European data protection law in the police sector: a legal framework to protect individuals in the context of preventative police surveillance?

LL.M. Law and Technology
Tilburg Institute for Law, Technology and Society, Tilburg University
Aldo Sghirinzetti
Snr 2031351
November 2019
Supervisor: Magdalena Brewczyńska
Second Reader: Prof. Dr. Bert-Jaap Koops
**Table of contents**

List of abbreviations ........................................................................................................................................... 4

1. Introduction .................................................................................................................................................. 5
   1.1 Background.............................................................................................................................................. 5
   1.2 Aim and research questions ................................................................................................................... 7
      1.2.1 Main research question .................................................................................................................. 8
      1.2.2 Sub-questions ................................................................................................................................... 8
   1.3 Methodology, methods and chapters’ overview ...................................................................................... 8
      1.3.1 Methodology .................................................................................................................................... 8
      1.3.2 Methods .......................................................................................................................................... 9
      1.3.3 Chapters’ overview ......................................................................................................................... 10
   1.4 Preliminary remarks and limitations ...................................................................................................... 11
   1.5 Significance ........................................................................................................................................... 13

2. Preventative police surveillance and the individual: in need of legal protection ..........14
   2.1 Introduction ........................................................................................................................................... 14
   2.2 The role of criminal procedure in regulating police surveillance: opacity and transparency tools ........................................... 16
   2.3 Opacity and transparency tools in English and Italian criminal procedure .......... 17
      2.3.1 England and Wales ....................................................................................................................... 18
      2.3.2 Italy ................................................................................................................................................ 21
   2.4 Enter preventative police surveillance ................................................................................................. 23
   2.5 Preventative police surveillance and privacy as non-domination ................................. 27
   2.6 Conclusion ........................................................................................................................................... 29

3. The European data protection regime and its applicability to preventative police surveillance ........................................... 30
   3.1 Introduction ........................................................................................................................................... 30
   3.2 CoE data protection law ....................................................................................................................... 32
      3.2.1 Convention 108+ ............................................................................................................................. 32
3.2.2 The Police Recommendation ................................................................. 33
3.3 EU Data protection law ............................................................................. 36
3.3.1 Before the Law Enforcement Directive ................................................ 36
3.3.2 The Law Enforcement Directive ............................................................ 37
3.4 Security-related concepts in European law: in need for definitions .......... 39
3.5 Conclusion ............................................................................................... 41
4. Checks and balances for preventative police surveillance: the safeguards provided in data protection law ................................................................. 43
4.1 Introduction .............................................................................................. 43
4.2 Antipower in the surveillance context ....................................................... 43
4.3 Heald’s anatomy of transparency and its relevance for data protection law .... 46
4.4 The safeguards provided by data protection law ....................................... 48
  4.4.1 Information and access rights ............................................................... 49
  4.4.2 The accountability of data controllers ................................................ 51
  4.4.3 The role of Data Protection Authorities .......................................... 54
4.5 Conclusion ............................................................................................... 56
5. Conclusion ................................................................................................... 59

Bibliography ....................................................................................................... 63

Table of cases .................................................................................................. 63
Table of legislation ........................................................................................... 63
Secondary sources ............................................................................................ 65
## List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV</td>
<td>Closed-circuit television</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>Cpp</td>
<td>Codice di procedura penale (Italian Code of Criminal Procedure)</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)</td>
</tr>
<tr>
<td>MSs</td>
<td>Member States of the European Union</td>
</tr>
<tr>
<td>PACE</td>
<td>Police and Criminal Evidence Act 1984</td>
</tr>
</tbody>
</table>
1. Introduction

1.1 Background

The evolution of technology and its assimilation in our daily lives is changing several power structures, challenging the way current laws protect citizens from powerful actors in different contexts, such as employment relationships, commerce, and the relationship between individuals and the police. Digital technology enables organisations to collect ever-increasing amounts of information on individuals, to be put to different uses depending on the context and the powerful actor. So, for example, the worried employer monitors digital workstations’ usage to find out about idle employees, internet platforms collect data on almost anything we do online in order to provide us with targeted advertising, and the police monitor social media in order to gather information on an ongoing protest.

These trends have brought David Murakami Wood and others to consider that this ‘surveillance society’ is a prominent trait of modern life. In a frequently cited report, they neatly portray these patterns through the account of a week in the daily life of an average UK citizen in the year 2006. From the airport to the school, from the street to the hospital, large scale technological systems collect information on every individual within their reach. Social security databases, frequent flier discount programs, traffic monitoring systems, and many other surveillance assemblages ‘represent a basic, complex infrastructure which assumes that gathering and processing personal data is vital to contemporary living’.

In the context of law enforcement, the increased imprint of surveillance technology and data collection goes hand in hand with an increase of the importance of security-management policies. Over the last few decades, narratives oriented towards the minimisation of (quite different) risks to our societies have escalated in the public debate. In a feedback loop, politicians, the media, and the general public promote a universal call for risk-management policies, so that safety is established almost as ‘an overarching value

---

3 Murakami Wood and others (n 2) para 1.2.
4 The term security is used here on purpose in a very broad sense: as it will emerge from the following paragraphs, security policies include now not only facing extreme social problems, such as terrorism and organised crime, but also managing less critical problems related to urban life, such as petty crime or even the presence of beggars.
that trumps all other considerations.’ High profile incidents and real or perceived social problems warrant each time new security initiatives. ‘Someone has to do something about it’, is the usual refrain.

As a consequence, ‘legal measures for preventing and investigating crime respond to public expectations and perceptions of insecurity rather than intrinsic needs of crime-fighting and actual insecurity.’ Hence, non-criminal or quasi-criminal behaviour is more and more often equated to criminal behaviour in being viewed as a social problem or risk to be managed by the criminal justice system. Not only in the perception of the general public, but also in that of law enforcement institutions.

This tendency can be seen in several aspects of the criminal justice system. On the one hand, substantive criminal law is broadening in scope as preparatory acts are increasingly criminalised (e.g., within the context of cybercrime acts and anti-terrorism measures) and other forms of behaviour are regulated in quasi-criminal administrative measures. As already noted, the consequence is that, along with extreme forms of deviant social behaviour, also less problematic forms of behaviour are managed as part of crime control strategies. On the other hand, criminal procedure is expanding, for instance, through the growth of interception powers and the inevitable expansion of existing ones, enabled by the use of new technologies.

These trends are a key factor in a paradigm shift, where criminal law is becoming – or probably, at least partially, already became – a primary tool to regulate perceived social risks. A major feature of this paradigm shift is the move from a reactive role of the criminal justice system, to a preventative one. In the reactive model, specific surveillance

---

6 Koops, ‘Technology and the Crime society’ (n 5) 104.
8 For instance, in Italy, this phenomenon is related to an expansion in the use of mayors’ local powers to enforce measures for ‘public safety’ control. Rossella Selmini, ‘Towards Città Sicure? Political Action and Institutional Conflict in Contemporary Preventive and Safety Policies in Italy’ (2005) 9 Theoretical Criminology 307. Most recently, a government decree introduced the possibility for mayors to ‘fine and then banish from accessing certain areas of the city those who “put in place behaviours that restrict the free accessibility and use” of transport infrastructure’. This resulted, for example, in the ban of a beggar from the stairs of a metro stop, and of a drunk person with past criminal records, who was ‘bothering’ passengers of a tram line. Il Post, ‘Cos’è il “DASPO urbano”’ Il Post (Milano, 25 September 2018) <https://www.ilpost.it/2018/09/25/daspo-urbano/> accessed 6 September 2019.
10 For a more extensive discussion of the concept of paradigm shift in criminal law and its consequences on legal protection, see Koops, ‘Technology and the Crime society’ (n 5) 115ff.
powers are employed by the police after a specific activating fact (e.g., after they have knowledge of a crime), while in the preventative model broad surveillance powers are employed by default, because a threat to public security might materialize at any moment. This can be seen, for example, in the increased use of predictive tools in several government areas,\(^\text{11}\) in the employment of ‘big data policing’,\(^\text{12}\) but also in new and untargeted applications of instruments previously used in a targeted fashion.\(^\text{13}\) As the boundaries of criminal law blur in this shift towards pre-crime and intelligence-led approaches,\(^\text{14}\) therefore, police surveillance is increasingly employed outside traditional criminal investigations. This, as we will see in the second chapter of this work, challenges the legal tools that regulate traditional surveillance powers and which protect individuals’ rights, and in particular their right to privacy.

### 1.2 Aim and research questions

Zooming in on one of the various aspects characterising the abovementioned paradigm shift in criminal justice – the shift towards untargeted measures of police surveillance in the context of preventative approaches to crime control – this thesis will try, firstly, to clarify the effects of such a trend on privacy protection and, secondly, to identify possible alternative means of protection, outside criminal procedure. These alternative means of protection will be looked for, specifically, in European data protection law since, as it will emerge from the following chapters of this work, this would seem a particularly useful instrument to regulate preventative police surveillance.

It will be key to put this problem in the perspective of our current democratic institutions and the rule of law. In fact, it is not only critical to provide individuals with actionable rights, to receive protection from police abuse of surveillance powers, but even more to


\(^\text{13}\) Video surveillance, for example, is classically used to acquire evidence against a specific individual in a criminal investigation, but more recently it has been massively deployed to control crime in public spaces. Marc J Blitz, ‘Local Law Enforcement Video Surveillance: Rules, Technology, and Legal Implications’ in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (1st edn, Cambridge University Press 2017). Additionally, the use of IMSI-catchers in an untargeted fashion has been documented by journalists at least once in the UK. Ben Bryant, ‘VICE News Investigation Finds Signs of Secret Phone Surveillance Across London’ (*Vice News*, 14 January 2016) <https://news.vice.com/en_us/article/bjdkdw/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london> accessed 30 March 2019. IMSI-catchers are technological devices which can identify the unique subscription number assigned to a user of a mobile telecommunication network. For a more detailed discussion of IMSI-catchers’ untargeted and preventative use, see Section 2.4.

\(^\text{14}\) Mireille Hildebrandt, ‘Criminal Law and Technology in a Data-Driven Society’ in Markus D Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal Law* (Oxford University Press 2014) 15.
preserve the balance among different State powers, and between these powers and individuals’ rights.\textsuperscript{15}

1.2.1 Main research question

How is it possible to provide for individuals’ legal protection in the context of preventative police surveillance?

1.2.2 Sub-questions

1. How are individuals classically protected from undue police surveillance in the criminal justice system, and how do new forms of preventative police surveillance challenge this?

2. How does the European data protection regime, including but not limited to the EU Law Enforcement Directive, protect individuals in the context of preventative police surveillance?
   
   2.1. Is the European data protection regime applicable to preventative police surveillance?
   
   2.2. What are the most important safeguards provided therein?

1.3 Methodology, methods and chapters’ overview

1.3.1 Methodology

The methodology chosen for this work is doctrinal legal research. This methodology entails researching from a legal-internal perspective; that is, to analyse the legal problem from a purely legal point of view. Smits describes this approach as a ‘description through systematisation’ and as a creation through description. Even though he considers the doctrinal approach to be mainly descriptive, and indeed most of the sub-questions in this thesis are descriptive, he maintains that a normative component is also inherent in the description itself.\textsuperscript{16} Throughout the thesis, I will make use of legal and political theory, mainly from neorepublican literature, in order to provide for a theoretical framework to answer the main research question. This choice is firstly due to the fact that the neorepublican conceptualisation of freedom as non-domination seems particularly fit to properly acknowledge some of the consequences of preventative police surveillance on


individuals’ privacy.\textsuperscript{17} Secondly, neorepublican literature also presents some introductory ideas on how to face these consequences, subsumed in the concept of ‘antipower’.\textsuperscript{18} Thirdly, being strongly concerned with the maintenance of the right balance between State power and individuals’ freedom, it can help guiding the normative component which is intrinsic to doctrinal legal research.

