1 of the General Administrative Law Act, are sufficiently specific to restrict a fundamental right. In his article, Teunissen (2009) refers to case law in which the administrative judge frequently allows government action, whereas, according to Kortmann, the government action is in violation of, in particular, the principles of legality and speciality, by which government action requires a specific legal basis (Bantema, Twickler & De Vries, 2022).

These conflicting opinions show that there is division and ambiguity among legal experts about how specific the regulations from the General Municipal Bylaw should be to potentially restrict fundamental rights in certain circumstances. The Central Netherlands District Court did not address this issue in its ruling, however, because it stated that the action of the municipality of Utrecht was without a doubt in violation of Article 7 of the Constitution (Rechtbank Midden-Nederland, 2023).

#### *11.5.3.3 Extent of disorder*

There is also the question of the extent of the disorder (brought about by the challenging behaviour). That there was disorder is evident. The weekends of 20 and 27 November 2021 were fraught with disorderliness throughout the country because of the aforementioned pandemic restrictions. However, the periodic penalty in the municipality of Utrecht is based not on the right to freedom of movement, as in the case of the municipality of Tilburg (and as formulated in Article 12 ICCPR and Article 2 of the Fourth Protocol to the ECHR), but on freedom of expression (i.e. Article 7 of the Dutch Constitution). According to the limitation system in the Dutch Constitution, restrictions are only allowed by law of the national government. The Penal Code, established by the central government, contains such a provision in Article 131, which prohibits incitement (to disturb public order). The General Municipal Bylaw is established by a local government, not the national government, and in principle cannot restrict freedom of expression. This argument recurs often: municipalities cannot restrict fundamental rights through the General Municipal Bylaw, because only the national government is allowed to do so and only in certain circumstances.

#### *11.5.3.4 Conflicting views of the municipality and legal experts*

Brouwer and Schilder are of the opinion that in the Utrecht case, the mayor's decision cannot be upheld because of the restrictive system of the Dutch Constitution and because the periodic penalty implies censorship and is therefore contrary to the freedom of expression (Brouwer & Schilder, 2022). Monitoring the order to refrain from posting content online that could incite disruption to public order requires a substantive test of the expressions. According to the municipality, there is no question of censorship or interference with the expression, because the penalty is only forfeited at the moment the person concerned makes further calls aimed at disturbing public order in the municipality of Utrecht. The person concerned may therefore express any opinion, but within the limits of the law. The spreading of inflammatory messages is seen as contrary to the law, and the periodic penalty is therefore justifiable, according to the municipality (Gemeente Utrecht, 2021). The investigating authorities are charged with supervising compliance with the order by the person concerned, and they can make use of the powers in the Code of Criminal Procedure. The municipality, it says, has no independent power of its own to supervise online offences (Gemeente Utrecht, 2021). The court confirmed this reasoning in its ruling (Rechtbank Midden-Nederland, 2023, considerations 8-11).

WILLEM BANTEMA

It is interesting how the municipality views the application of the subsidiarity principle. According to the municipality, imposing a periodic penalty to prevent further inflammatory statements on social media is the only (administrative) option the mayor can use besides criminal law. It is emphasised by the municipality that the periodic penalty can have a quick effect and thus protect public order (Gemeente Utrecht, 2021). Boumanjal, the lawyer of the person from Zeist upon whom a periodic penalty was imposed by the mayor of Utrecht, wonders whether the surveillance monitors the IP address of the person concerned, and whether they check which websites the person visits and which platforms he uses. If this is the case, it seems to him that this violates the right to privacy under Article 10 of the Dutch Constitution. All these powers may only be applied by investigative agencies under strict conditions (Boumanjal, 2021). The court does not address this argument.

#### 11.5.3.5 *Reflection from the focus group and expert meeting*

In the underlying research, outcomes from the literature and case histories were presented to experts and legally experienced practitioners from municipalities. In the discussion from the expert meeting, M.A.D.W. de Jong, Associate Professor at Radboud University Nijmegen, felt that the articles in the General Bylaw on which the decision was based were insufficiently specific. The difference in enforcement was also highlighted: physical area bans can be monitored physically, affecting residents' freedom of movement. In contrast, an online ban necessitates monitoring residents' expressions, impacting their privacy as well. Thus, two additional fundamental rights are at stake, in her opinion.

The focus group noted that the sanction used, the periodic penalty, is referred to in the press as a 'digital area ban'. It said that this is now known to be a well-established term, but it should be questioned whether this terminology is correct, because the term refers to an injunction that does not apply to the entire internet, but only to special online messages that may incite provocative behaviour that could lead to disorder. The focus group also assumed that fundamental rights may not be restricted by a local law and that this case involved freedom of expression in accordance with Article 7 of the Dutch Constitution.

The focus group also highlighted the complexity of enforcement in these cases. Among other issues, they raised the question of who can be considered an excessive offender in the case of incitement to riot. According to the lawyers present, a distinction may need to be made between the person who calls for a riot and the actual rioters in the physical domain. Finally, the focus group suggested that an emergency ordinance and emergency order could be useful for prevention and referred to useful non-legal interventions, such as sending a letter, posting messages on social media and engaging in conversation on social media with people who call for riots. Also mentioned in this context was the digital neighbourhood agent, who is often in close contact with the neighbourhood and can serve as a mediator.

### 11.5.3.6 *Reflection of the Court*

A court ruling in the Utrecht case followed on 3 February 2023. The judge believes that a digital platform such as Telegram cannot be construed as a public place. While a group chat (accessible to everyone) on Telegram is public, it is not a place, within the meaning of the General Municipal Bylaw, that is within the mayor's purview. According to the judge, the mayor also misinterprets Article 2:2, paragraph 1(g) of the General Municipal Bylaw by saying that only the disorderly conduct must take place in a public place; the conduct that gives rise to it may take place in a non-physical place. The General Municipal Bylaw provision is clearly intended for the situation where the challenging behaviour that gives rise to disorder is displayed in the public place. Should the reasoning be correct, this General Municipal Bylaw article would lead to an impermissible restriction of the freedom of expression contained in Article 7, paragraph 3 of the Dutch Constitution. A General Municipal Bylaw may not restrict the content of statements. It is also stated in the court ruling that such a restriction of freedom of expression can only take place through a national law according to the restriction system of the Dutch Constitution. In summary, the mayor is not authorised to impose a periodic penalty (Rechtbank Midden-Nederland, 2023).

Based on the Utrecht case study, the General Municipal Bylaw does not appear to be an appropriate instrument to deal with online content that may disrupt public order. This is not only due to local regulations, which are focused on physical public spaces rather than virtual public spaces, but also primarily because fundamental rights may not be restricted through a local law in the Netherlands. The perspective of the judge and experts in the focus group align. The following section explores how this issue is addressed in Belgium.

## 11.6 DESCRIPTION OF BRUSSELS GENERAL POLICE REGULATIONS (BELGIUM)

### 11.6.1 *Description of the Belgian case study*

This topic is also relevant in Belgium and has been widely discussed there. In contrast to the Dutch situation, there is an explicit reference to virtual public space in the Common General Police Regulations of Belgium (in the 19 Brussels municipalities). The Common General Police Regulations for all 19 Brussels municipalities examined in this section apply to the Brussels-Capital Region. This Region has a parliament that exercises legislative power. The executive power lies with the Brussels-Capital Government. The region consists of 19 municipalities, all of which have broad autonomy in the exercise of their powers. The Brussels-Capital Government exercises control over these municipalities (be.brussels, n.d.).

WILLEM BANTEMA

From 1 September 2020, a Common General Police Regulation came into force for all 19 Brussels municipalities. These regulations can be compared to the Dutch General Municipal Bylaw. Section 1, Article 4(5) states the following:

For the purposes of these regulations, the term ‘publicly accessible space’ includes not only actual spaces but also virtual spaces that are accessible to the public, such as accounts on social media, forums, and other digital platforms that are not limited to a small number of people who share common interests (politie.be, 2024).

Article 5 of the regulations states that in the described spaces (including virtual ones), people are expected to comply with the orders of the police or authorised officials, among other things with a view to maintaining public safety and tranquillity. If a legal topic is regulated at the federal level in Belgium, it may no longer be regulated in the lower regulations. What is not regulated on the federal level may be regulated by the *communes*, the municipalities. In the area of virtual public order, nothing is regulated at the federal or state levels, so the *communes* can and may implement their own regulations (uvcvw, n.d.).

Two respondents from Belgium were interviewed, but only limited information was provided. This information revealed, among other things, that the Common General Police Regulations are enforced by a specially appointed supervisor and, in some cases, by a mediator for each area of the municipality. If there is a violation, it is dealt with under criminal law; a fine usually follows, but a mediation process also takes place. In this context, it is important to act quickly and effectively. The interview revealed that the problems surrounding disruptions of public order from the internet are solved pragmatically as much as possible with the help of mediation.<sup>3</sup> People do not expect conflicts with Article 6 ECHR in this respect. ‘You have to try something anyway’, as the interviewees said. More practical experience could not be demonstrated by the experience of the interviewees. It remains to be seen how professional practice regarding these regulations develops.

### 11.6.2 Reflection on the Belgian case study

The expert meeting sought opinions on the Belgian approach to handling online incitement, where interviews indicated that communication and mediation are effective tools. The combination of criminal law and mediation, as applied in the Brussels

---

<sup>3</sup> In mediation, a neutral third party, the mediator, is brought in to mediate a conflict and reach an outcome that is acceptable to both parties.

municipalities, seems juridically sound and effective, according to De Jong. Bantema wonders how far this remains effective in the long term and whether there should not be an ultimate sanction in the event of a repeat offence. According to De Jong, talking to a mayor is important, and criminal law acts as an incentive in this regard. In terms of administrative law, the mayor can always act in the physical environment by, for example, working with an emergency ordinance or an emergency order. It is worth noting that in Belgium, unlike in the Netherlands, mayors have hardly any powers of their own to maintain public order and safety.