Concerning the choice of jurisdictions, this thesis is written from a European perspective and it will mainly deal with legal sources from the law of the Council of Europe and of the European Union. Nevertheless, in the second chapter, I will use English and Italian law of criminal procedure to analyse how this law regulates police surveillance within criminal investigations. It is important to note that there is no comparative purpose in such analysis, as the recourse to national law is necessary only because this field of law is not sufficiently harmonised yet. These jurisdictions will therefore provide illustrative examples of how, even in quite different legal traditions,\textsuperscript{19} the law of criminal procedure follows the same steps in regulating police surveillance powers. Namely, by defining the conditions under which they can be exercised, and by providing for safeguards to avoid abuses.

\subsection*{1.3.2 Methods}

In order to write this thesis, I carried out a desk research and a qualitative analysis of primary and secondary sources following the subsequent steps:\textsuperscript{20}

- Identify a legal problem;
- Formulate research questions;
- Choose search terms;
- Locate, select and read background information (secondary sources);
- Locate, select and read primary sources;
- Synthesise results;
- Draw conclusions.

\textsuperscript{17} See Section 2.5.
\textsuperscript{18} See Sections 3.1 and 4.2.
\textsuperscript{19} The English system is accusatorial, while the Italian system – although with important accusatorial transplants – preserves an inquisitorial backbone. Nevertheless, it is worth noting that, at least according to some authors, the distinction between inquisitorial and accusatorial systems might not be that relevant anymore. See JR Spencer, ‘Adversarial vs inquisitorial systems: is there still such a difference?’ (2016) 20 The International Journal of Human Rights 601.
After having identified key words, I executed online searches, mainly using the Google Scholar engine and the WorldCat database. Sources were then selected reading abstracts and/or table of contents, or reading their entire content. Oftentimes, after having identified a particularly relevant secondary source, I used its bibliography or looked at other sources citing it to further extend my research.

1.3.3 Chapters’ overview

After this introduction, Chapter 2 will sketch out the background of how preventative forms of police surveillance challenge the legal protection offered to individuals by the law of criminal procedure. Making use of De Hert’s and Gutwirth’s conceptualisation of opacity and transparency tools and drawing examples from two European jurisdictions – Italy, and England and Wales – I will clarify the role of criminal law in protecting individuals from undue police surveillance. After a brief explanation of preventative police surveillance and why this falls outside the scope of criminal procedure, an account of the right to privacy through the lens of the neorepublican theory of non-domination will help explaining the need for privacy protection in this context. Moreover, the neorepublican concept of ‘antipower’ will provide for the basic elements in the search for possible solutions.

In Chapter 3, I will introduce the European data protection framework, including both the law of the Council of Europe (‘CoE’) and that of the European Union (‘EU’). Moving from De Hert’s and Gutwirth’s conceptualisation of data protection as a transparency tool, I will explain why it is highly desirable to use it as a tool for legal protection in the context of preventative police surveillance. Throughout the chapter, I will then analyse the scope of the certain European data protection instruments – namely, CoE’s Convention for the Protection of individuals with regard to automatic processing of personal data22 and its

---

21 To start my research, I used keywords such as ‘untargeted surveillance’, ‘preventative surveillance’, ‘police’, ‘law enforcement’, ‘legal protection’, ‘criminal law’, ‘criminal procedure’. These keywords were combined to form search strings such as ‘surveillance AND “legal protection” AND (police OR “law enforcement”)’ and adapted to find relevant results according to initial findings.

22 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS 108. Convention 108 has been recently modernised by an additional protocol which brings it in line with the reform of the data protection framework at the EU level. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [2018] CETS 223. The consolidated text, along with an explanatory memorandum, is available on the website of the Council of Europe. See Council of Europe, ‘Convention 108+. Convention for the protection of individuals with regard to the processing of personal data’ (Council of Europe 2018) <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regard/16808b36f1> accessed 19 July 2019 (hereafter, I will mainly refer to the modernised version as ‘Convention 108+’ and, only when this is necessary for chronological consistency, to ‘Convention 108’).

In Chapter 4, I will use the neorepublican concept of antipower in order to identify which elements could provide for legal protection in the context of preventative police surveillance. Analysing data protection law through the lens of Heald’s anatomy of transparency, I will describe how data protection increases the transparency of such practices and how it can provide for a balancing instrument in the context of the power relation between citizens and the police.

Finally, Chapter 5 will summarise the conclusions drawn after each chapter and answer the main research question. It will also contain some suggestions on how data protection measures could be further improved to serve as an antipower in the context of preventative police surveillance, and some suggestions for further research.

1.4 Preliminary remarks and limitations

As explained above, the paradigm shift in criminal law described in the first paragraphs of this thesis is a complex phenomenon, affecting different dimensions of the criminal justice system.25 The scope of this thesis will cover only one of them, namely the shift from a reactive model towards a preventative one. The focus will be partly on the effects of this shift on individuals’ privacy protection (Chapter 2) and, even more, on how to provide for alternative means of legal protection in this new context. This thesis will therefore not deal with other important issues, such as the surveillance carried out by private actors exercising police functions, or by security and intelligence services in the context of national security.26

Moreover, this thesis will focus solely on preventative police surveillance. That is, surveillance activities carried out by the police force, which can be defined as ‘the governmental department charged with the preservation of public order, the promotion of

---

23 Council of Europe, ‘Recommendation on the use of personal data in the police sector’ (R (87) 15, adopted by the Committee of Ministers on 17 September 1987).
26 Nevertheless, a discussion on the problem of distinguishing between national security and other security-related concepts will be carried out in Chapter 3.
public safety, and the prevention and detection of crime. Other law enforcement agencies are out of the scope of this work.

Another important clarification concerns the references to the rights to privacy and data protection. Although it is beyond the scope of this work to inquiry the relationship between such rights, I will try to clarify why I use data protection law as a main potential instrument to solve what I identify as a privacy problem.

First of all, in the context of this thesis, I am mainly concerned with the protection of informational privacy, which can be considered, according to Koops and others, ‘as a derivative or added layer of, or perhaps a precondition to, other forms of privacy’. As an overarching value, informational privacy protects the interest ‘in restricting access or controlling the use of information’ about different aspects of people’s lives. This interest, I believe, needs to be strongly protected in the context of the relationship between individuals and the State, as a precondition for democracy and the rule of law.

The overlap between (informational) privacy and data protection can be seen, for example, in the scope of Article 8 of the European Convention on Human Rights (‘ECHR’), which has been interpreted as covering a ‘wide range of issues’, including data protection. Not all personal data processing falls within the scope of Article 8, but only those which constitute an interference with individuals’ privacy.

Notwithstanding the fact that data protection ‘serves other, further fundamental rights and values besides privacy’, and that it is now a stand-alone right set at the EU ‘constitutional level’, European law on data protection has historically affirmed the importance of the right to privacy as the main fundamental right it intends to protect.

---

29 Koops and others (n 28) 569, 574.
31 This is generally assessed by the European Court of Human Rights (‘ECtHR’) having regard to ‘the nature of the data processed and the extent of the processing’. Gellert and Gutwirth (n 30) 526.
32 Maria Tzanou, ‘Data protection as a fundamental right next to privacy? “Reconstructing” a not so new right’ (2013) 3 International Data Privacy Law 88, 90. See also Gellert and Gutwirth (n 30) 530.
33 See section 3.3, and also De Hert and Gutwirth (n 15) 16.
34 The EU Data Protection Directive intended to ‘protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data’. Very similar words stated the objective of the Council Framework Decision. CoE Convention 108+ aims to ‘protect every individual (…) with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.’ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, Art 1(1) (‘Data Protection Directive’ or ‘DPD’); Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial
For this reason, I believe that ‘privacy [can still be considered] “one—if not the—major” value that data protection laws aim to safeguard’\textsuperscript{35} and it can be employed to solve privacy issues – in particular informational privacy issues.

1.5 Significance

I believe that this thesis will contribute, firstly, to clarify some of the issues raised by preventative police surveillance. In particular, using neorepublican ideas to explain why privacy should be considered not only from the individuals’ perspective, but even more crucially from the angle of power relations, could complement views in existing literature focused on privacy intrusions in the context of surveillance.

Secondly, this thesis will contribute to the academic debate on data protection in the law enforcement context, which is at the moment obfuscated by ever-present discussions on the General Data Protection Regulation.

Finally, I believe this work can also contribute to neorepublican legal-political theory, as applying the concept of antipower to data protection can be useful to further develop the concept itself, particularly as regards its use in the specific context of surveillance.

\textsuperscript{35} Maria Tzanou, ‘Data protection as a fundamental right next to privacy? “Reconstructing” a not so new right’ (2013) 3 International Data Privacy Law 88, 91.
2. Preventative police surveillance and the individual: in need of legal protection

2.1 Introduction

According to the Black’s Law Dictionary definition, surveillance means ‘close observation or listening of a person or place in the hope of gathering evidence.’ This definition reflects the role of surveillance in police investigations as traditionally regulated by the law on criminal procedure. Among others, this law serves two important functions: it provides the police with a legal basis to conduct surveillance activities, and it guarantees that these do not unduly interfere with citizens’ rights, including the right to privacy, by setting conditions for the exercise of those powers. These guarantees are provided mainly in two ways. Firstly, procedural rules clarify when and how certain investigative measures can be conducted; secondly, they provide for safeguards which ensure the accountability of the police, including mechanisms of supervision, usually by judicial bodies with guarantees of impartiality.

These principles are part of the traditional reactive model that is common to European criminal justice systems, in which the police act on the knowledge of a crime (usually reported to them by members of the public) and gather evidence about a suspected individual in view of a prosecution. The increased use of technology by the police, however, and the blurring of the line between the police’s role in criminal investigations and other functions of the police force – such as the prevention of threats to public security – has led to a shift of surveillance practices towards a preventative approach, widely recognised in literature. Here, the focus is not any more on crime investigation and prosecution, but rather on the prevention of crime and other risks to public security.

---

36 All translations are from the author, unless otherwise specified.
39 See Ed Cape and others, ‘Procedural rights at the investigative stage: towards real commitment to minimum standards’ in Ed Cape and others (eds), Suspects in Europe. Procedural Rights at the Investigative Stage of the Criminal Process in the European Union (Intersentia 2007) 20. The role of the law on criminal procedure in both restricting police power and protecting citizens’ rights will be examined in more details in Section 2.2 on tools of opacity and transparency.
40 See, eg, Koops, ‘Technology and the Crime society’ (n 5); Evelien De Pauw and others (eds), Technology-led policing (Maklu 2011); Mireille Hildebrandt (n 14); John Vervaele, ‘Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?’ in S Gutwirth, R Leenes and P De Hert (eds), Reloading Data Protection (Springer 2014); Andrew Guthrie Ferguson (n 12).
41 ‘Public security’ is used in this work as a term distinct from that of national security, which is outside the scope of this thesis. For a discussion on the problem of defining and distinguishing such terms, see Section 3.4.
In this mutated context, the definition of surveillance provided earlier falls short of fully acknowledging the multifaceted reality of police surveillance. A different and broader definition is therefore required in order to acknowledge this change of perspective.

Surveillance comprises the targeted or systematic monitoring (…) of persons, places, items, infrastructures or flows of information, in order to identify hazards and manage risk and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future.

In this surveillance environment, it is less clear what is the legal justification for the police using surveillance measures, what is the purpose of each act of surveillance, and what kind of protection is provided for individuals’ fundamental rights, including the right to privacy.

The purpose of this chapter is therefore to clarify the consequences of this paradigm shift on privacy protection, answering the first research question of this thesis:

1. How are individuals classically protected from undue police surveillance in the criminal justice system, and how do new forms of preventative police surveillance challenge this?

The chapter will proceed as follows: In Section 2.2, I will introduce the distinction between opacity and transparency tools, which will further explain the functions of criminal procedure introduced in the previous paragraphs. In Section 2.3, I will draw examples from English and Italian jurisdictions to better illustrate the function of these tools in regulating police powers and providing for protection from abuses. In Section 2.4, I will present some examples of preventative police surveillance and discuss how they challenge the traditional protective framework provided by criminal law. In Section 2.5, I will finally discuss how a neorepublican account of the right to privacy can help us better understand the implications of this kind of surveillance and identify possible means to control the exercise of such powers.


43 Regina Berglez and Reinhard Kreissl, ‘D 3.3 Report on security enhancing options that are not based on surveillance technologies’ (SurPRISE project, 2013) 6 <http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf> accessed 12 October 2019 (emphasis added). Also this definition might not cover all instances of surveillance, but it is broad enough to include most forms of preventative police surveillance described in this work. See Section 2.4.
2.2 The role of criminal procedure in regulating police surveillance: opacity and transparency tools

In the opening of this chapter, I introduced the importance of the rules of criminal procedure in regulating police powers and protecting individuals’ right to privacy. In order to properly account for the functions of these rules, there is a need to consider them in the broader institutional context of European democratic states. These functions are extensively discussed in a seminal work from De Hert and Gutwirth. According to these authors, power in modern democracies is ‘by definition limited’ by ‘the enactment of three basic constitutional principles, namely the recognition of fundamental rights and liberties, the rule of law (constitutionalism) and democracy.’

The first two elements are of particular relevance in the context of this thesis, as both of them contribute in different ways to protecting individuals and regulating the use of power. Fundamental rights, and in particular the right to privacy, establish a private sphere of the individual, separated from the control of the State, thus limiting the boundaries of State power.

The rule of law, in turn, subjects public bodies ‘to a set of restricting constitutional rules and mechanisms’. This guarantees, firstly, the principle of legality – that is, the rule according to which State agents derive their powers from the law and exercise them accordingly. Secondly, it provides for ‘a dynamic system of mutual control or checks and balances’, which guarantees the ‘mutual accountability of state powers’.

The two different functions played by fundamental rights and by the rule of law, namely defining individuals’ private spheres and regulating State interferences with them, is mirrored by the distinction between opacity and transparency tools. The first category consists in legal instruments allowing for interferences in the private sphere of individuals, which are permitted ‘only, in principle, if a series of stringent conditions are met’. A paradigmatic example provided by the authors is that of home protection: on the one hand, the constitutional legislator stipulates the inviolability of the home, on the other, it grants State agents the possibility of lawful trespass, for example upon the execution of a search warrant.

---

44 De Hert and Gutwirth (n 15) 4.
45 De Hert and Gutwirth (n 15) 4-5.
46 De Hert and Gutwirth (n 15) 5-6.
47 De Hert and Gutwirth (n 15) 8.
Through such tools the (constitutional) legislator enacts hard or clear norms. Choices about the way liberty interests and other interests should be balanced are made in an abstract way.\textsuperscript{48}

The second category entails mechanisms of transparency, accountability and independent supervision, which ‘take into account that the temptations of abuse of power are huge, and empower the citizens and special watchdogs to have an eye even on the legitimate use of power.’\textsuperscript{49} A good example of this kind of tools would be the rules establishing that a judge reviews warrant requests in order to control that the necessary requirements are fulfilled (e.g., that there is a clear link between the search itself and a substantive criminal provision and that the standard of proof is satisfied).

Opacity tools embody normative choices about the limits of power; transparency tools come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power.\textsuperscript{50}

To conclude, one way of summarising this theoretical framework could be the following. When framing opacity tools, the State determines that the individual has a sphere of autonomy, which the State itself has the power to intrude only \textit{if} certain conditions are met. Conversely, transparency tools provide that \textit{when} the State exercise this power, it does not abuse it.

\section*{2.3 Opacity and transparency tools in English and Italian criminal procedure}

This section will present some examples of tools of opacity and transparency, drawn from the law of criminal procedure in two European jurisdictions: England and Wales (‘England’) and Italy. In particular, the investigative powers\textsuperscript{51} of search and interception will be analysed. I chose these two powers for three main reasons. Firstly, because they constitute particularly privacy-invasive powers, as they have the potential of disclosing a great deal of personal and intimate information about an individual. Secondly, because the way in which they are regulated well exemplifies some aspects highlighted by De Hert and Gutwirth: the law requires strict conditions to be met for the police to be able to exercise them, and it provides for safeguards, mainly in the form of supervision from

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{48} De Hert and Gutwirth (n 15) 9.
\item\textsuperscript{49} De Hert and Gutwirth (n 15) 9-10.
\item\textsuperscript{50} De Hert and Gutwirth (n 15) 9.
\item\textsuperscript{51} An investigative power is ‘the authority conferred on a governmental agency to inspect and compel disclosure of facts germane to an investigation’. This includes means to look for evidence or to apprehend suspects, but also to interview witnesses or to order a survey of evidence. Bryan A Garner, ‘investigatory power’, \textit{Black's Law Dictionary} (n 27) 1288.
\end{itemize}
\end{footnotesize}
judicial bodies, to control that such exercise is lawful. Thirdly, because they are among the most commonly used surveillance powers in the classic reactive model of police investigations.

2.3.1 England and Wales

Despite not having a written constitution, England has several sources of law, such as the Magna Charta and ‘books of ancient authority’, which are considered to have a constitutional status.\(^{52}\) In particular as regards fundamental rights, the Human Rights Act 1998 incorporates the European Convention on Human Rights in the legal system, therefore also providing for the right to respect for private and family life, home and correspondence (Article 8).\(^ {53}\) The sources of criminal procedure are found in common law and in several statutes. Concerning police organisation, in England the police force is structured locally and it is formally independent from the executive, even if they follow the guidance of the Home Secretary.\(^ {54}\) During the investigative phase, the police lead the investigation and are not supervised by a prosecutor.\(^ {55}\) Every constable (police officer) ‘hold[s] office under the crown’ and ‘is personally responsible for deciding how to use legal powers and perform legal duties.’\(^ {56}\) Nevertheless, they still have to request warrants in order to be able to exercise certain surveillance powers.\(^ {57}\)

Of relevance for the issues discussed are the Police and Criminal Evidence Act 1984 and the Investigatory Powers Act 2016.\(^ {58}\)

Concerning searches, the police can enter premises without a warrant in case they have a serious reason to believe that a suspect of an arrestable offence is located in the searched

---

\(^{52}\) Penny Darbyshire, ‘Criminal Procedure in England and Wales’ in Richard Vogler and Barbara Huber (eds), Criminal Procedure in Europe (Duncker and Humblot 2008) 55.

\(^{53}\) The hierarchical role of the Human Rights Act 1998 is weakened by the principle of parliamentary supremacy and the fact that courts can only interpret the law in a compatible way, and not invalidate legislation which does not meet its requirements. Nevertheless, the role of the ECHR has been critical in improving procedural safeguards in English criminal procedure. For example, with regard to the introduction of statutory provisions regulating the interception of communications after Malone. Malone v The United Kingdom (1984) Series A no 82.

\(^{54}\) JR Spencer, ‘The English system’ in Mireille Delmas-Marty and JR Spencer (eds), European Criminal Procedures (Cambridge University Press 2002) 150-51. After the institution of Police and Crime Commissioners, who are elected officials in charge of ensuring the effectiveness of police action in local areas, the political independence of the police is more debated, even though this discussion does not directly involve the executive branch of the government. See, eg, Stuart Lister, ‘The New Politics of the Police: Police and Crime Commissioners and the “Operational Independence” of the Police’ (2013) 7 Policing: A Journal of Policy and Practice 239.

\(^{55}\) Ed Cape and Jacqueline Hodgson, ‘The investigative stage of the criminal process in England and Wales’ in Ed Cape and others (eds), Suspects in Europe. Procedural Rights at the Investigative Stage of the Criminal Process in the European Union (Intersentia 2007) 61; Spencer (n 54) 165.


\(^{57}\) Spencer (n 54) 165.

\(^{58}\) Spencer (n 54) 144-45; Cape and Hodgson (n 55) 61.
place, or they can enter the premises of an arrested person to look for evidence. Persons, vehicles and public places can be searched in order to find stolen goods or ‘prohibited articles’ (stop and search power). In these cases, the constable needs to have a reasonable suspicion that such articles will be found.

These provisions well illustrate the abovementioned function of criminal procedure as a tool of opacity: they allow the police to enter the premises of an individual without a warrant, only if they are convinced that this will result in arresting the suspect of a crime or in securing evidence related to the crime for which the person is arrested. The police can also search public places or cars, or conduct searches of persons, but only if looking for specific stolen or prohibited items, and upon reasonable suspicion.

In other cases, conversely, the police need to request a justice of the peace to grant a warrant in order to search premises. Several conditions need to be met in order for this power to be lawfully exercised. For example, the offence for which the investigation is carried out needs to be indictable, the evidence sought needs to be ‘likely to be of substantial value to the investigation’ and not to ‘consist of or include items subject to legal privilege’ or other particular kinds of material.

The request for a warrant needs to be accompanied by a written notice containing specific information on the reasons for the request, and the applicant needs to answer potential questions from the magistrate.

Again, the link to an indictable criminal offence, a standard of proof and the exclusion of protected material, among others, are strict conditions without which a warrant will not be granted: they act as opacity tools. Additionally, transparency tools are here provided as well. The warrant application needs to be written and to spell out the legal justification for it; the applying constable can be further questioned by the justice of peace, and, finally, the justice of the peace herself exercises control by verifying that all legal requirements are met.