In the focus group with municipal lawyers, the combination of criminal fines and mediation was mentioned as a creative option. A caveat should be noted here, however, regarding mass protests with much emotion, such as farmers' protests. In such cases, the size of the protest makes mediation difficult, and sponsors for fines and periodic penalty payments can often be found in big protest groups, so the effect of a sanction is reduced, if present at all. Regarding the monitoring of sentiments and expressions, those present indicated that there are limits to monitoring by municipalities but that in the tripartite consultations the police can be asked to start monitoring within the framework of criminal law, if there is reason to do so. The role of social media platforms was also questioned. One wonders whether these platforms can be addressed by the municipality.

As mentioned above, the choice was made in Belgium to make all articles of the General Municipal Bylaw also applicable to virtual spaces (in addition to physical public spaces). Additional research shows that no lively legal practice has emerged so far, and that local rules regarding 'virtual spaces' are primarily used as a means of facilitating conversation (mediation). However, the method of formulation may provide inspiration for the Dutch situation. This will be discussed further in the next section.

## 11.7 ARTICLES OF THE GENERAL MUNICIPAL BYLAW THAT EXPLICITLY FOCUS (MORE) ON THE ONLINE DOMAIN

### 11.7.1 *Expanding the definition of public space*

One of the ways to make the General Bylaw usable for tackling online disorder is to extend its scope to the virtual domain. In the case of Utrecht, an existing article in the General Bylaw was used that, like many laws and regulations in administrative law, focuses on the physical domain. The extension presented here is based on and inspired by the text from the General Police Regulations of Brussels. Such an extension could also be implemented in the Dutch General Municipal Bylaw and could then read as follows:

In addition to physical spaces, this regulation also applies to virtual spaces accessible to the public, such as accounts on social media, forums and other

WILLEM BANTEMA

digital platforms that are not limited to a small number of people with common interests.

In this way, it would become possible to apply provisions of the General Bylaw that in principle focus on physical public space to virtual space. Instead of declaring the entire General Bylaw applicable to virtual space, the definition of the term ‘public place’ could be expanded:

A place accessible to the public, including the road as referred to under c and the virtual spaces accessible to the public, such as accounts on social media, forums and other digital platforms that are not limited to a small number of people sharing *common interests*.

If the prohibition is breached or a breach is likely to occur, it can be enforced administratively with a (preventive) remedial sanction, such as a periodic penalty or (with reference to a criminal provision) a fine. Feedback on this proposal was not received from the focus group and expert meeting, because it was created afterwards. In its ruling in the Utrecht case, the court considered that ‘public place’ in this municipality’s General Municipal Bylaw article (Article 2.2) meant a physical place.

In the explanation of the Utrecht ruling, the court further determined that digital platforms, such as group chats on Telegram, can be classified as a public place. However, this does not mean that it is the type of public space the Municipal Bylaw focuses on, as these public spaces are only physical. The court furthermore states that Telegram, although a public space because it is accessible to everyone, is not within the powers of the mayor. This last statement is interesting because it might refer to the jurisdiction of the mayor, which is limited by the municipality boundaries. The public space of Telegram is worldwide.

### 11.7.2 *Adaptation of the General Municipal Bylaw in Almelo*

Besides Utrecht, where an existing Municipal Bylaw article was used to crack down on online troublemakers, another municipality in the Netherlands went a step further. In the municipality of Almelo, a town in the eastern part of the Netherlands, a General Municipal Bylaw article was recently introduced as groundwork to deal with online-incited disturbances. In the case of violation, a periodic penalty can be imposed. Like the proposal presented above, the article is an elaboration of the General Municipal Bylaw article referred to in Utrecht. In addition to Article 2:1a (which has not been amended), a new article has been added, namely Article 2:1b (Gemeente Almelo, 2022). This article reads as follows:

## 11 EFFICACY OF THE DUTCH GENERAL MUNICIPAL BYLAW

- 1 It is forbidden to make, share and/or maintain expressions through digital means, including through the Internet, virtual spaces and social media, which could lead to a physical disturbance of public order within the territory of the municipality of Almelo, or to the creation of a serious fear thereof.
- 2 Without prejudice to the provisions of Section 54a of the Penal Code, operators of websites, domain name holders and social media platforms are prohibited from making statements, as referred to in the first paragraph, via their communication service: share or further disseminate or have disseminated (a), uphold (b), or keep online and accessible or visible (c).
- 3 Administrators of websites, domain name holders, hosting providers and social media platforms are obliged to block, remove and keep removed, by order of the mayor, expressions as referred to in the first paragraph, whether or not through their own notice-and-take-down procedures.

11.7.3 *Reflection on current events*

A few experts reflected on the General Municipal Bylaw of Almelo in the magazine *Binnenlands Bestuur*.<sup>4</sup> This is not part of the research, but it gives a picture of how people think about current affairs (Knapen, 2022). De Jong is critical and indicates that mayors should not take measures aimed at curbing freedom of expression. She also argues for national rules as opposed to rules that differ in each municipality. For her, freedom of expression weighs heavily as one of the core values of the rule of law. She also indicates that the article is a form of censorship as it bans expressions on the internet in advance. This is not allowed under Article 7 of the Dutch Constitution (freedom of expression). For example, the local triangle consists of the mayor, the police and the district attorney. They gather regularly to discuss the public order situation.<sup>5</sup> According to De Jong, there is only one route: criminal law. Incitement is punishable under Article 131 of the Penal Code, and anyone who engages in incitement can be prosecuted. She adds that enforcing a penalty based on the General Municipal Bylaw article carries risks, as it involves interfering with freedom of expression and privacy, because digital devices must be checked for utterances. De Jong also refers to the fact that most laws are written for the physical domain, and they cannot simply be applied in the online world. In summary, De Jong argues that the digital area ban that Almelo is proposing is not possible, because it is a fundamental break with the Dutch vision of freedom of demonstration and the protection of the freedom of expression. She therefore advocates cooperation within the

---

4 Binnenlands Bestuur (Domestic Governance) is the only journalistically independent platform in the Netherlands for government officials and administrators, bringing news, background and opinion on governance and policy.

5 Article 7 of the Constitution deals with freedom of speech and the prohibition of censorship.

WILLEM BANTEMA

local triangle to tackle the problem. It seems that the Central Netherlands court followed this line of reasoning in its ruling of 3 February 2023.

Bantema argues that there are four criteria for developing workable legislation (Knappen, 2022). First, it must be determined whether a regulation is desirable or necessary and whether other non-legal solutions are possible. The second criterion is whether it will stand up in court (legal tenability). The third is the question of organisational feasibility. Finally, the fourth criterion is whether the remedy is effective. Bantema argues that when all four criteria are met, useful law has been developed. Bantema also argues that online incitement cannot be tackled through a General Municipal Bylaw, because physical freedom of movement (and area bans) is an entirely different area from regulations that address freedom of expression.

In response to the Almelo article, Bantema refers to online messages that are sometimes vague. The call will often not be ‘let’s go riot’ but, for example, ‘we’re going for coffee’. It then becomes a play on words that is difficult to act against. Finally, Bantema sees a problem in that the government cannot constantly monitor citizens online: ‘There is no explicit administrative law power for a municipality to systematically monitor someone.’ In addition, Bantema also refers to the discussion about the limits of administrative law powers. For instance, mayors have no cross-border powers: a young man from Venlo cannot be tackled in Groningen because he incited riots there online. Moreover, the causal link between online behaviour and the effect on public order must be clear, and that relationship is often indirect.

Marietta Buitenhuis sees more possibilities than De Jong. In special circumstances, she does see options for a legal basis.<sup>6</sup> She indicates that, to a certain extent, certain restrictions on the fundamental right of freedom of expression appear to be permitted in case law, where rulings have stated that a restriction of a fundamental right may only be an indirect consequence of the internet ban. Buitenhuis is also curious about how the judge will handle cases like the Utrecht case. That does not mean that Buitenhuis does not anticipate any potential problems. She mainly sees problems in enforcement and enforceability. Buitenhuis wonders how one can check whether someone posts a call to disrupt public order on social media. These posts are often done anonymously or with an alias. The mayor does not have access to IP addresses and cannot take Tweets offline. If they are not enforceable and enforced, there is no point in including such General Municipal Bylaw articles, according to Buitenhuis. Buitenhuis sees possibilities with the law in a formal sense. She points out that fundamental rights can be restricted – under certain conditions – by laws made by the central government. According to Buitenhuis, mayors cannot order hosting companies to take messages offline (see Articles 2

---

6 Mariëtte Buitenhuis is a lawyer with AKD, a law firm in the Netherlands. She specialises in public order enforcement issues. The possibilities of taking enforcement action against online disorder have her particular attention. See for articles on this topic Buitenhuis (2022).

and 3). There are no local powers or procedures for that. Incidentally, Buitenhuis does see favourable possibilities in relation to the light powers of injunction (Article 172, paragraph 3 of the Municipalities Act), but due to the limits of space in this study, these possibilities are not discussed here (for more information see Buitenhuis, 2022).

## 11.8 DISCUSSION AND CONCLUSION

### 11.8.1 Discussion

Beyond all the criticism of the General Municipal Bylaw as the legal basis for dealing with online-incited disturbances, drawing attention to some nuances is in order. For instance, since COVID-19, the relationship between online behaviour and public order has become increasingly clear (see also Wood et al., 2022). This clarity should make the substantiation of measures easier and more plausible. The issue of different jurisdictions also calls for nuance. For example, one may question to what extent jurisdiction is an issue when it is assumed that there is a clear impact on public order in a specific municipality. Furthermore, the question is to what extent inciting riots or deliberately disturbing public order is protected by freedom of speech. As stated, most examples in the literature concern protest and show a clear role of social media in the organisation of the events (Briggs, 2012; Treadwell et al., 2013). More case law will eventually clarify the legal possibilities of the General Municipal Bylaw as groundwork for tackling online disorder. The District Court of the Central Netherlands ruled on this in the first instance and, for the time being, overturned the underlying decision for an online area ban.