Another key surveillance power in criminal investigations is the interception of communications. Wiretap regulation in England was historically under-regulated until the 1980s. Since then, several statutory provisions were introduced. The latest of these provisions is the abovementioned IPA. Under IPA, the police can request a warrant for

---

59 PACE, ss 17(1), 17(2)(a) and 18(1); Spencer (n 54) 190; Cape and Hodgson (n 55) 67.
60 PACE, s 1(2)(a).
61 PACE, s 1(3); Darbyshire (n 52) 76.
62 PACE, ss 8(1)(a), (b) and (d); Spencer (n 54) 191; Feldman (n 56) 158-9.
63 PACE, ss 15(3), 15(2)(a) and 15(4); Feldman (n 56) 160.
64 See n 53.
the targeted interception of communications to the Secretary of State, which is a member of the executive, who ensures that it is requested for a legitimate purpose (including the broad concept of prevention or detection of serious crime) and that it is a necessary and proportionate measure with respect of such purpose. The Secretary of State must also be satisfied ‘that the method of naming or describing the subject-matter’ is in compliance with several requirements. Such requirements include, among other things: an indication of the statutory provisions related to the requested warrant, background information on the operation or investigation, names and descriptions of people or premises, and a description of the communications to be intercepted. Finally, IPA introduces the so-called ‘double lock’: after a first scrutiny from the Secretary of State, the warrant needs to be approved also by a Judicial Commissioner, who will review the necessity of the warrant and the proportionality of the measures described therein, applying ‘the same principles as would apply on an application for judicial review’.

In the case of IPA, opacity tools seem to be restricted to a minimum, as interception warrants can be requested for very general purposes. At the same time, transparency tools seem to provide for a more extensive control of the exercise of surveillance powers: the Secretary of State first, and the Judicial Commissioner at a later time, will review warrant requests, which need to include a detailed set of information on the purpose and context of the interceptions.

Although, for the purposes of this thesis, it is not the case to indulge in a discussion on the quality of the provisions of IPA, it is not possible to avoid mentioning the considerable legal debate that surrounds the evolution of investigatory powers in England. Indeed,

---

66 Home Office (n 65) para 5.17.
67 Home Office (n 65) para 5.29; IPA, s 31.
the whole history of most recent statutory interventions on this matter can be seen as the evolution of a conflict between two separate and contradictory trends: on the one hand, the necessity to comply with the standards set out by ECtHR case law; on the other hand, the attempt of the legislator to significantly expand investigative and other surveillance powers following post-9/11 anti-terrorism policies. Without discussing the quality or the legitimacy of the surveillance framework provided by IPA, or its desirability, for the purpose of this work it is important to remark that, in any case, its provisions confirm the fact that under European law principles, it is considered as a default that such powers should be regulated and that some form of oversight should be provided. Indeed, we can see this norm in the fact that while surveillance powers are expanded, at the expense of opacity tools, transparency tools are also increased, trying to counterbalance the augmented State reach.

2.3.2 Italy

In Italy, the written Constitution provides for the inviolability of personal liberty and of the home, as well as of the liberty and confidentiality of correspondence and of any other form of communication, and recognizes the rights contained in the ECHR as having the same status of the Constitution. The Constitution also provides for some principles of criminal procedure, while the main source of procedural requirements for the criminal investigation is provided by the Code of Criminal Procedure. During the investigative phase, the public prosecutor is in charge of the investigation. She can take actions to gather evidence, but she can also delegate these to the police, in particular the execution of searches and the interceptions of communications. The police are also authorised to act on their own initiative in a number of circumstances, generally those of urgency. Despite its role in the investigative phase, the public


71 Bert-Jaap Koops, ‘Criminal Investigation and Privacy in Italian Law’ (n 38) 6-7.


A prosecutor is considered to be an impartial body as it is part of the judiciary. Also, a ‘judge for preliminary investigations’ (giudice per le indagini preliminari) supervises fundamental rights protection in specific circumstances, such as during the interception of communication. Since the public prosecutor has an active role in gathering evidence against the suspect, in situations where particularly invasive powers are to be used (e.g., interception of communications), the authorisation of a judge that is not a party involved in the investigation guarantees a greater degree of impartiality.

Although part of the executive and organised under the Ministry of the Interior, in the context of criminal investigations the police act as ‘judiciary police’ (polizia giudiziaria), under the control of the public prosecutor who must be always kept informed of their investigative activities.

As regards searches, the police need a ‘motivated decree’ (decreto motivato) from the public prosecutor, supported by a written indication of the crime and its relation to the person or items object of the search. The standard of proof is ‘more than mere suspicion’ and there are notification requirements depending on the circumstances (e.g., for searches of persons, a copy of the authorising decree needs to be given to the interested individual, while for the search of places this needs to be given to the owner or tenant, if present). The police can also proceed to warrantless searches in specific circumstances, such as in flagrante delicto. They must nevertheless have well-grounded reasons to proceed without a warrant and need to provide a written record of the measures taken to the public prosecutor, who retroactively validates the search.

---

74 Tonini (n 72) 113, 115; Van Cleave (n 73) 305; Perrodet (n 72) 360.
75 Tonini (n 72) 34, 502; Giulio Illuminati and Michele Caianiello, ‘The investigative stage of the criminal process in Italy’ in Ed Cape and others (eds), Suspects in Europe. Procedural Rights at the Investigative Stage of the Criminal Process in the European Union (Intersentia 2007) 133; Perrodet (n 72) 361; Bert-Jaap Koops, ‘Criminal Investigation and Privacy in Italian Law’ (n 38) 5, 8.
77 Cpp, Arts 56, 59, 357; Tonini (n 72) 128-29; Illuminati and Caianiello (n 75) 133-34; Perrodet (n 72) 353, 409. For a discussion on the relationship among different police functions and different police forces in Italy, see Paolo Bonetti (n 76) 21ff.
78 Van Cleave (n 73) 314. See also Tonini (n 72) 387ff.
79 Cpp, Arts 249, 250; Tonini (n 72) 389-90; Van Cleave (n 73) 313-14.
80 In Italy there is also a number of special laws providing for more extensive police powers to conduct warrantless searches. Also in these cases, the police need to notify the public prosecutor for ex-post validation. Cpp, Art 352 comma 1. See Van Cleave (n 73) 316-17.
81 Cpp, Art 352 comma 4; Tonini (n 72) 390; Van Cleave (n 73) 315.
The interception of communications can be authorised only for a specific series of offences and the public prosecutor must request the approval of the judge for the preliminary investigations.\textsuperscript{82} The authorisation lasts fifteen days and it can be renewed for another fifteen days each time it is requested. In case of emergency, validation can also be given retroactively within three days from the start of the interceptions.\textsuperscript{83} The authorisation is based on ‘serious indications of a crime’ (gravi indizi di reato) and an assessment of the ‘absolute necessity’ of the measures for continuing the investigation.\textsuperscript{84} Without proceeding to an extensive discussion, as with the English jurisdiction, we can see that also in Italy the criminal procedure acts both as a tool of opacity, such as when setting standards of proof or allowing interceptions only in case of specific offences,\textsuperscript{85} and as a tool of transparency, such as when providing for notification obligations in the context of searches, or requiring the supervision of the investigative judge, in addition to that of the public prosecutor, when conducting wiretaps.

2.4 Enter preventative police surveillance

The police powers presented in the previous section are related to their role in the investigation of criminal offences. Even though such role is certainly a fundamental police task, it is not the only one they serve in modern states. In the current section, I will therefore present other forms of police surveillance, which are usually deployed outside the context of criminal investigations, and which I label as ‘preventative police surveillance’. I will then try to explain why the legal protection offered by criminal procedure is not suitable in these circumstances.

In the two jurisdictions analysed, the police are also vested with powers related to crime prevention and the maintenance of public order.

In Italy, along its function of judiciary police, the police force has also a function of ‘security police’ to maintain public order, exercised under the authority of public

\textsuperscript{82} Cpp. Arts 266 and 267 comma 1.

\textsuperscript{83} Cpp. Art 267 comma 2.

\textsuperscript{84} Cpp. Art 267 comma 1; Tonini (n 72) 399-400.

\textsuperscript{85} These offences are either particularly serious offences, such as those related to organised crimes, or less serious offences which are ‘particularly vile’ or consist in ‘activities for which interceptions are a particularly useful investigation tool’, such as stalking. Tonini (n 72) 399.
security which is conferred to the Ministry of the Interior, who coordinates the police forces. In this context, the police are therefore dependent on the executive.

In England, the different functions of the police are less clearly defined, as the exercise of police powers is historically related to the common law. And when different police powers and the organisation of police bodies are regulated by statutes, these acts do not provide for a clear justification of police functions. Nevertheless, an account of police roles can be derived from government papers and documents of police bodies:

[T]o uphold the law fairly and firmly; to prevent crime; to pursue and bring to justice those who break the law; to keep the Queen’s Peace; to protect, help, and reassure the community (...).

In the past, these functions would mainly entail the physical presence of police officers on the territory of the State and forms of mostly overt, manned, surveillance, in order to prevent and detect crime, or to ensure the public order and the maintenance of the peace. When technologies were used, these mostly enhanced existing human capabilities. For example, cars allowed officers to move faster, while binoculars allowed them to see further. In current times, though, the police are increasingly aided by more advanced technologies in the carrying out of their everyday activities. These enhance surveillance quantitatively and qualitatively, also going beyond human capabilities. For example, digital technologies allow the police to monitor more extensive areas, from a distance, to store information and retrieve it in a second moment, or to combine data from different sources.

86 This authority is defined as follows: ‘the authority of public security shall ensure the maintenance of the public order, the security of the citizens, their safety and the protection of private property; it shall ensure the observance of the laws and regulations of the State, both general and special (...).’ Regio Decreto 18 giugno 1931, n 773, in materia di ‘Approvazione del testo unico delle leggi di pubblica sicurezza’, Art 1. See Arturo Iannuzzi, ‘Il Diritto della Pubblica Sicurezza: Nozioni e Classificazioni Principali’ in Arturo Iannuzzi (ed), Compendio di Pubblica Sicurezza (DIKE Giuridica Editrice, 2018) 1-2, 4.
87 Paolo Bonetti (n 76) 10, 12-3. The two fundamental laws regulating the police force are the abovementioned R D 773/1931 and L 121/1981. On the distinction between these two functions of the police, see also Tonini (n 72) 127-8.
88 Although when it comes to security-related surveillance activities, the border between the concepts of public security and national security tends to blur, the scope of this thesis leaves out security and intelligence services and focuses on the police organisation. See Section 1.4.
91 The relationship between different kinds of technologies and different levels of intrusiveness emerges also in the case law concerning investigatory powers in several jurisdiction. See Bert-Jaap Koops, Bryce C Newell and Ivan Skorvánek, ‘Location Tracking by Police: The Regulation of ‘Tireless and Absolute Surveillance’ (2019) 9 UC Irvine Law Review 635, 677-79.
This has brought many authors to recognise the emergence of a ‘technology-led policing’—not always indicated with this expression. In this context, it is not always easy to concretely understand the real extent of the use of surveillance technologies, or the legal context in which they are used. Also, the effective employment of technologies by the police can be under-reported. This is for example the case with IMSI-catchers, the use of which is specifically regulated by criminal procedure in some countries, but which are also being allegedly used in an untargeted fashion by some police forces in order to track participants of protests or demonstrations. The problem with this technology is also related to scarce transparency as to their effective use, and by the fact that in certain circumstances such use is constitutively untargeted, as the device interacts ‘with those phones which come into its range generally, rather than being targeted at specific phones.’ Other technologies, such as Closed-circuit television (‘CCTV’) cameras, are more broadly and commonly used by police forces all over Europe. The most paradigmatic example of extensive employment of CCTV cameras is constituted by the UK. Firstly introduced during the late 1950s, CCTV cameras started being employed more often by UK police forces in the 1960s during public events and to control crime in business districts. But the installation of CCTV systems spiked during the 1990s, driven by Home

---

92 See n 40.
93 For example, a report published in 2013 on the implementation of the CoE Police Recommendation, which will be discussed in Chapter 3, found that among Contracting Parties, those countries that allow the police to process personal data not only where ‘necessary for the prevention of a real danger or the suppression of a specific criminal offence’, but also for broader security-related purposes, less than a half presented satisfying evidence on an appropriate legal framework sanctioning such wider police powers. Joseph A Cannataci and Mireille M Caruana, ‘Report: Recommendation R (87) 15 – Twenty–five years down the line’ (Research commissioned by the Council of Europe, 2013) 15 <https://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf> accessed 28 May 2019.
94 An IMSI is a unique identifier assigned to a user of a telecommunication network. IMSI-catchers, also called ‘stingrays’, are technological devices that ‘behave’ as a mobile network’s base station and can that be used for different purposes: to monitor the IMSI numbers emitted by nearby phones looking for a connection, to disrupt communications of one or more phones, or to intercept metadata or content of communications. See Paul F Scott, ‘Secrecy and surveillance: lessons from the law of IMSI catchers’ (2019) 33 International Review of Law, Computers & Technology 1, 3-6.
95 Koops, Newell and Škorvánek (n 91) 669ff.
97 Scott (n 94) 13.
Office funding, and it further increased after the 2005 London bombings. Despite their broad deployment, the use of CCTV cameras ‘is not always supported by specific national regulations’. The first statutory provision regulating the development of CCTV networks by local authorities was introduced only in 1994 by the Criminal Justice and Public Order Act. CCTV circuits are nowadays used jointly by local authorities and police forces for a broad set of security-related purposes, such as ‘detecting, reducing and deterring crime, disorder, anti-social and undesirable behaviour, and reducing the fear of crime.”

Similarly, in Italy, the use of CCTV cameras emerged thanks to a combination of local measures related to ‘urban security’ and the incentives provided by the government in order for local authorities to implement CCTV systems. Since the early 2000s, such authorities were given the power to issue ordinances related to public security and in the following years several legislative instruments were approved to coordinate central and local public safety policies. The last legislative intervention on this matter is provided by a law which promotes coordination agreements between local administrations and police headquarters, often including the sharing of CCTV live footage. CCTV cameras are then used by the police to monitor urban areas 24/7 and to store data for possible evidential use.

---


102 Eijkman and Weggemans (n 101) 146.

103 Criminal Justice and Public Order Act, s 163.

104 Webster (n 100) 232.

105 The Italian government allocated a total amount of 90 million euros for the period 2018-2020 for municipalities to set up or improve their video surveillance systems. Decreto Legge 4 ottobre 2018, n 113, in materia di ‘Disposizioni urgenti in materia di protezione internazionale e immigrazione, sicurezza pubblica, nonché misure per la funzionalità del Ministero dell'interno e l'organizzazione e il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata’, Art 35-quinquies.


107 Chiara Fonio, ‘The silent growth of video surveillance in Italy’ (2011) 16 Information Polity 379, 382; see also Cocq and Galli (n 7) 279ff.

Also, the police are more and more often equipped with body-worn cameras, the use of which also raises several legal questions. As with CCTV cameras, this kind of devices can be used for probatory reasons, but they can also livestream images to police control rooms and therefore be used as general monitoring tools for the purposes highlighted above.

Often, especially as regards visual surveillance technologies, information flows are then directed to control rooms, where the police are able to monitor public spaces on an ongoing basis.

2.5 Preventative police surveillance and privacy as non-domination

The use of the abovementioned, and possibly other, digital surveillance technologies in a preventative way – that is, not to gather evidence for crime investigation and prosecution, but to prevent crime and/or maintain public order or protect public security – has consequences for the legal protection of individuals. Namely, that the protection provided by the rules of criminal procedures described in the previous sections arguably does not apply. There is a problem related to the legal scope of such rules: if surveillance technologies are not used to investigate a specific crime and a specific suspect, those rules cannot apply to them. Rather, they can be considered as surveillance infrastructures, operating in the context of everyday police tasks, which can impact on the privacy of potentially any individuals within their reach, without the necessity of them being related to any crime or risk to public order.

In order to better frame the problem with preventative police surveillance and its consequences with respect to individuals’ privacy, I will refer to the neorepublican concept of non-domination.

---


110 In Italy TIM, the former national telco monopolist, provides all police control rooms with a video surveillance system that enables them to control several video sources: local CCTV networks, the CCTV circuits of the national railway network, footage from police helicopters and cars, and open source intelligence (OSINT) sources such as television. Francesco Biscuso, Cesare Macera and Gianfranco Marra, ‘Il sistema di comando e controllo di Sala Operativa della Polizia di Stato’ (Telecomitalia.com, 2017) <https://www.telecomitalia.com/content/itportaliit/notiziariotecnico/edizioni-2017/n-2-2017/capitolo-7/approfondimenti-2.html> accessed 30 April 2019.
In a series of papers, Andrew Roberts and Bryce Clayton Newell present an interpretation of the right to privacy through the lens of this theory. According to Roberts, the neorepublican conception of freedom as non-domination complements liberal theories on freedom that do not provide for a justification of the anxieties related not only to concrete invasions of the private sphere, but also to power relations that enable a potential invasion. The liberal conception of freedom is focused on the absence of interference and therefore frames the right to privacy mainly as a negative right, while for neorepublicans such a right can be affected without the need for a concrete interference to take place. Domination as conceptualised by neorepublicans is a condition in which an agent is subject to the control of another agent who is in a position of power to interfere with her autonomy: ‘if an agent or agency has the power to interfere arbitrarily in an individual’s choices, freedom is diminished even if the power is never exercised.’ From the neorepublican point of view, the effective exercise of power, but also the awareness of the agent, are therefore not decisive.

If I am unaware that I am being watched or that others have acquired information about me, the loss of privacy that I suffer is harmful to the extent that those who watch or collect the information acquire such power.

The concern is therefore not so much about the (concrete or potential) individual loss of privacy, but rather about the power imbalance that is created or reinforced. This is particularly so in the context of surveillance from State agents, since the ‘acquisition of personal information exposes individuals [to the risk] that governments will use it to retain domination and expand its power.’ In this context, ‘improper or inadequate democratic safeguards against abuse could potentially allow institutions to dominate and subjugate the people systemically.’

In order to restore citizens’ autonomy and a certain balance in the relationship between her and the powerful agent, neorepublicans refer to the notion of ‘antipower’ as an instrument that reduces domination by regulating the powerful agent. This can include, among other things, ‘checks on and separations of power (...), access to independent

113 Roberts (n 112) 325.
114 Roberts (n 112) 335.
115 Roberts (n 112) 336.
courts or other bodies with powers to review government action, and open access to information.  

Police surveillance, therefore, affects individuals’ right to privacy not only when the police intervene in individuals’ private sphere – such as when conducting a search in the context of criminal investigation – but also when it is deployed in a preventative way, as a general monitoring tool. In order to avoid the State dominating its citizens, there is therefore a particular need to resort to means of transparency and oversight, to provide for an antipower.

2.6 Conclusion

The police have nowadays several technological tools to conduct preventative surveillance outside of the context of criminal investigations. Even if the information gathered is not used and no concrete interference with citizens’ private sphere follows these surveillance activities, a neorepublican account of the right to privacy enables us to consider that the untargeted police gaze over citizens is in itself problematic as it increases government powers and exposes citizens to domination. Since the traditional opacity and transparency tools provided by criminal procedure do not apply in this context, there is a need to look for alternative means of protection outside of the criminal law domain. This is particularly important since in the case of this infrastructural kind of surveillance the normative choices regarding the definition of the possibility for the State to intrude in the private sphere of the individual have already been made. For example, by the enactment of legislation allowing for the police to monitor CCTV circuits to prevent crime and manage security-related risks.

Moreover, the introduction of new technologies, whether backed up by regulatory intervention or not, tends towards irreversibility: as technologies increasingly 'become institutionalised and ingrained in society, (...) it becomes pointless to ask whether we can do without them.'  

Both these trends, therefore, gradually undermine the relevance of opacity tools. For this reason, the focus should be on establishing transparency tools to control police surveillance powers.

---

117 Newell (n 116) 425.
118 Koops, ‘Technology and the Crime society’ (n 5) 123. See also Murakami Wood and others (n 2) paras 9.12.1-9.12.2.
3. The European data protection regime and its applicability to preventative police surveillance

3.1 Introduction

The theoretical framework presented in the previous chapter clarified the importance, in the context of preventative police surveillance, of shifting the focus of considerations related to privacy protection from individual infringement cases to power relations. When police surveillance does not target a specific individual but becomes infrastructural, information collection enables the police to potentially interfere in individuals’ private lives. According to a neorepublican account of the right to privacy, this means that the police is in a position of domination towards the citizenry. Thus, there is a need for legal tools that can act as an antipower, to ensure the lawful exercise of such surveillance powers and hence preserve the balance between State powers and individuals’ private sphere. It is interesting to note that such concept, that of antipower, as it emerges from the literature analysed in the previous chapter, seems quite similar to the concept of ‘tools of transparency’, also presented therein. Antipower seems to foresee different means to ensure that someone ‘watches over the watchmen’: examples include citizens’ access to information on government activities, separation of powers and external oversight of government actions. In a similar way, transparency tools themselves constitute ‘legal means of control’ of government powers, providing – among other things – oversight of government action from ‘controlling bodies’ or other State powers.

De Hert and Gutwirth present data protection as a tool of transparency, highlighting its role in protecting citizens’ privacy (and other fundamental rights) and in guaranteeing accountability by ensuring that the processing of personal data is subject to procedural safeguards. To be sure, up to a certain extent, data protection can also constitute a tool of opacity (e.g., as regards the general prohibition for automated individual decision-making or the restrictions applied to the processing of sensitive data), but even when there are rules that prohibit certain types of data processing as a default, they are usually counterbalanced by envisaged exceptions and the focus is usually on the presence of adequate safeguards.

---

119 In fact, transparency tools ‘put counter powers into place.’ De Hert and Gutwirth (n 15) 10. See Section 2.3.
120 See Section 2.5; Newell (n 116) 425.
121 De Hert and Gutwirth (n 15) 9.
122 De Hert and Gutwirth (n 15) 15-16.
123 De Hert and Gutwirth (n 15) 16-18.
normative choices on the opportunity of allowing the use of certain personal information have already been made (for example by a law authorising the police to use certain surveillance technologies) and provides for the means to control such processing activities in order to avoid abuse of power and fundamental rights infringements. For this characteristic, data protection constitutes, according to the authors, ‘a general framework for all kinds of surveillance.’ It (mostly) leaves out normative questions on the opportunity of intruding the private sphere of the individual and asks the simpler question if personal data are being processed. For this reason, it seems pertinent to turn to data protection as a mean of legal protection in the context of preventative police surveillance. Moreover, as emerged from the previous chapter, it is not always easy to understand what is the regime regulating the preventative use of technology by the police. For this reason, being able to apply data protection as a one-size-fits-all instrument for all surveillance technologies used by the police would be particularly useful. Even in situations where it is not clear which legislation authorizes the police to deploy a certain technology and which rules (if any) apply to its use, data protection legislation would still provide for a general set of procedural safeguards to protect citizens’ private sphere. And indeed, all the surveillance technologies described earlier in this work involve the processing of personal data. CCTV and body-worn cameras process, among other things, pictures of individuals’ faces, while IMSI-catchers process unique identifiers of devices that are directly linked to mobile telecom services’ subscribers. The same can be said also for other kinds of surveillance technologies. In all these cases the data processed relate to identified or identifiable individuals.