It is also advisable not to lose sight of issues such as necessity (i.e. whether there are alternatives), feasibility, enforcement and effectiveness. When the relevant requirements are not met, a measure will achieve little beyond a strong normative signal. Current events in 2024 show that an increasing number of municipalities want to experiment with online administrative law enforcement, partly to address issues related to drill rap,<sup>7</sup> which involves youths creating drill rap videos that incite offline violence between gangs (Omroep West, 2023). It is to be hoped that in 2024, (1) administrative law experiments will yield results in case law and thus provide more information about their legal tenability and feasibility; (2) social and political discussions will be held about the desirability and necessity of administrative law enforcement online; and (3) more research will be conducted into the effectiveness of different types of measures and policy in dealing with disturbances instigated online.

---

7 Drill rap is a subgenre of hip-hop known for its raw lyrics that often discuss crime, street life and gang conflicts.

WILLEM BANTEMA

There is increasing talk in the media of an ‘online area ban’. Researchers have tried to provide a definition of this concept:

The imposition of a restriction on a person or organisation in making online statements for a certain period due to a serious fear of a disturbance of public order, which may be evidenced by serious objections, because previous statements have (partly) led to this, or in the case of such statements leading to fear of public order the first time. (Vuik & Bantema, 2021)

The case in Utrecht fits with this definition, as statements were made that led to public order disturbances before. The new General Municipal Bylaw in the municipality of Almelo goes even further by imposing a fine in the first instance when there is a serious fear of a disturbance. In any case, a digital area ban remains distinct from a physical area ban, and the term is misleading, since citizens can continue to use the internet and social media, except for specific statements that can result in fines. When politicians launch new plans, they would be wise to avoid using the term ‘online area bans’, because using the term would play into the hands of the biggest critics of these plans, even though the measures they propose are often less invasive of privacy.

### 11.8.2 Conclusion

This study started by questioning to what extent municipalities can act against online-incited public order disturbances via the General Municipal Bylaw and how such Bylaw articles can or should be formulated. The first conclusion, based on legal possibilities, is a pessimistic one regarding the chance of success of the General Municipal Bylaw as an instrument. The legal possibilities and limitations were discussed because of the case in the municipality of Utrecht and because of the amendment of the General Municipal Bylaw in Almelo. Attention was also paid to the way in which an attempt was made in Belgium to declare the Common General Police Regulations (the equivalent of the Dutch General Municipal Bylaw) applicable to the virtual public domain.

In general, the restrictive system of the Dutch Constitution poses challenges for municipalities in establishing regulations within the General Municipal Bylaw. The root of an online disturbance often intersects with issues of opinion, thereby implicating freedom of expression. The article revealed that freedom of expression should not be restricted through the General Municipal Bylaw. It also emerged from the literature and discussions with experts that it is assumed that the General Municipal Bylaw is meant for the physical domain and that, as a result, there are currently no administrative law enforcement options online. The question is whether, in cases where municipalities do enforce administrative law (the Municipalities Law, a law established by the national government) for online statements that have the effect of disrupting public order,

the courts will take a different view. If the judge disapproves, there may be a task for the national government to create a possibility for municipalities to still regulate the virtual domain. In any case, the court annulled the decision containing the chosen construction of the municipality of Utrecht, in which an existing General Municipal Bylaw article was applied.

Not only did legal bottlenecks emerge, but issues regarding the enforcement and implementation of such General Municipal Bylaw rules were also highlighted. These include the complexity of determining the offender, demonstrating the relationship between online activities and public order disturbances, disturbances fuelled online from other municipalities (or abroad) and legislation that is formulated and intended for the physical domain. This study discussed two General Municipal Bylaw proposals in which the regulations are explicitly and clearly focused on online action and the potential consequences for public order in a specific municipality. These proposals do not directly solve the problems outlined, however, because even when they are clearly targeted at online behaviour or content, freedom of expression still comes into play and should not be restricted via a General Municipal Bylaw. In addition, there are also concerns about the enforcement and enforceability of such rules should the legal basis be upheld by the administrative court.

In addition to the suitability of the General Municipal Bylaw as an instrument, specific textual possibilities and textual proposals that have been tried and tested in practice were also investigated. For example, both the municipality of Almelo and several Brussels municipalities have explicitly addressed the effects of online behaviour on public order. It was previously determined that the General Municipal Bylaw is not an appropriate instrument, but the textual proposals examined could potentially be used to amend a law on the national level, such as the Municipalities Act. In general, the broader a text proposal is (see, for example, Almelo), the more room it offers for restricting fundamental rights. In addition, the risk with a specific article (where fundamental rights are less likely to be affected and it is clearer what the government expects) is that it has limited applicability to cover a range of online phenomena that can affect public order. One of the key principles that follows from the analyses is that municipalities should not restrict communication in advance. Any bill will therefore have to focus exclusively on preventing a repeat offence rather than on preventing the offence and/or message in advance.

## REFERENCES

Bantema, W., Twickler, S., Munneke, S., Duchateau, M., & Stol, W. (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*. Sdu Uitgevers.

WILLEM BANTEMA

- Bantema, W., & Twickler, S. (2023). Waar mondiale het lokale treft: de APV als instrument in de strijd tegen online aangejaagde ordeverstoringen. *Computerrecht*, 65(2), 118-125.
- Bantema, W., Twickler, S., & De Vries, S. (2022). *Juridische grenzen en kansen bij openbare-ordehandhaving: Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen*. Onderzoeksgroep Cybersafety.
- Bantema, W., Westers, S., Hoekstra, M., Herregodts, R., & Munneke, S. (2021). *Black Box van gemeentelijke online monitoring: Een wankel fundament onder een stevige praktijk*. Sdu Uitgevers.
- Bantema, W., Westers, S., & Munneke, S.A.J. (2020). *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen*. Boom bestuurskunde.
- be.brussels. (n.d.). Municipal duties. be.brussels. <https://be.brussels/en/about-region/structure-and-organisations/local-authorities-and-municipalities/municipalities>
- Boumanjal (2021, 30 November). Online area ban for agitator legally untenable. *Security.nl*. <https://www.security.nl/posting/731985/Advocaat%3A+online+gebieds+verbod+voor+%27opruier%27+juridisch+niet+houdbaar>
- Briggs, D. (Ed.) (2012). *The English riots of 2011: A summer of discontent*. Waterside Press.
- Brouwer, J.G., & Schilder, A.E. (2022, 21 February). Online call for disturbance of public order: Penalty unmaintainable. *Openbareorde.nl*. <https://www.openbareorde.nl>
- Buitenhuis, M. (2022). De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 1). *Gemeentestem*, 44, 230-238.
- De Jager, W. (2024, 14 May). TikTok drops €25,000 from drone, causing commotion in Zurich. *Dronewatch*. <https://www.dronewatch.nl/2024/05/14/tiktokker-laat-geld-vallen-vanuit-drone-veroorzaakt-opschudding-in-zurich/>
- Elson, J. (2023, 11 June). Champions League final pitch invaders were motivated by huge cash prize as it's revealed controversial Russian influencer Mellstroy offered fans £300,000 to pull off idiotic stunt at Wembley. *Daily Mail Online*. <https://www.dailymail.co.uk/sport/football/article-13484263/Champions-League-final-pitch-invaders-Russian-streamer-Mellstroy.html>
- Gemeente Almelo (2022, 29 November). Raadsbesluit van de gemeente Almelo tot wijziging van de APV 2021. *Gemeente.nu*. <https://www.gemeente.nu/bestuur/gemeenteraad/almelo-past-apv-aan-voor-online-ordeverstoringen/>
- Gemeente Utrecht (2021). Response to written council questions, no. 295, reference 9565194, Policy area of public order and safety. *Utrecht.nl*.
- Gemeente Utrecht (2021, 26 November). Online area ban for man who called for riots in Utrecht. <https://www.utrecht.nl/nieuws/nieuwsbericht-gemeente-utrecht/online-gebiedsverbod-voor-man-die-opriep-tot-rellen-utrecht/>
- Hoge Raad (2002, 28 May). *ECLI:NL:HR:2002 (Tilburg)*. <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2002:AE1494>