In this and the following chapter I will therefore consider the data protection regime applicable to preventative police surveillance in the European context, in order to answer the second research question of this thesis:

2. How does the European data protection regime, including but not limited to the EU Law Enforcement Directive, protect individuals in the context of preventative police surveillance?

---

125 See Section 2.4.
126 See Law Enforcement Directive, Art 3(1); Convention 108+, Art 2(a).
In order to answer this research question, two sub-questions will be addressed, one for each chapter:

2.1 Is the European data protection regime applicable to preventative police surveillance?

2.2 What are the most important safeguards provided therein?

This chapter will therefore present the evolution of both CoE and EU data protection legislation, it will discuss its scope, and clarify if it is applicable to the processing of personal data by the police in the context of preventative surveillance. Chapter 4 will analyse the main safeguards provided by European data protection law.

3.2 CoE data protection law

3.2.1 Convention 108+

The 1981 CoE Convention for the protection of individuals with regard to the processing of personal data – recently modernised by an additional protocol which brings it in line with the reform of the data protection framework at the EU level\(^\text{127}\) – was the first binding legal instrument regulating the processing of personal data ever implemented at the European level. Compared to subsequent EU instruments, its scope is broad, and it applies to all kinds of data processing from both private and public institutions, with the exception of household activities.\(^\text{128}\)

However, in the contexts of law enforcement, national security and defence, several exceptions apply to the general principles provided therein.\(^\text{129}\) Unfortunately, the Convention itself does not define the terms which identify the scope of these exceptions. The Explanatory Memorandum of Convention 108+ does provide for a definition of national security as ‘the protection of state security and constitutional democracy from, inter alia, espionage, terrorism, support for terrorism and separatism’,\(^\text{130}\) but there is no definition of the other terms. These include ‘public order’, which is mentioned only once along with national security,\(^\text{131}\) and ‘public safety’, mentioned four times, considering both Convention 108+ and its Explanatory Memorandum, half of them along with national security.

---

\(^{127}\) See n 22.

\(^{128}\) Convention 108+, Art 3.

\(^{129}\) Paul de Hert and Juraj Sajfert, ‘Police, privacy and data protection from a comparative legal Perspective’ in Monica den Boer (ed), *Comparative Policing from a Legal Perspective* (Edward Elgar Publishing 2018) 308.


\(^{131}\) Convention 108+, Art 20(c).
The fact that the distinction within these concepts is not clear means that it might be difficult to understand which exceptions are allowed for what kind of processing activities. At the same time, the most important exceptions are foreseen by Article 11 of the Convention, which reads that an exception is allowed only when it is ‘provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for (...) the protection of’, among other things, national security, public safety, and the prevention of crime. For this reason, the possible overlap between these different areas might not affect in a decisive way the application of exceptions to data protection law – i.e., whether a data processing will be regulated under national security or crime prevention provisions, such provisions will allow in any case to apply the exceptions provided for by Article 11.

In conclusion, it seems safe to assume that Convention 108+ applies, as a default, to all kinds of police data processing, including those related to preventative surveillance, while these may be exempted from the application of several data protection provisions.

3.2.2 The Police Recommendation

For a long time, Convention 108 has been the only legal instrument regulating processing of personal data in the police sector, but it mainly provided for basic data protection principles (namely: fairness, lawfulness, purpose limitation, storage limitation, data quality and proportionality) and basic data subject rights (access and rectification), leaving a broad discretion to Contracting Parties concerning practical means of implementation.

In 1987, the CoE adopted a Recommendation ‘Regulating the use of personal data in the police sector’ (‘Police Recommendation’) in order to assist the Contracting Parties in implementing Convention 108 in such field. The explanatory memorandum of the

132 On the definition of national security and the distinction between this notion and the other abovementioned concepts, see Ian Cameron, National Security and the European Convention on Human Rights (Kluwer Law International 2000) 54ff.

133 In such circumstances, several data protection principles (eg, transparency, purpose specification and accuracy) can be disapplied, data controllers can be exempted from data breach notifications, and all data subjects’ rights can be curtailed. Convention 108+, Art 11(1), read in conjunction with Arts 5(4), 7(2) and 9.

134 Convention 108+, Art 11(1).

135 I refer here simply to Convention 108 since the Police Recommendation was adopted before the modernisation process.

136 Diana Alonso Blas, ‘First Pillar and Third Pillar: Need for a Common Approach on Data Protection?’ in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer 2009) 227; De Hert and Sajfert (n 129) 308.

137 Council of Europe, ‘Recommendation on the use of personal data in the police sector’ (R (87) 15, adopted by the Committee of Ministers on 17 September 1987).
Police Recommendation stresses the importance, particularly in this area, of striking the right balance between, on the one hand, public interests related to combating crime and maintaining public order, and, on the other hand, the privacy of individuals – ‘for it is in this domain that the consequences of a violation of the basic principles laid down in the Convention could weigh most heavily on the individual.’

The Police Recommendation covers ‘all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order’.

De Hert, Papakonstantinou and Riehle consider that the approach of the Police Recommendation is inherently in tension with current trends of police data processing practices as it seems focused on ‘reactive and prudent policing, whereas today’s police models are based on more proactive concepts.’ As an example, these authors present the fact that the Police Recommendation allows data collection for police purposes only ‘for the prevention of a real danger’. At the same time, the Explanatory Memorandum clarifies that national legislation can authorise ‘wider police powers to gather information’ and that the notion of real danger has to be interpreted extensively ‘as not being restricted to a specific offence or offender’.

On the one hand, some of the principles contained in the Police Recommendation can be considered ‘burdensome’ for the police and restrictive for their surveillance activities. Apart from the abovementioned example, this can be seen in the ‘control and notification’ principle, where it is recommended that the police should consult with the supervisory authority ‘in any case where the introduction of automatic processing methods raises questions about the application of this recommendation’, in provisions concerning

---

138 Council of Europe, ‘Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector’ (‘Explanatory Memorandum’) para 14. According to De Hert, Papakonstantinou and Riehle ‘all police data on persons can be considered sensitive, whether its use violates privacy or not.’

139 Police Recommendation (n 137), p 2 (emphasis added).

140 De Hert, Papakonstantinou and Riehle (n 138) 126-7.

141 Police Recommendation (n 137) Principle 2.1.

142 Explanatory Memorandum (n 138) para 43.

143 Police Recommendation (n 137) Principle 1.3.
information duties and accuracy of data,\textsuperscript{144} or in the way the Police Recommendation deals with the exchange of information between police forces or other public bodies.\textsuperscript{145} On the other hand, the clarifications provided in the Explanatory Memorandum often seem to go in the opposite direction, being more permissive in terms of collection and use of data. This can be seen, for example, where it clarifies that the recommendation to consult the supervisory authority do not allow the latter to block any data processing activities,\textsuperscript{146} where it states that, in cases of ‘street videos and similar mass surveillance methods’ the police itself can determine the practicability of communicating to the data subject the existence of personal data related to her,\textsuperscript{147} or where it acknowledges that ‘it may not always be feasible to ensure a strict separation between’ data processed for police purposes and data processed for administrative purposes.\textsuperscript{148}

It is interesting to note these opposite trends since they well reflect the inherent tension between the consolidation of data protection law and the expansion of police powers in the last decades. As with the exceptions provided in Convention 108+, a strict or loose transposition of the principles of the Police Recommendation will have implications for the safeguards applied to police surveillance.

Nevertheless, this does not affect the scope of this legal instrument, which, as noted, not only applies to the ‘suppression of criminal activities’, but also to their prevention and to the ‘maintenance of public order’,\textsuperscript{149} which, even in the absence of clear definitions, seem to be legal concepts providing for the justification of preventative forms of police surveillance, as discussed in the previous chapter. Moreover, the Explanatory Memorandum clearly acknowledges the distinction between the reactive and preventive functions of policing, and it requires to lay down distinct rules regulating data processing in these two different contexts.\textsuperscript{150}

According to the analysis provided above, it seems therefore quite safe to assume that also forms of preventative police surveillance are integrated in the scope of CoE data protection law.

\textsuperscript{144} Police Recommendation (n 137) Principles 2.2 and 3.1.
\textsuperscript{145} Police Recommendation (n 137) Principle 5.
\textsuperscript{146} Explanatory Memorandum (n 138) para 35.
\textsuperscript{147} Explanatory Memorandum (n 138) para 44.
\textsuperscript{148} Explanatory Memorandum (n 138) para 54.
\textsuperscript{149} See n 139.
\textsuperscript{150} Explanatory Memorandum (n 138) para 22. Unfortunately, the CoE does not go further in explaining in more details how these principles should be adapted to each context.
3.3 EU Data protection law

3.3.1 Before the Law Enforcement Directive

In the European Union the rationale of the first data protection legislation was related to internal market considerations and therefore the Data Protection Directive, adopted in 1995, did not apply to the former Third Pillar and to ‘processing operations concerning to public security, defence, State security (…) and the activities of the State in areas of criminal law.’

At a later stage, in 2008, the EU adopted new rules under the police cooperation provisions of the Treaty on European Union in order to regulate data processing in the police context. However, these rules were only applicable to the exchange of information between the police forces of Member States (‘MSs’) and not to domestic processing.

Nevertheless, even before the adoption of the Law Enforcement Directive, the principles of European data protection law were already applied to domestic data processing for police purposes in some countries. This is mainly due to the fact that several MSs, implementing the DPD, applied its standards also to the police sector, but also due to the adoption of CoE’s Police Recommendation.

After the Lisbon Treaty, the right to data protection has been fully integrated in the EU legal system as a fundamental right and it has been set as the legal basis for EU data

---


152 Following the Maastricht Treaty, the European Union was structured on three ‘pillars’: the European Communities, the Common Foreign and Security Policy, and the Police and Judicial Cooperation in Criminal Matters. The pillar structure has been abolished with the entry into force of the Treaty of Lisbon. See Klaus-Dieter Borchardt, The ABC of EU law (Publications Office of the European Union 2017)16ff.

153 Data Protection Directive, Art 3(2).

154 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/61. Domestic processing was actually part of the original scope also of the Framework Decision, but it was abandoned during the negotiations. See De Hert and Papakonstantinou, ‘The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters’ (n 138) 407.


156 See Blas (n 136) fn 19 at 231-32; De Hert, Papakonstantinou and Riehle (n 138) 133. See also CPDP Conferences, ‘CPDP 2019: law enforcement and data subjects’ rights’ (31 February 2019) 30:42-32:24 comments by Vagelis Papakonstantinou <https://www.youtube.com/watch?v=b8ab7oU4ZC0> accessed 23 July 2019. On the standard-setting role of the DPD in the area of the former Third Pillar see also De Hert and Papakonstantinou, ‘The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters’ (n 138) 405.

157 Cannataci and Caruana (n 93) 1, 52. From the report authored by Cannataci and Caurana it is possible to draw a general picture of the national legislations in this area before the introduction of the LED.

protection legislation.\textsuperscript{159} In fact, Article 16 TFEU confer to the EU a broad mandate do regulate ‘all processing activities taking place within the scope of EU law’.\textsuperscript{160} The new legal framework emerged from the reform process started in 2012\textsuperscript{161} includes two main legal texts applicable to MSs. The first is a regulation, the GDPR,\textsuperscript{162} which is applicable to data processed for commercial and administrative purposes. The second, the Law Enforcement Directive, is applicable to data processed for law enforcement purposes.