- Knapen, M. (2022, 27 December). Online area ban remains legally complex. *Binnenlands Bestuur*. R <https://www.binnenlandsbestuur.nl/juridisch/online-gebiedsverbod-blijft-juridisch-complex>
- Kortmann, C.A.J.M., Bovend'Eert, P.P.T., Broeksteeg, J.W.L., Kortmann, C.N.J., & Vermeulen, B.P. (2016). *Constitutioneel recht*. Kluwer.
- NRC (2023, 6 February). 40 mayors ask The Hague for more online tools to prevent riots. *NRC*. <https://www.nrc.nl/nieuws/2023/02/06/40-burgemeesters-vragen-den-haag-meer-online-middelen-om-rellen-te-voorkomen-a4156285>
- Omroep West (2023, 29 March). The Hague, Delft, and Zoetermeer want to experiment with online area ban. *Omroep West*. <https://www.omroepwest.nl/nieuws/4674647/den-haag-delft-en-zoetermeer-willen-experimenteren-met-online-gebiedsverbod>
- Politie.be. (2024, 3 April). Algemeen politiereglement-Ukkel. Algemeen Politiereglement Ukkel | Lokale Politie Ukkel / W-B / Oudergem
- RTV Utrecht (2022, 16 June). Mayor revokes online area ban for agitator. *RTV Utrecht*. <https://www.rtvutrecht.nl/nieuws/3552484/burgemeester-trekt-online-gebiedsverbod-in-voor-opruier>
- Rechtbank Midden-Nederland (2023, 3 February). *ECLI:NL:RBMNE:2023:375 (Utrecht)*. <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2023:375>
- Rijksoverheid. (n.d.). Public order and safety. <https://business.gov.nl/regulation/public-order-and-safety/>
- Teunissen, J.M.H.F. (2009). Publiek domein en de legaliteitseis. *Gemeentestem*, 2009(47), 231-245.
- Treadwell, J., Briggs, D., Winlow, S., & Hall, S. (2013). Shopocalypse Now: Consumer Culture and the English Riots of 2011. *The British Journal of Criminology*, 51(1), 1-17.
- Tuncay, N. (2018). Social Media Ban: Virtually Social or Physically Social? In *4th International Congress on Education, Distance Education and Educational Technology – ICDET* (166-182). Çözüm Educational Publishing.
- Tweede Kamer der Staten-Generaal (2013, 12 June). *Rapport van de commissie-Haren*.
- UVCVW. (n.d.). La police administrative. <https://uvcvw.be>
- Ververis, V., Marguel, S., & Fabian, B. (2019). Cross-Country Comparison of Internet Censorship: A Literature Review. *Policy & Internet*, 12(4), 450-473.
- Vuik, G., & Bantema, W. (2021). Perspectief uit de praktijk: Het digitale gebiedsverbod als gemeentelijk instrument tegen online aangejaagde ordeverstoringen. *Bestuurswetenschappen*, 75(3), 94-108.
- Wennekes, L. (2022, 5 December). Almelo adjusts APV for online disturbances. <https://www.gemeente.nu/bestuur/gemeenteraad/almelo-past-apv-aan-voor-online-ordeverstoringen/>
- Wood, R., Yannitell-Reinhardt, G., Rezaedaryakenari, B., & Windsor, L. (2022). Resisting Lockdown: The Influence of COVID-19 Restrictions on Social Unrest. *International Studies Quarterly*, 66(2), 1-16.



## 1 2 PARTNERS IN CRIME-FIGHTING?

### *A systematic literature review of online citizen-led policing and its relations to government law enforcement*

Rianne Dekker

#### **Abstract**

*Social media has enhanced citizens' capacity to self-organise against crime and various types of online citizen-led policing have emerged. It is still unclear how they relate to and engage with government law enforcement efforts, as most research thus far has focused on police-led participatory initiatives. This chapter presents a systematic literature review of 95 academic articles exploring three conceptualisations of the relationship between online citizen-led and state policing. The meta-synthesis of findings first shows that engagement with law enforcement is more likely when citizen initiatives target crimes that fall under the purview of the police, especially in areas with security deficits. Conversely, initiatives focusing on non-criminal offences or government transgressions, including police misconduct, often operate independently. Second, the practices of online citizen-led policing vary: some groups prioritise civic responsibility and professional conduct, while others are driven by entertainment, monetisation or mob mentality. Third, differing perceptions of government law enforcement exist, ranging from aspiring partnership to assuming an independent role. Conclusions about the relationship between citizen-led and state policing vary across research paradigms. This chapter recommends future studies to explicate their ontological and epistemological foundations, reflect on the police function and pursue systematic comparisons to better understand the role of online citizen-led policing in security arrangements.<sup>1</sup>*

#### **12.1 INTRODUCTION**

In this digital age, the realm of policing has expanded beyond the exclusive domain of government law enforcement agencies. Through the proliferation of recording technologies such as smartphone cameras, dashcams and tracking devices, and options to share and research this content online, citizens' capacity to self-organise and to undertake a variety of policing activities has expanded. These activities range from

---

<sup>1</sup> This research was conducted as part of the project 'To the Rescue or Going Rogue?' (project number VI.Veni.211R.032) of the research programme Veni SGW, which is (partly) financed by the Dutch Research Council (NWO).

RIANNE DEKKER

leveraging self-taught digital forensics to solve cold cases, to exposing scammers and groomers in undercover investigations, and crowdsourcing intelligence in search of suspects or missing persons. Social media has provided new platforms for information gathering and allows groups of citizens to establish and pursue their own security agendas.

Online self-organisation against crime (either traditional forms of crime or cybercrime) challenges the state's monopoly on the legitimate use of force (cf. Weber, 1987 [1919]). This is most visible in instances in which citizens continue to pursue extrajudicial punishment, for example through doxing – online naming and shaming (Douglas, 2016) – or physical confrontation of suspected offenders. However, various groups maintain good working relations with government authorities and refrain from extrajudicial punishment. Current research on the relationship between civilian policing and government law enforcement has extensively focused on police-led participatory initiatives, including community policing initiatives (Diphoorn & Van Stapele, 2021) and (cyber)volunteers (Whelan & Harkin, 2021) in which the goals and methods of civilian policing are actively coordinated by the police. It remains unclear how online citizen-led policing relates to government law enforcement.

Practices of online citizen-led policing have attracted the attention of different academic disciplines, including criminology, media studies, surveillance studies and public governance. Because of the diffused nature of academic evidence and debate on this topic, in this chapter a systematic literature review and meta-synthesis of current findings is used to collect and compare current evidence and formulate an answer to the research question: *How do different varieties of online citizen-led policing relate to government law enforcement efforts in different contexts?* The analysis focuses on three ways in which the relationship between online citizen-led policing and state policing can be conceptualised and operationalised. The first way is by assessing whether the focus on deviance aligns or differs between online citizen-led policing and government law enforcement. The second is by reviewing current evidence on the activity of online citizen-led policing collectives and evaluating whether this adheres to police norms of practice, for example in collecting and analysing evidence. Third, the relationship between online citizen-led policing and government law enforcement can be studied by looking how citizens perceive their role compared to that of government law enforcement and whether they would desire further integration of these roles.

The structure of the chapter is as follows. After introducing the strategy of collection of relevant literature and meta-synthesis in section 12.2, section 12.3 presents the findings of the meta-synthesis. This section is structured according to the three main coding categories on which the meta-synthesis focused: the focus on online citizen-led policing; the practice of online-citizen-led policing; and the perceptions of government law enforcement. The subsections present common findings across different studies, but also highlight and discuss contrasting findings in context. The conclusions section, section 12.4, summarises the results and discusses their relevance for theory and

practice. It discusses limitations to this study, related to the method of systematic literature review and meta-synthesis, and presents avenues for future research.

## 12.2 METHODOLOGY

### 12.2.1 *Collection of relevant literature*

This chapter is based on a meta-synthesis of a systematically retrieved sample of academic literature on the phenomenon of online citizen-led policing. A systematic literature review is a 'systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars and practitioners' (Fink, 2010, p. 3). In contrast to a narrative literature review, a systematic review adheres to a set of principles that aim to limit biases in the sample of studies (Petticrew & Roberts, 2006, p. 9; Booth et al., 2012). This chapter follows the widely used PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) statement, ensuring transparent and complete reporting of the systematic literature review (Moher et al., 2009; Liberati et al., 2009). This consists of four steps: (1) identification: searching relevant records and excluding duplicates; (2) abstract-level screening; (3) full-text screening; and then (4) inclusion and analysis of the final set of studies.

A search string based on the main concept of research – online citizen-led policing – was used to ensure sensitivity and specificity of the database queries (Petticrew & Roberts, 2006, pp. 81-82). The search query combines search terms referring to online citizen-led policing from different disciplines. The search string uses operators to include variations of words. For example, 'web\$sleuth\*' will search for 'websleuth', 'web-sleuth' and 'web sleuth', and different extensions such as 'websleuths' and 'websleuthing'. The search string used is as follows:

*Web\$sleuth\* OR amateur\$sleuth\* OR 'digital vigilant\*' OR digilant\* OR netilant\* OR 'internet vigilant\*' OR 'virtual vigilant\*' OR 'digital witness\*' OR smart\$mobs OR cyber\$vigilant\* OR cyber\$mob\* OR 'online sham\*' OR 'online citizen polic\*' OR 'online civilian polic\*' OR 'online citizen-led polic\*' OR 'online civilian detect\*' OR 'online detective\*' OR 'online citizen investigat\*\*' OR 'online citizen tracking' OR 'do-it-yourself polic\*' OR 'DIY policing' OR 'human flesh search\*' OR 'online justice\$seek\*' OR 'crowdsourc\* polic\*' OR 'crowdsourc\* justice' OR 'lateral surveillance' OR 'citizen surveillance' OR 'peer surveillance' OR 'p\$edophile hunt\*' OR scambait\* OR hackvis\* OR OSINT OR OSI*

Based on this search string, relevant journal articles were collected from 17 academic databases. These were selected based on their inclusion of publications from the

RIANNE DEKKER

respective disciplines. First, this includes five large academic databases that comprise publications from various publishers and disciplines, including the disciplines relevant to the research questions: (1) Web of Science; (2) Scopus; (3) WorldCat; (4) EBSCO Academic Search Premier; and (5) Proquest. Additionally, 12 databases of large academic publishers and databases of open access publications were searched. These are: (1) Sage; (2) Springer; (3) ScienceDirect; (4) Oxford Academic; (5) Emerald; (6) Taylor & Francis Online; (7) JSTOR; (8) DOAJ (Directory of Open Access Journals); (9) OAPEN (Open Access Publishing in European Networks); (10) OAIster; (11) OpenDOAR; and (12) BASE/Bielefeld Academic Search Engine.

After creating a combined list of records, ResearchRabbit AI's recommendation engine was prompted to suggest additional publications. ResearchRabbit consolidates multiple scientific databases, covering materials that can be found in major databases used by academic institutions (such as Scopus, Web of Science and others). Based on the set of publications retrieved directly from databases queries, ResearchRabbit offers recommendations based on citation networks and similarities in contents (ResearchRabbit, 2024). Their exact algorithm remains proprietary, but inclusion of suggestions is ultimately based on decisions of the researcher.

As expected, there was much overlap between publications listed in the different databases. Exclusion of duplicates was therefore part of the review protocol. To avoid including multiple publications on the same work, and to ensure methodological transparency and rigour of studies included in the meta-synthesis, pre-prints, conference proceedings, books, book chapters, commentaries and popular publications were excluded. As a result, the literature review includes theoretical and empirical contributions to international peer-reviewed journals which contribute to the scholarly debate in the English language.

Full-text articles were then assessed for eligibility in the final round of screening. Reasons to exclude the publications at this stage included: (1) citizen participation in policing did not involve any *online* engagement; (2) online policing did not move beyond individual activity rather than collective engagement; and (3) arrangements were initiated or led by police or private security actors rather than citizens themselves. The final sample of 95 articles that were included in the meta-synthesis are presented in the appendix (<https://public.yoda.uu.nl/i-lab/UU01/JL2YG0.html>; <https://doi.org/10.24416/UU01-JL2YG0>).

### 12.2.2 *Meta-synthesis*

The systematically retrieved sample of articles was subjected to meta-synthesis. This entails a qualitative comparison and translation of original findings from which new interpretations are generated (Walsh & Downe, 2005). This was done by way of manually coding the individual articles and comparing the studies based on the study's objective.

The choice for the method of meta-synthesis was based on the fact that many articles are conceptual or they report on highly different (qualitative) case studies which do not allow for quantitative meta-analysis.

A limitation of meta-synthesis is combining and interpreting findings from studies departing from different ontological and epistemological perspectives. Zimmer (2006, p. 315) argues that it is possible to synthesise across these perspectives as long as careful attention is paid to the context and assumptions underpinning the primary studies. Therefore, the geographical and social context of the studies and implicit and explicit references to the studies' ontologies and epistemologies were coded and taken into account throughout the analysis.

Section 12.3 presents the aggregated findings after coding the focus, practices and views of government law enforcement of empirically researched examples of online-citizen led policing. The coding of the focus of online citizen-led policing included codes on types of transgressions and offenders. Regarding the practices involving online citizen-led policing, we coded the uses of online tools and information resources, how collectives self-organised on social media platforms and which norms of professionalism they develop. The category of perceptions of law enforcement includes codes on how those engaged in online citizen-led policing view law enforcement, including codes on contacts and views on the capacity to resolve crime. The next section presents the most common codes and patterns of co-occurring codes. Less frequently applied codes and possibly contradictory findings are also highlighted in the discussion of the synthesised results. Before discussing the findings related to the three code categories, the findings section will first introduce a general outlook on the literature on online citizen-led policing, including the years of publication, different disciplines in which the phenomenon has been researched and different labels under which the concept has been captured.

### 12.3 FINDINGS

Research into online citizen-led policing emerged in the late 2000s when social media and recording technologies became within reach for citizens, enabling them to engage in peer surveillance and policing. The first publications describing online citizen-led policing stem from 2008. The main journals publishing studies on this phenomenon include criminological journals such as *Crime, Media, Culture* (8 articles) and *Global Crime* (7 articles published in a 2020 special issue on digital vigilantism) and journals from communication studies, including *Social Media + Society* and *Information, Communication & Society* (4 each). In addition, three relevant articles were published in *Surveillance and Society*, which is a journal from the field of surveillance studies.

The studies included in the meta-synthesis have attempted to capture the emerging phenomenon of online citizen-led policing by using various terms such as

‘online civilian/citizen policing’ (Huey et al., 2013; Hadjimatheou, 2018), ‘lateral/peer surveillance’ (Andrejevic, 2004; Dennis, 2008; Gabdulhakov, 2018), ‘online shaming’ (Škorić et al., 2010; Oravec, 2019), ‘websleuthing’ (Yardley et al., 2018; Wästerfors et al., 2023), ‘cyber vigilantism’ (Smallridge et al., 2016; Chia, 2019) and ‘digital vigilantism’ (Trottier, 2017; Loveluck, 2020). Notable as well is the use of several neologisms, including ‘digilantism’ (Nhan et al., 2015) and ‘netilantism’ (Chang & Zhu, 2020) by which these studies conceptualise justice-seeking online as something inherently different from its offline predecessors such as vigilantism. Research has not converged towards one dominant concept and definition, but a variety of concepts and definitions has remained present in more recent years.

The variety of conceptualisations already signposts different findings on how online citizen-led policing efforts relate to those of the police. The term vigilantism, included in various labels, stresses extrajudicial justice-seeking, whereas terms like policing and surveillance stress its resemblance to police activities. The next section will present the results of the meta-synthesis based on three categories of coding. The first is the types of transgressions and offenders on which online citizen-led policing has focused according to current studies.

### 12.3.1 *The focus of online citizen-led policing*

Studies describe a variety of transgressions on which online citizen-led policing has focused. First, this includes a focus on crime or other tasks that commonly are part of operational police duties, such as finding missing persons (Gray & Benning, 2019) and surveillance of public spaces (Mols & Pridmore, 2019). The types of crime on which online citizen-led policing focuses, however, is selective. Many initiatives focus on crimes or security threats that have a major impact on personal lives or communities, such as child sexual abuse in the case of ‘paedophile hunting’ (Tippett, 2024), missing persons cases (Gray & Benning, 2019), and terrorist attacks (Nhan et al., 2015). Scholars (Kohm, 2009; Blitvich, 2022) have noted that these instances of online citizen-led policing display characteristics of a moral panic, signalling a heightened sense of threat from these instances of deviance (cf. Goode & Ben Yehuda, 1994). This for example is argued in relation to paedophile hunting in the context of the United Kingdom (Hadjimatheou, 2018; De Rond et al., 2021; Tippett, 2024).

In addition to crimes that provoke an emotional response, the literature includes many cases of online citizen-led policing focusing on areas of crime in which a ‘security deficit’ exists or is perceived to exist, such as surveillance initiatives (Mols & Pridmore, 2019; Trottier, 2014a) and the area of cybercrime where hacktivists and scambaiters are active (Huey et al., 2012; Byrne, 2013). Some studies have argued that perceived or actual government inaction in a certain area of crime is a driver of online citizen-led policing, alongside increased expectations of levels of security in society (Button

& Whittaker, 2021; Chang et al., 2018). Such cases of online citizen-led policing with a focus on a security deficit are in some contexts seen as an expression of civic morale or civic engagement (Cheong & Gong, 2010; Favarel-Garrigues, 2020; Škorić et al., 2010). In China, for example, online citizen-led policing goes by the household name 'human flesh search (engines)', which refers both to the use of social media as search engines, and to the fact that the searches are dedicated to finding and doxing the identity of someone who committed a crime or offence (Cheong & Gong, 2010). Human flesh search engines are considered an act of patriotism: citizens aim to help out the government by contributing to public order maintenance.

Many forms of online citizen-led policing, however, do not focus on crime, but on moral transgressions which are outside of the scope of government law enforcement. On the one hand, there are situations which violate a social norm, such as adultery or littering. A famous early case of online citizen-led policing which several studies cite is the 'dog poo girl' incident in 2005, in which a South Korean girl was doxed after not having cleaned up after her dog in a Seoul subway train. In these cases – perhaps again because these behaviours are not addressed by state policing – online shaming is used to discipline offenders (Škorić et al., 2010; Trottier, 2017; Oravec, 2019). On the other hand, online citizen-led policing focusing on moral transgressions can have a focus on specific norm violation as a form of political activism. An example of this is 'drought-shaming' (Milbrandt, 2017), in which excessive water use in times of drought is publicly shamed online. Another example is digilantism against misogyny online ('slutshaming') in the context of Australia (Jane, 2017), but also its polar opposite: misogynist and nationalist digilantism against unpatriotic intellectual women in China (Huang, 2023). These examples demonstrate that activist online citizen-led policing is present on different sides of the political spectrum (see also Vicensová, 2020; Tanner & Campana, 2020). Activist online citizen-led policing sometimes advocates for criminalisation of offences, but also pushes for broader political and societal change.

A specific type of activist online citizen-led policing is focused on norm or rule violations by government institutions, including the police itself. Online citizen-led policing initiatives have focused on global justice-seeking, for example in exposing war crimes, human rights investigations or cases of government corruption. Examples include Bellingcat and more specific instances of 'human flesh search' focusing on corrupt government officials (Škorić et al., 2010; Gao & Stanyer, 2014). Cop-watching initiatives in the US have been focusing on police violence towards black people as a form of activism against police misconduct (Dennis, 2008). During protests, citizens record and try to dox undercover cops whom they accuse of the use of excessive force or inciting riots (Chang & Zhu, 2020; Li & Whitworth, 2023). Partnering with the police is does not match the role of critical watchdogs of the police and state more broadly which these forms of online citizen-led policing tend to assume.

In summary, when reviewing the focus of online citizen-led policing, we find that only some types of online citizen-led policing focus on criminal offences and share

RIANNE DEKKER

security aims with the police. When online citizen-led policing is focused on high-impact crime, or areas of crime where a security deficit exists, it could be a welcome addition to government law enforcement. Other types of online citizen-led policing focusing moral transgressions do not align with current police aims, although some initiatives push for criminalisation of certain behaviours and an expansion of police duties. Collaboration between government law enforcement and online citizen policing is least likely when online citizen-led policing initiatives assume a watchdog role and target government corruption or criticise the police. In the next section, I will review the activity of online citizen-led policing, including the use of online tools and information resources and how different logics influence how online citizen-led policing collectives develop norms of action.

### 12.3.2 *The activity of online citizen-led policing*

Core to many definitions of online citizen-led policing is use of online resources and methods by citizens to collect and study evidence on transgressions. For example, Yardley et al. (2018, p. 82), define web sleuthing as:

amateur detective work including but not limited to searching for information, uploading documents, images and videos, commenting, debating, theorising, analysing, identifying suspects and attempting to engage with law enforcement and other organisations and individuals connected to the cases.