3.3.2 The Law Enforcement Directive

As already mentioned, in 2016 EU countries already had, at least to some extent, national legislation applicable to police data processing which followed European data protection standards. Nevertheless, the legislation in this field was far from being harmonised, and the LED is therefore considered to be a desirable step in this direction.\textsuperscript{163} Concerning its scope, according to Articles 1 and 2, the LED applies to the processing of personal data for purposes related to 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’\textsuperscript{164} (material scope), carried out by authorities that are competent to perform these tasks (personal scope).\textsuperscript{165} As with previously mentioned CoE instruments, the broad scope of the LED seems to accommodate the need for regulating preventative police surveillance. If there is personal data processed by the police, which is one of the ‘competent authorities’, as defined in Article 3 indent 7 of the LED, and this data is processed for one of the law enforcement purposes mentioned above, and not any other (e.g., for administrative purposes), the LED

\textsuperscript{159} Article 16 of the Treaty on the Functioning of the European Union, which constitutes the new legal basis for the EU data protection regime, actually includes the right to data protection and the free flow of information. Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ 326/47 (TFEU).

\textsuperscript{160} Hielke Hijmans, The European Union as Guardian of Internet Privacy (Springer 2016) 265.


\textsuperscript{164} Law Enforcement Directive, Art 1(1) (emphasis added); see also Law Enforcement Directive, Recital 12.

\textsuperscript{165} Law Enforcement Directive, Arts 2(1) and 3(7).
As previously mentioned, the law enforcement purposes include not only the investigation of crimes, but also their prevention and detection, and activities related to the safeguarding of public security. Recital 12 of the LED further clarifies these concepts as including ‘police activities without prior knowledge if an incident is a criminal offence or not’, which may include activities ‘at demonstrations, major sporting events and riots’ and the task to maintain law and order ‘where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society.’ It seems therefore logical to infer that the data processing related to those activities that I label as preventative police surveillance in this thesis (mainly the use of CCTV cameras and other visual surveillance tools, but including also other forms of untargeted and preventive surveillance outside the scope of a criminal investigation) will fall within this broad category.

Nevertheless, the introduction of the notion of public security could present some issues. Firstly, the distinction might not be so clear between this concept and that of national security, which is outside the scope of EU law and explicitly excluded from the scope of application of the LED. Secondly, as Sajfert and Quintel argue, its introduction expands the scope of the LED ‘from the core criminal law enforcement realm’ to preventative contexts. According to these authors, this may lead to ‘an overly broad interpretation of the scope of the LED at the expense of the GDPR.’ Although, under the current data protection regime it seems disputable whether the GDPR would apply to the data processing activities that I described in the first chapter under the umbrella term of preventative police surveillance.

It seems to me that it was actually a clear, although possibly objectionable, choice of the legislator – using terms such as ‘prevention’, ‘detection’ and ‘public security’ – to include data processing for purposes not related with a specific criminal offence in the scope of

---

166 Mireille M Caruana, ‘The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement’ (2017) 33 International Review of Law, Computers & Technology 249, 253. Although, it is important to note that the distinction between security-related and administrative tasks might create some implementation issues: according to the author ‘Member States define the activities of their authorities, in relation to law enforcement or merely administrative purposes, differently’ and ‘the same data processing operation could be covered by the GDPR in one Member State’ and by the LED in another.


170 Sajfert and Quintel (n 168) 22.
the LED. This choice seems even more clear since Article 2(2)(d) of the GDPR, using exactly the same language as Article 1(1) of the LED, expressly exclude ‘law enforcement purposes’ from the scope of the GDPR. For these reasons, more than with an ‘overly broad interpretation’, it seems to me that the problem could be that a broad and not clearly defined set of terms might create uncertainty concerning which data processing they are applicable to.

Moreover, even if the term ‘public security’ had been hypothetically excluded from the LED, I believe that this domain might still fall outside the scope of EU law, and therefore not within that of GDPR. While some authors consider the broad legal basis provided by Article 16 TFUE as covering the whole domain of data protection, also at MSs’ level, irrespective of EU competences, I believe that Article 4(2) of the Treaty on European Union still limits the possibility for the EU to fully regulate areas that are closely related to public order and security. Until the European Data Protection Board (‘EDPB’) or the Court of Justice will have provided their interpretation of these concepts, the scope of the LED will be ultimately determined by the interpretation given to them by MSs.

3.4 Security-related concepts in European law: in need for definitions

As seen in the previous sections of this chapter, the scope of the European data protection instruments applicable to the police sector seems to be broad enough to be applicable to those surveillance activities that are not part of criminal investigations, but which are part of preventative strategies to control crime and risks related to public security. It seems

---

171 According to Hijmans ‘all processing by Member States falls by definition within the scope of EU law’. Hijmans (160) 267, 268.
172 To clearly define the scope of EU law in the context of data protection is a very complex issue which is out of the scope of this thesis. Nevertheless, in the following section I will attempt a more extensive discussion of security-related concepts in European law. On this issue, see also Plixavra Vogiatzoglou and Stefano Fantin, ‘National and public security within and beyond the Police Directive’ in Anton Vedder and others (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security (Intersentia 2019).
173 Law Enforcement Directive, Art 51(1)(b). The EDPB is an independent body established by the GDPR. Its members are MSs’ DPAs and the European Data Protection Supervisor, and it ‘contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU’s data protection authorities’. EDPB, ‘About EDPB’ (EDPB) <https://edpb.europa.eu/about-edpb/about-edpb_en> accessed 18 October 2019.
particularly safe to draw this conclusion in the context of Convention 108+, which applies as a default to all State activities.

At the same time, the fact that the legal texts analysed do not provide with a consistent language but use apparently interchangeably the terms of public security, public order, and public safety makes it difficult to understand the exact boundaries of the scope of the exemptions provided by Convention 108+ and of the applicability of the Police Recommendation and the LED.175 This is particularly problematic because of the confusion there could be with the notion of national security, which is still in the scope of Convention 108+, but not of the other instruments.

Unfortunately, the lack of definitions of these terms and the consequent unpredictability as to their scope involves the whole spectrum of European fundamental rights legislation. Indeed, some of these terms appear in the ECHR as well. They are among the legitimate interests that can justify an interference with certain fundamental rights. Thus, public safety appears in Article 8(2) of the ECHR, along with the concepts of national security and of the ‘prevention of disorder’, which, paraphrased, might constitute the same concept of ‘maintenance of public order’ mentioned in the Police Recommendation,176 which is in turn mentioned in Article 9(2), again along with public safety. Article 10(2) and 11(2) present the same concepts of Article 8(2) (national security, public safety and prevention of disorder). The concepts of public order and national security reappear also in Article 6 as legitimate interests to restrict the public pronunciation of judgments, and in Article 1(2) of Protocol 7 to the ECHR as legitimate interests to expel aliens. Finally, Article 2(3) of Protocol 4 presents national security and public safety as legitimate interests to restrict freedom of movement, along with the concept of ‘maintenance of ordre public’. It is interesting to note the use of the French term in the English legal text as it exemplifies a complex issue of interpretation of this concept, which, depending on the jurisdiction, can refer to fundamental values of the State such as the rule of law and the democratic constitutional order, to the concept of public policy, to the ‘general or common welfare’, or to ‘public security and an orderly way of life in the public sphere’.177


176 See above p 34.

177 Roel de Lange, ‘The European Public Order, Constitutional Principles and Fundamental Rights’ (2007) 1 Erasmus Law Review 3, 7-10. Additionally, the author asserts that ‘in EC law the concept of ordre public is sometimes used to denote the status of some fundamental provisions in the EC Treaty’. On the problematic distinction between ordre public, public order and public policy in ECHR law, see Svensson-McCarty (n 175) 187.
Unfortunately, the case law of the European Court of Human Rights does not help in defining these concepts and their boundaries. From an initial analysis of some case law, it seems that the Court does not provide for a definition of any of them. The cases where they appear are related to different issues, from the publications of leaflets criticizing government policies, to poems possibly inciting to riots, and cases related to the use of religious headdresses in public spaces. In these cases, some of these terms are often presented in combination, without clarifying if a certain restriction of fundamental rights pertained to one sphere or another (such as public order or national security).

The case law of the Court of Justice of the European Union does not provide for further clarifications either. Interestingly, as reported in the Digital Rights Ireland case, the Data Retention Directive annulled by the same judgement considered public order as an overarching concept subsuming that of national security, public security, and ‘the prevention, investigation, detection and prosecution of criminal offences’.

### 3.5 Conclusion

While these considerations are important to acknowledge the problems MSs and Contracting Parties may face when applying data protection instruments, and in particular their exemptions, to specific data processing activities, this does not affect the positive answer to be given to the relevant research sub-question of this thesis: the European data protection regime can, as a default, apply to preventative police surveillance. If not for other reasons, because the inclusion of concepts such as crime prevention, public order and public security in the scope of the legal texts analysed would otherwise not be explicable. If the legislator had not intended to include them in the scope of data protection legislation, it could have simply referred to crime investigation.

At the same time, the distinction between these security-related concepts and that of national security might be problematic for two main reasons. Firstly, as this concept delimits the scope of application of the Police Recommendation and the LED, European

---

178 In order to assess this, I carried out a research in the online database of the ECtHR (https://hudoc.echr.coe.int) using as key words ‘public order’, ‘public safety’, ‘public security’ and ‘national security’, and further refining the results with relevant filters.

179 In this case, the research was made in the online database of the CJEU (http://curia.europa.eu/juris/recherche.jsf?cid=3709896) using the same key words and further refining the results in order to include only relevant judgments.


states might try to expand the concept of national security to exclude some forms of preventative police surveillance from the scope of application of these legal texts. Secondly, some surveillance technologies, such as CCTV circuits, might be used by the police both for different purposes and by different actors simultaneously, thus making it problematic to apply different data protection standards to the same data processing.\textsuperscript{182} In the case of Convention 108+, as previously noted, this issue seems to be less problematic, as the most important exceptions are provided for all security-related purposes, including national security.

4. Checks and balances for preventative police surveillance: the safeguards provided in data protection law

4.1 Introduction

After having provisionally established in the preceding chapter that European data protection law can be applied to preventative police surveillance, it is now possible to consider how this legal framework can provide for individuals’ legal protection in this context. In other words, I will be looking for those safeguards that can contribute to the creation of an antipower, in the neorepublican sense of the term, in order to answer to the relevant sub-question:

2.2 What are the most important safeguards provided [in European data protection law]? 

Before analysing the law, I will spend a few more words on the concept of antipower and on that of transparency, for two main reasons. One is to justify the choice in the selection of the safeguards that will be analysed, and the other is to further clarify the relationship between antipower and transparency.