This can focus on offences occurring in cyberspace, such as grooming or online scams; however, access to information on forms of crime in the offline environment, such as theft or abuse, has also become democratised, bringing them into the focus of online citizen-led policing. This section reviews how online citizen-led policing initiatives operate and evaluates whether this adheres to common norms of professionalism applied by government law enforcement.

According various studies (e.g. Yardley et al., 2018), individuals involved in online citizen-led policing are generally amateurs, without police training or a professional background in public security. Instead, their strength lies in their numbers, which often exceeds policy capacity in individual cases. Many studies therefore consider ‘crowdsourcing’ as the core practice of online citizen-led policing, which entails the option to tap into the collective intelligence of communities (Trottier, 2014a; Gray & Benning, 2019; cf. Surowiecki, 2004). There are, however, many respects in which online citizen-led policing diverges from this concept. For example, the process of collectively establishing what information is relevant or truthful in decentralised social media spaces is messy, and not every contribution to the debate is treated equally. The algorithms managing social media heavily influence information exchanges, and in

online policing communities certain individuals tend to claim authority and assume leadership roles (Wästerfors et al., 2023).

Some publications (e.g. Nhan et al., 2017) highlight that online citizen-led policing also includes citizens who are experts in certain areas, such as cybersecurity (Huey et al., 2013), which advantages these collectives' ability to analyse evidence and eventually solve cases. In addition, through experience amateurs can gain expertise in policing, for example when they specialise in distinctive forms of online policing such as paedophile hunting or scambaiting through engagement with multiple cases. Some amateurs build an expert reputation among their online audience (Ireland, 2023; Wästerfors et al., 2023), but this does not necessarily mean that they act according to police norms. Studies on paedophile hunters, for example, have described how they lure and entrap suspects in undercover 'catfishing' operations (Purshouse, 2020; De Rond et al., 2022). Doxing of suspected offenders, which is, according to several definitions (Trottier, 2017; Loveluck, 2020), at the heart of online citizen-led policing, would in most contexts present a disproportionate breach of privacy (Ong, 2012).

A lack of professionalism in online citizen-led policing has also been described as resulting in a racial bias in identifying suspected offenders. This has for example been described in relation to surveillance initiatives (Mols & Pridmore, 2019; Nhan et al., 2017), and Byrne (2013) and Nakamura (2014) describe how scambaiting focused on Nigerian email scams includes many elements of historical anti-black violence. Examples of extrajudicial punishment and racial bias show that a lack of professional norms might not only prevent options for partnering with police, but can also be harmful to society. A legal analysis by Kosseff (2016) raises the more fundamental issue that online citizen-led policing is undercutting the legitimacy of democratic systems by choosing its own focus and methods and lacking a democratic mandate and accountability mechanisms. This raises the question of whether online citizen policing can fit in with police norms at all.

The activity of online citizen-led policing is explained by varying motivations for it that were introduced in section 12.3.1. Only a subset of online citizen-led policing initiatives are driven by civic morale, and could be expected to actively strive to adhere to police norms. Other forms of online citizen-led policing are driven by moral panic. Whereas the police have norms in place to maintain professional distance from cases, engagement in online citizen-led policing is sometimes characterised by closeness: the citizens involved may have been the victim of a crime or they feel emotionally outraged by certain instances of crime. This closeness might lead to an online 'mob mentality' in aspiring to quickly solve cases by any means possible (Blitvich, 2022; cf. Rheingold, 2003). Several studies have demonstrated that online collectives display high levels of social cohesion and sense of purpose (e.g. Chiang et al., 2023; Mols & Pridmore, 2019). This might also lead online citizen-led policing to diverge from professional and transparent procedures and incite them to behave as smart mobs in which the ends of solving a case may justify the use of illegitimate means.

RIANNE DEKKER

Apart from restoring the public or moral order, online citizen-led policing initiatives also cater to themselves and their online audiences, influencing their mode of action. Studies have reported that entertainment and gaming are important elements that motivate individuals to engage in online citizen-led policing initiatives (Lovell, 2020; Chiang et al., 2023). For example, Dynel and Ross (2021) offer an analysis of scambaiting as a form of humorous entertainment. Scammers' strategies are depicted as amusingly naïve and inefficient, while Reddit scambaiters' deceptive messages targeted at scammers demonstrate wittiness and creativity in order to earn online praise from other users. A scambaiting website quoted in another study advertises scambaiting as a game: 'much fun can be had and at the same time you will be doing a public service' (Nakamura, 2014, p. 261). The prize is not always limited to online plaudit; some online citizen-led policing collectives also earn money through donations or other forms of monetisation. For example, some paedophile-hunting collectives sell advertisement space or merchandise (Kohm, 2009), and mugshot-scraping websites earn money from arrestees who are required to pay them a 'removal fee' (Visagh, 2013). In order to cater to their audience, online collectives have been described as finding inspiration in the true crime genre, such as *America's Most Wanted* and *Crimewatch* (Trottier, 2014a), in using similar ways of reporting. Kohm (2009) describes how the NBC show *To Catch a Predator* actually collaborated with paedophile hunters from Perverted Justice to lure and confront suspected offenders.

This section has demonstrated that the activity of online citizen-led policing is steered by different logics. Online collectives motivated by a sense of civic responsibility are most likely to assume police norms of professionalism. However, mob mentality, entertainment and monetisation are described as competing logics which steer online citizen-led policing away from using professional and accountable methods.

### 12.3.3 Perceptions of government law enforcement

As the variety of labels for online citizen-led policing already signals, online collectives may hold different views of government law enforcement which inform their relations with police, or the absence thereof. Some types of online citizen-led policing initiatives perceive their role as those of responsible or engaged citizens, acting as aides to the police (Mols & Pridmore, 2019; Cheong & Gong, 2010; cf. Dekker & Meijer, 2020). Even though their activities do not always adhere to police norms of professionalism – as discussed in section 12.3.2 – they actively bring cases to the police in order to bring suspected offenders before court (e.g. Huey et al., 2013). Active collaboration has been described frequently in relation to cybercrime. Chang et al. (2018) describe how, given the limited resources and capabilities of states in the domain of cybersecurity, governments have seized opportunities to collaborate with online citizen-led policing as co-producers of public security. Button and Whittaker (2021) distinguish three waves of online policing

initiatives in the UK context and signal a trend in which initiatives against cyber-fraud move from quasi-vigilantism towards state assimilation. In this latter type of state-citizen relations, online citizen-led policing gains a position in security arrangements and supports state policing activities.

Even in the unlikely case of paedophile-hunting groups, Chiang et al. (2023) encountered positive working relationships between hunting groups and the police, especially at an interpersonal level. This finding adds nuance to the common idea that paedophile hunters possess a negative view of the police and vice versa. In contrast, Ireland (2023) analysed the responses to an e-petition launched by a paedophile-hunting group in the UK seeking legality for their enforcement operations. Paradoxically, this claim for legitimacy went hand in hand with statements delegitimising police capabilities and eventually became dominated by QAnon conspiracy followers who claim that the societal elite of politicians and celebrities is operating a global child sex-trafficking scheme. This undermined the initial attempt to forge relations with government security actors.

Positive perceptions of government law enforcement and partnerships with the police cannot fully be explained by the focus of online citizen-led policing initiatives on a certain area of crime. This also seems to be dependent on the government context and its preference for institutionalising certain forms of citizen-led policing. Gabdulhakov (2021), for example, presents a case of a digital vigilante group in Russia targeting corrupt merchants, who often belong to ethnic minorities. This digital vigilante group is supported by the government to confront and dox these merchants, with financial rewards and fame. In an earlier article, Gabdulhakov (2018) argues that this type of state engagement with digital vigilante groups fits with a history of state-backed citizen-led justice in Soviet Russia.

While many cases of online citizen-led policing refrain from actively seeking collaboration with government law enforcement and rely on their own methods of disciplining others and seeking justice, they may still partner with the police involuntarily. The information shared and generated by online citizen-led policing provides an extension of the 'eyes and ears' of law enforcement and is effectively becoming part of the surveillant assemblage (Herold, 2008; Mols & Pridmore, 2019; cf. Haggerty & Ericsson, 2000). Trottier (2014b) contends that online citizen-led policing enables a 'ground-up manifestation of state control' by making social life visible. Social media monitoring and analysis allows the police to harness this information. Enhancing state control has also been described as moving beyond surveillance capacity and towards repressive actions. Gabdulhakov (2020) describes how, while police surveillance in cyberspace is generally lacking, Russia has established control over online expression through pro-state vigilantes. These vigilantes discipline other citizens into correct behaviour in online spaces.

This section has outlined how online citizen-led policing initiatives have varying perceptions of government law enforcement, with a variety of initiatives actively striving

RIANNE DEKKER

for legitimization of their role as a partner in security arrangements and other initiatives, for example in the area of cybercrime, already being state-supported. Whereas some instances of online citizen-led policing are incited by a discontentment with police action, this does not necessarily mean that these collectives maintain negative views of police and aim for their role to remain independent. However, the modus operandi and social affiliations might prevent further institutionalisation of working relations, and this is highly dependent on the state context, varying between democratic and autocratic regimes.

#### 12.4 CONCLUSIONS

Online citizen-led policing has become a widespread phenomenon, as the extant literature indicates, yet there is no consensus on how this phenomenon interrelates with government law enforcement. Are online citizen-led policing efforts by citizens to be considered vigilante schemes which operate outside of established law enforcement institutions, or does online citizen-led policing also act as partner in crime-fighting and on which factors does that depend? This literature review aimed to offer a preliminary explanation of the relationship between online citizen-led policing and state policing based on different varieties of online citizen-led policing and the government contexts in which they exist. The research question this study addressed is: *How do different varieties of online citizen-led policing relate to government law enforcement efforts in different contexts?* Findings in current literature on online citizen-led policing from a variety of academic disciplines were reviewed and synthesised via three categories of coding. The first coding category is the area of deviance online citizen-led policing focuses on, the second the activities which online citizen-led policing communities engage in, and the third how they view their role in relation to that of government law enforcement.

The meta-synthesis on this first dimension reveals that online citizen-led policing initiatives differ in focusing on issues of deviance, ranging from legal and to moral transgressions. Partnerships are most likely with online citizen-led policing initiatives focusing on criminal offences, particularly in areas of crime where a security deficit exists. Other types of online citizen-led policing do not align with current police aims, although some initiatives push for criminalisation of certain behaviours and an expansion of police duties. A subset of online citizen-led policing initiatives focuses on transgressions by government actors, including the police itself. Partnerships are unlikely, as these types of online citizen-led policing assume an independent ‘watchdog’ role.

Current research findings based on the activity of online citizen-led policing demonstrate that the practice of online citizen-led policing is steered by different logics. Some collectives are motivated by a sense of civic responsibility. They generally strive to adhere to police norms of professionalism in order to refer cases that will be

admissible before court. However, many online citizen-led policing initiatives engage in criminalised behaviour, such as doxing, themselves. Several studies highlight that a mob mentality, entertainment and monetisation are competing logics which steer online citizen-led policing away from following professional and accountable procedures. In these cases, good working relations with government law enforcement are less plausible. Again other initiatives actively choose to use extra-legal methods of justice-seeking and disciplining as they believe the legal system is inadequate or failing to deliver justice.

Lastly, I synthesised findings on how online citizen-led policing initiatives perceive government law enforcement and whether they might actively strive for partnerships or instead view their own role as independent from that of the state. In expected and also some unexpected cases, online citizen-led policing initiatives held positive views of government law enforcement and they were actively striving for a role as a legitimate partner in existing security arrangements. Other initiatives, for example in the area of cybercrime, were effectively state-supported. Any normative interpretations in terms of good or bad online citizen-led policing are highly dependent on the state context, varying between democratic and autocratic regimes.

The literature conceptualises online citizen-led policing very differently and on that basis also comes to different conclusions with respect to how it relates to government law enforcement. Alignment between state policing and online citizen-led policing existed in relation to a large variety of initiatives, and the state context offered an explanation of whether working relations developed and in relation to which types of online citizen-led policing. An important limitation presented by the method of systematic literature review and meta-synthesis is that a literature review cannot make any claims about the prevalence of different forms of online citizen-led policing, government responses and their effects. This is highly biased by the cases selected in the research based on different case selection strategies and limitations of access. Furthermore, meta-synthesising results crossing different research paradigms presented a challenge to this literature review, but also contributed to developing an explanation as to why studies into online citizen-led policing conceptualise the phenomenon and its relations to government law enforcement in highly different ways, arriving at different conclusions, empirically and normatively, about whether online citizen-led policing can be considered a partner in crime-fighting.

A schism exists between studies departing from a functionalist paradigm and those departing from a critical paradigm. Most studies, similar to other studies on citizen participation in policing (cf. Terpstra, 2016), implicitly use a functionalist paradigm in empirically evaluating online citizen-led policing and its relations to government law enforcement. They consider citizen-led policing to be an instrument that can be used at the discretion of government law enforcement. This ignores the context of policing: the role of the police is not static, but differs between states and policing paradigms. Any

RIANNE DEKKER

conclusion about partnerships between online citizen-led policing and government law enforcement and statements about functional or dysfunctional outcomes for public security are therefore limited to a situated definition of government law enforcement.

Another strand of literature departs from a critical paradigm in which citizen policing generally is assumed to enhance state capacity – according to Foucaultian idealtypes of panoptic surveillance and governmentality (Foucault, 1991; 1995). However, when such studies refrain from empirically studying how governments steer and use online citizen-policing, they might overgeneralise the capacity and desire of states to utilise their power and ignore checks and balances put in place by which democratic states constrain this power.

A way forward would be for future research to be more explicit about the ontological and epistemological underpinnings of the research used to study empirical examples of online citizen-led policing. This will allow readers to better understand the findings and implications. Furthermore, future studies could be more explicit about how they conceptualise the police function and reflect on its contextualised nature. Lastly, current literature could benefit from moving beyond single case studies towards a more systematic comparison of cases and contexts.

## REFERENCES

- Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, 2(4), 479-497.
- Blitvich, P.G.C. (2022). Moral emotions, good moral panics, social regulation, and online public shaming. *Language & Communication*, 84, 61-75.
- Booth, A., Papaoianno, D., & Sutton, A. (2012). *Systematic Approaches to a Successful Literature Review*. Sage.
- Byrne, D.N. (2013). 419 digilantes and the frontier of radical justice online. *Radical History Review*, 117, 70-82.
- Button, M., & Whittaker, J. (2021). Exploring the voluntary response to cyber-fraud: From vigilantism to responsabilisation. *International Journal of Law, Crime and Justice*, 66, 1-9.
- Chang, L.Y., Zhong, L.Y., & Grabosky, P.N. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, 12(1), 101-114.
- Chang, L.Y., & Zhu, J. (2020). Taking justice into their own hands: Predictors of netilantism among cyber citizens in Hong Kong. *Frontiers in Psychology*, 11, 556903.
- Cheong, P.H., & Gong, J. (2010). Cyber vigilantism, transmedia collective intelligence, and civic participation. *Chinese Journal of Communication*, 3(4), 471-487.

- Chia, S.C. (2019). Crowd-sourcing justice: tracking a decade's news coverage of cyber vigilantism throughout the Greater China region. *Information, Communication & Society*, 22(14), 2045-2062.
- Chiang, E., De Rond, M., & Lok, J. (2023). Identity in a Self-styled 'Paedophile-hunting' Group: A Linguistic Analysis of Stance in Facebook Group Chats. *Applied Linguistics*, early view online.
- Cornwall, A. (2002). Locating Citizen Participation. *IDS Bulletin* 33(2), 49-58.
- Dennis, K. (2008). Keeping a close watch – the rise of self-surveillance and the threat of digital exposure. *The Sociological Review*, 56(3), 347-357.
- Dekker, R., & Meijer, A.J. (2020). Citizens as aides or adversaries? Police responses to digital vigilantism. In D. Trottier, R. Gabdulhakov & Q. Huang (Eds.), *Introducing Vigilant Audiences* (pp. 281-306). Open Book Publishers.
- De Rond, M., Lok, J., & Marrison, A. (2022). To catch a predator: The lived experience of extreme practices. *Academy of Management Journal*, 65(3), 870-902.
- Diphooorn, T., & van Stapele, N. (2021). What Is Community Policing? Divergent Agendas, Practices, and Experiences of Transforming the Police in Kenya. *Policing: A Journal of Policy and Practice*, 15(1), 399-411.
- Douglas, D.M. (2016). Doxing: a conceptual analysis. *Ethics and Information Technology*, 18(3), 199-210.
- Dynel, M., & Ross, A.S. (2021). You don't fool me: On scams, scambaiting, deception, and epistemological ambiguity at r/scambait on Reddit. *Social Media + Society*, 7(3), 20563051211035698.
- Favarel-Garrigues, G. (2020). Digital vigilantism and anti-paedophile activism in Russia. Between civic involvement in law enforcement, moral policing and business venture. *Global Crime*, 21(3-4), 306-326.
- Fink, A. (2010). *Conducting Research Literature Reviews. From the Internet to Paper* (3rd ed.). Sage.
- Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon & P. Miller (Eds.), *The Foucault Effect: Studies in Governmentality*. University of Chicago Press.
- Foucault, M. (1995). *Discipline and Punish: The Birth of the Prison* (2nd ed.). Vintage Books.
- Gabdulhakov, R. (2018). Citizen-led justice in post-communist Russia: From comrades' courts to dotcomrade vigilantism. *Surveillance & Society*, 16(3), 314-331.
- Gabdulhakov, R. (2020). (Con)trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia. *Global Crime*, 21(3-4), 283-305.
- Gabdulhakov, R. (2021). Media Control and Citizen-Critical Publics in Russia: Are Some 'Pigs' More Equal Than Others? *Media and Communication*, 9(4), 62-72.
- Gao, L., & Stanyer, J. (2014). Hunting corrupt officials online: The human flesh search engine and the search for justice in China. *Information, Communication & Society*, 17(7), 814-829.

RIANNE DEKKER

- Goode, E., & Ben-Yehuda, N. (1994). *Moral Panics: The Social Construction of Deviance*. Blackwell.
- Gray, G., & Benning, B. (2019). Crowdsourcing criminology: Social media and citizen policing in missing person cases. *Sage Open*, 9(4), 2158244019893700.
- Hadjimatheou, K. (2021). Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters. *Criminology & Criminal Justice*, 21(4), 547-565.
- Haggerty, K.D., & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51, 605-622.
- Herold, D.K. (2008). Development of a civic society online? Internet vigilantism and state control in Chinese cyberspace. *Asia Journal of Global Studies*, 2(1), 26-37.
- Huang, Q. (2023). The discursive construction of populist and misogynist nationalism: Digital vigilantism against unpatriotic intellectual women in China. *Social Media + Society*, 9(2), 20563051231170816.
- Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice*, 13(1), 81-97.
- Ireland, L. (2023). The acquisition of legitimacy for civilian policing: A case study of pedophile hunting groups. *Crime, Law and Social Change*, 79(2), 195-216.
- Jane, E.A. (2017). Feminist digilante responses to a slut-shaming on Facebook. *Social Media + Society*, 3(2), 2056305117705996.
- Kohm, S.A. (2009). Naming, shaming and criminal justice: Mass-mediated humiliation as entertainment and punishment. *Crime, Media, Culture*, 5(2), 188-205.
- Li, Y.T., & Whitworth, K. (2023). Coordinating and doxing data: Hong Kong protesters' and government supporters' data strategies in the age of datafication. *Social Movement Studies*, 23(3), 1-18.
- Liberati, A., Altman, D., Tetzlaff, J., Mulrow, C., Gøtzsche, P., Ioannidis, J., Clarke, M., Devereaux, P., Kleijnen, J., & Moher, D. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. *Academia and Clinic*, 151(4), 65-94.
- Loveluck, B. (2020). The many shades of digital vigilantism. A typology of online self-justice. *Global Crime*, 21(3-4), 213-241.
- Milbrandt, T. (2017). Caught on camera, posted online: mediated moralities, visual politics and the case of urban 'drought-shaming'. *Visual Studies*, 32(1), 3-23.
- Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Annals of Internal Medicine* 6(6), 2642-2669.
- Mols, A., & Pridmore, J. (2019). When citizens are 'actually doing police work': The blurring of boundaries in WhatsApp neighbourhood crime prevention groups in The Netherlands. *Surveillance & Society*, 17(3/4), 272-287.

- Nakamura, L. (2014). 'I WILL DO EVERYthing That Am Asked': Scambaiting, digital show-space, and the racial violence of social media. *Journal of Visual Culture*, 13(3), 257-274.
- Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston marathon bombings. *British Journal of Criminology*, 57(2), 341-361.
- Ong, R. (2012). Online vigilante justice Chinese style and privacy in China. *Information & Communications Technology Law*, 21(2), 127-145.
- Oravec, J.A. (2020). Online social shaming and the moralistic imagination: The emergence of Internet-based performative shaming. *Policy & Internet*, 12(3), 290-310.
- Petticrew, M., & Roberts, H. (2006). *Systematic Reviews in the Social Sciences: A Practical Guide*. Blackwell Publishing.
- ResearchRabbit (2024). FAQ. Accessed 14 March 2024, from <https://researchrabbit.notion.site/Welcome-to-the-FAQ-c33b4a61e453431482015e27e8af40d5>.
- Rheingold, H. (2003). *Smart mobs: The next social revolution*. Basic Books.
- Škorić, M.M., Wong, K.H., Chua, J.P.E., Yeo, P.J., & Liew, M.A. (2010). Online shaming in the Asian context: Community empowerment or civic vigilantism? *Surveillance & Society*, 8(2), 181-199.
- Smallridge, J., Wagner, P., & Cowl, J.N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology*, 8(1), 57-70.
- Surowiecki, J. (2005). *The wisdom of crowds*. Anchor.
- Tanner, S., & Campana, A. (2020). 'Watchful citizens' and digital vigilantism: a case study of the far right in Quebec. *Global Crime*, 21(3-4), 262-282.
- Terpstra, J.B. (2016). Tussen Heumensoord en Winschoten. Over de tegenstrijdige betekenis van burgerparticipatie in de veiligheidszorg. *Justitiële Verkenningen*, 42(5), 80-88.
- Tippett, A. (2024). The rise of paedophile hunters: To what extent are cyber-vigilante groups a productive form of policing, retribution and justice? *Criminology & Criminal Justice*, 24(4), 711-732.
- Trottier, D. (2014a). Crowdsourcing CCTV surveillance on the Internet. *Information, Communication & Society*, 17(5), 609-626.
- Trottier, D. (2014b). Police and user-led investigations on social media. *Journal of Law, Information and Science*, 23(1), 75-96.
- Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, 30, 55-72.
- Vasigh, M. (2013). Smile, you are under arrest: the misappropriation and misuse of mug shots online. *Information & Communications Technology Law*, 22(3), 277-298.
- Vicenová, R. (2020). The role of digital media in the strategies of far-right vigilante groups in Slovakia. *Global Crime*, 21(3-4), 242-261.

RIANNE DEKKER

- Walsh, D., & Downe, S. (2005). Meta-synthesis Method for Qualitative Research: A Literature Review. *Journal of Advanced Nursing*, 50(2), 204-211.
- Wästerfors, D., Burcar Alm, V., & Hannerz, E. (2023). The bumpy paths of online sleuthing: Exploring the interactional accomplishment of familiarity, evidence, and authority in online crime discussions. *New Media & Society*, early view online.
- Weber, M. (1987 [1919]). *Politik als Beruf* (8th ed.). Duncker & Humblot.
- Whelan, C., & Harkin, D. (2021). Civilianising specialist units: Reflections on the policing of cyber-crime. *Criminology & Criminal Justice*, 21(4), 529-546.
- Yardley, E., Lynes, A.G.T., Wilson, D., & Kelly, E. (2018). What's the deal with 'websleuthing'? News media representations of amateur detectives in networked spaces. *Crime, Media, Culture*, 14(1), 81-109.
- Zimmer, L. (2006). Qualitative Meta-synthesis: A Question of Dialoguing with Texts. *Journal of Advanced Nursing*, 53(3), 311-318.

## ABOUT THE AUTHORS

**Dr Greg Alpar** is the education innovator of iCIS, the Computing Science (CS) department of Radboud University. Prior to this position, he worked as an Assistant Professor at the Open University of the Netherlands, teaching CS and software engineering courses and doing research in cryptography and privacy. He has published extensively on topics including encryption, identity management and CS education.

**Dr Willem Bantema** is Professor of Governance in a Digitalizing Society at NHL Stenden University of Applied Sciences. His main area of interest is the role of local governments regarding safety and security in the digital society.

**Maike Berkenpas BSc** is a teacher and researcher at NHL Stenden University of Applied Sciences, Cybersafety Research Group. Her primary focus is digital resilience of citizens and organisations.

**Kimberly Bluhm MSc** is a researcher at NHL Stenden University of Applied Sciences. Her primary field of interest is behaviour change in relation to cyber resilience.

**Bas Böing** is captain at the Dutch National Police and a PhD candidate at the Department of Psychology of Conflict, Risk and Safety at the University of Twente. His primary field of interest is ethnic profiling, for which he has developed a virtual reality simulation to train police officers.

**Carlos J. Calleja** is a PhD candidate at the Norwegian Police University College. His primary field of interest is how the law regulates preventive policing on the internet.

**Dr Tanja Kammersgaard Christensen** is an Assistant Professor at the Department of Law of Aalborg University. Her primary field of interest is data protection.

**Dr Rianne Dekker** is an Assistant Professor at the Utrecht University School of Governance (USG/USBO).

**Kevin Emplit** is a PhD candidate in the Department of Sociology at Université libre de Bruxelles. His research primarily focuses on the digitalisation of police operations and the changing nature of the day-to-day work of frontline police officers, their working conditions and internal hierarchical relations in the digital era.

**Nienke de Groes** is a PhD candidate at the Institute of Security and Global Affairs of Leiden University.

*ABOUT THE AUTHORS*

**Dr Jurjen Jansen** is a Professor of Digital Resilience of Citizens and Organizations at NHL Stenden University of Applied Sciences and the Dutch Police Academy. His research interests include human-centred cyber resilience, policing in a digitised society, online crime, behaviour change and human-computer interaction.

**Dr Wouter Landman** is an independent researcher and consultant. His research interests include policing in a digitised society and digital transformation in police organisations.

**Dr Lene Wachter Lentz** is an Associate Professor in the Department of Law at Aalborg University. Her research focuses on cybercrime, digital investigations and digital evidence used in court.

**Maxime Mauquoy** is a researcher at the Institut National de Criminologie et de Criminologie (INCC) in Brussels. His primary field of interest is forensic intelligence, and the issues involved in its implementation.

**Lies Vande Meulebroucke** is a PhD candidate in the Department of Criminology at Vrije Universiteit Brussel. Her research primarily focuses on the digitalisation of police operations and its impact on police legitimacy and public relations.

**Prof. Dr Markus Naarttijärvi** is a Professor of Law at Umeå University, Sweden. His primary field of interest is the intersection between emerging technology, security and the rule of law, with a specific focus on the use of surveillance and AI in policing.

**Dr Vlad Niculescu-Dinca** is Assistant Professor at the Institute of Security and Global Affairs of Leiden University. His interests lie in interdisciplinary research at the intersection of security governance, philosophy of technology, surveillance studies and policing studies.

**Meret Asara Paululat** is a clinical psychologist and a PhD candidate at the Department of Human Medicine at the University of Oldenburg. Meret focuses on combining clinical psychological research with interdisciplinary practical applications, with a special interest in policing and governance.

**Dr Sarah Van Praet** is a researcher at the National Institute for Criminalistics and Criminology in Brussels and a visiting lecturer at the faculty of Law and Criminology of the Université libre de Bruxelles.

*ABOUT THE AUTHORS*

**Dr Wendy Schreurs** is a scientific researcher at the Dutch Police Academy. Her primary field of interest is intelligence and data-driven police work and its implications for police organisations and the public.

**Prof. Dr Wouter Stol** is Professor in Cybersafety at NHL Stenden University of Applied Sciences and the Dutch Police Academy, Professor in Police Studies at the Netherlands Open University and chief inspector at the Dutch National Police. His main field of interest is everyday police practice in a digitalised society.

**Dr Inger Marie Sunde** is a Professor at the Norwegian Police University College.

**Prof. Dr ir. Jan Terpstra** is Emeritus Professor of Criminology at Radboud University, Nijmegen, and a Fellow at Leyden University, The Hague campus, both in the Netherlands. His research and publications cover the broad field of policing and security.

**Prof. Dr Pieter Tops** is Emeritus Professor for Undermining Studies at Leiden University.

**Dr ir. Peter W. de Vries** is an Assistant Professor at the University of Twente, the Netherlands. His research interests revolve around human-technology interaction.

**Saskia Westers MSc** is a researcher at NHL Stenden University of Applied Sciences. Her primary field of interest is policing in a digitised society.