4.2 Antipower in the surveillance context

A great part of the neorepublican discourse around power, freedom and democracy is concerned with the problem of making sure that the State does not exercise what neorepublicans call a ‘subjugating power’ over its citizenry. That is, a power that does not allow people to be free. Neorepublicans are aware that State agents, and in particular those in the executive branch of the government, are likely to exercise domination over their citizens if left with unchecked powers. For this reason, they look for constitutional mechanisms to keep the power balance between the State and those who are being governed.183 State agents are therefore to be controlled, so that they do not use the discretion they have in exercising their powers in a ‘constitutionally indefensible way to worsen the situation of the person they affect.’184 This is what antipower is about:

---

184 Pettit, ‘Freedom as Antipower’ (n 183) 586.
providing for mechanisms of control, so that the power given to the State remains within the legitimacy of the rule of law. 185

Unfortunately, though, neorepublicans only sketch the contours of this concept, without providing for specific guidance on how to construe institutions as antipowers. Philip Pettit explains that ‘antipower relates to subjugating power in the way that antimatter relates to ordinary matter: it represents something repellent to subjugating power, as antimatter represents something repellent to ordinary matter.’ 186 More concretely, he refers to dominating agents ‘[making] themselves answerable in the court’ and ‘being exposed to the possibility of effective rebuke’ as ways of ensuring the freedom of citizens. 187 He also considers that mechanisms of control may include, among other things, ‘separation of powers, availability of appeal and review, provision of information, and the like.’ 188

In a 1990 book on criminal justice, Braithwaite and Pettit, even though they do not mention the concept of antipower yet, briefly consider power constraints in the context of police surveillance. 189 They generally refer to ‘mechanisms of appeal or complaint’ and accountability as systems to check the powers of criminal justice institutions. When turning their attention to what they call ‘the brave new world of surveillance’, they acknowledge the ‘need for [a] countervailing power in the form of human rights commissions or similar bodies’. 190

In his later work on democratic theory, Pettit further refers to ‘expert or impartial or judicial bodies’, and more generally to ‘unelected authorities’ as useful instruments to control government’s powers. 191

Finally, Hoye and Monaghan, while applying neorepublican ideas to the context of mass surveillance, consider that ‘the particularity of the surveillance threat requires an antipower’, ‘an empowered institution that serves to actively counter-surveil the

185 According to Pettit, the rule of law entails a ‘separation and sharing of powers’ which ‘deny control over the law to any one individual or body’, so that the State can ‘protect against private forms of domination without perpetrating public forms.’ Pettit, On the People’s Terms (n 183) 5-6.
186 Pettit, ‘Freedom as Antipower’ (n 183) 589.
187 Pettit, ‘Freedom as Antipower’ (n 183) 586.
188 Pettit, ‘Freedom as Antipower’ (n 183) 589-91.
190 Braithwaite and Pettit (n 189) 88, 110.
191 Pettit, On the People’s Terms (n 183) 175, 239. According to the author such kind of institutions can, in certain situations, support elected assemblies in keeping the government at check, in particular when it is advisable to avoid ‘distorting effects of electoral pressures and private lobbies.’ At the same time, he also warns against risks that the establishment of these institutions can cause and recommends some safeguards to ensure that also their power does not constitute a form of domination.
surveilling powers’ using ‘technological sophistication beyond the reach of average citizens’, and that is able to inform the general public.\textsuperscript{192}

Ultimately, neorepublicans provide a general idea on how to protect the citizen from excessive State reach. However, they do not provide for concrete examples on how to design antipower in different contexts, such as those we are looking for in the realm of preventative police surveillance. Nevertheless, there are some elements that emerge from the abovementioned literature, that I will use in order to orientate my discussion on the safeguards provided in European data protection law and that are suitable to counterbalance police surveillance powers. Firstly, neorepublicans state the need for State agents to be answerable for their actions and to be exposed to ‘effective rebuke’; for this reason, I will analyse those provisions, in European data protection law, that provide for police accountability. And since accountability requires an agent to be accountable to another agent, the second kind of safeguards I will focus on is oversight, following neorepublican calls for separate independent bodies (e.g., courts, ‘expert or judicial bodies’, human rights commissions) to review the State’s exercise of power. Such bodies should also provide the public with relevant information and allow them to submit complaints. Hence, I will take due consideration of those data protection provisions that establish transparency requirements allowing individuals to be aware of the processing of their data from police forces.

These three elements – transparency, accountability and oversight – are clearly closely connected and mutually dependent. Without having knowledge of State practices, it is not possible for individuals to challenge them, and without the guarantee of having State action checked by an independent body, it is not possible to hold State agents accountable for their exercise of power and possibly receive redress.

Referring again to De Hert’s and Gutwirth’s work, the rule of law entails exactly these elements: government actions must be transparent in order to enable independent review (oversight) and thus ultimately accountability of the government for its actions.\textsuperscript{193} The connections between these concepts can be better understood through the lens of David Heald’s anatomy of transparency.


\textsuperscript{193} De Hert and Gutwirth (n 15) 5-6.
4.3 Heald’s anatomy of transparency and its relevance for data protection law

In order to tentatively establish the contours of an antipower to act in the context of preventative police surveillance, I will introduce the doctrinal construction on transparency from David Heald. This theoretical framework will hopefully allow me to build upon neorepublicans’ theory and sketch a picture of how data protection safeguards can be seen as an antipower.

In his seminal work, Heald construes the concept of transparency on two different dimensions: vertical and horizontal. Concerning the former, he distinguishes between a ‘transparency upwards’, related to those situations when those who are in a higher hierarchical position can observe the behaviour of those who are in a subordinate condition, and a ‘transparency downwards’, which occurs when the reverse happens: that is – taking as an example the context of individuals-government relationships – when the people can observe the conduct of State officials. Transparency downwards pertains, according to Heald, to the wider concept of ‘accountability’.194

As regards the horizontal dimension, the author differentiates between a ‘transparency outwards’, which entails – continuing the reference to individuals-government relations – members of a State agency being able to observe the conduct of individuals outside the agency, and a ‘transparency inwards’, when ‘outsiders’ can observe the conduct of those inside the agency. Transparency inwards relates, among other things, to peer surveillance and freedom of information legislation.195

In devising an antipower for police surveillance, it will be important to put safeguards in place in order to increase transparency inwards and downwards, as this would allow individuals and oversight bodies alike to be aware of how the police exercise its surveillance powers, and ultimately to hold them accountable.

Translating this discussion into the field of data protection law, it is possible to see these directions of transparency, for example, in data subjects’ rights and supervisory

194 David Heald, ‘Varieties of transparency’ in Christopher Hood and David Heald (eds) Transparency: The Key to Better Governance? (Proceedings of the British Academy 135, Oxford University Press 2006) 27. Applying Heald’s anatomy of transparency to police surveillance allows to make interesting considerations regarding the fact that transparency provisions constitute a form of counter-surveillance which enable the citizens, in a broad sense, to watch over the police. Going back to the concept of antipower, this seems particularly fitting to the idea of maintaining the power balance between the government and its citizens: if the former has more surveillance powers, in order for the latter not to be object of subjugating power (entailing domination), it is needed to expose also the government to surveillance. Unfortunately, there is not enough room in this work to carry out an extensive analysis of this double face of surveillance.

195 Heald (n 194) 28.
authorities’ investigative powers. On the one hand, information and access rights allow individuals to be aware, generally, of police surveillance activities and, specifically, of data processing related to them. This increases transparency both inwards – looking into police practices – and downwards – from individuals towards State agencies. On the other hand, Data Protection Authorities (‘DPAs’) have investigative powers that allow them to look into how police carries out surveillance. Ultimately, both these types of safeguards increase the accountability of the police force.

On top of this bi-dimensional characterisation, according to Heald, transparency can also be analysed through three dichotomies. Firstly, the author distinguishes between event and process transparency. The former refers to the transparency of single data points that are ‘externally visible and – at least in principle – measurable’, while the latter is related to (on-going) processes and is considered to be more difficult to obtain due to their usual opacity.196 Concerning process transparency, Heald further distinguishes between ‘procedural’ transparency, related to the knowability of the rules governing the processes of an organization, and ‘operational’ transparency, which refers to the application of these rules to specific cases.197

While devising legal safeguards for police surveillance, these aspects are important in different situations. Event transparency is needed to assess the compliance of single actions with applicable rules, for example the legality of a police officer accessing a database. Process transparency, though, is even more critical, as it allows to look past specific cases of abuse and more into institutional policies. For this reason, provisions enabling procedural and operational transparency will both be crucial. In data protection law, this could be translated into provisions such as Data Protection Impact Assessments (‘DPIAs’) and prior consultation obligations, which might allow DPAs to shed some light on the organisational policies and decision-making of the police.

The second dichotomy involves the concepts of ‘transparency in retrospect’, which allows for ex-post accountability, and ‘transparency in real time’, when ‘the accountability window is always open and surveillance is continuous.’198 Even though transparency in real time would be ideal, in order to be sure that the police never abuses surveillance powers, this would of course not be physically possible, because of the limited resources of Data Protection Authorities, and probably also not desirable, as it might affect the independence of the police to fulfil its own tasks. But even if, generally,

196 Heald (n 194) 30.
197 Heald (n 194) 31-32.
198 Heald (n 194) 32-33.
checks will be carried out ex-post, in some instances it could still be possible to create some sort of real-time transparency windows, for example with provisions allowing DPAs to carry out random checks at police premises.

Finally, Heald states that ‘for transparency to be effective, there must be receptors capable of processing, digesting, and using the information.’ The distinction is between what he calls ‘nominal’ and ‘effective’ transparency: the presence of transparency provisions can create only the illusion of government bodies being more accountable, if there is no other entity to check that such provisions are indeed implemented in practice. In which case, the transparency is nominal but not effective.199

This latter distinction is evaluative, and surely any system of control, any antipower, for preventative police surveillance should aim at ensuring effective transparency, and not only an appearance of it. This will, at least partially, depend on the powers given to those authorities entrusted with the supervision of police surveillance and their effective capability to hold the police accountable.200 Another important factor might be the possibility for NGOs and other civil society organisations with expertise on data protection to access information on police practices in the course of proceedings in front of DPAs or courts.201

In the following sections, I will introduce and analyse those safeguards provided by European data protection law that seems to improve the transparency of police surveillance across the different transparency dimensions presented by Heald.

### 4.4 The safeguards provided by data protection law

The following subsections will introduce and discuss the main safeguards provided by European data protection law that can serve as an antipower in the context of preventative police surveillance. Even though, as we have seen in the previous chapter, there are different legal texts, at the European level, that can be applicable to the police field, here I will mainly refer to the Law Enforcement Directive, as it constitutes the most detailed data protection legislation for the police sector so far. I will also refer to CoE law, when this can prove useful to analyse specific provisions.

---

199 Heald (n 194) 34-35.
200 For a more extensive discussion on this issue, see Section 4.4.3.
201 The Law Enforcement Directive allows such organisations to represent data subjects in the exercise of some of their rights. Namely, the right to lodge a complaint with a DPA, the right to appeal DPAs’ decisions in front of a court, and the right to an ‘effective judicial remedy against a controller or processor’. Law Enforcement Directive, Art 55.
4.4.1 Information and access rights

The most relevant rights recognised by the LED to data subjects are the rights to information and access, which are critical rights related to the fundamental right to data protection, and important instruments of transparency.

The right to information contains two provisions. Firstly, data controllers have to provide the generality of data subjects with a series of information on the controllers’ data processing activities (e.g., the identity of the controller, the purposes of the processing, the existence of the data subjects’ right to access). Secondly, in ‘specific cases’, they have to provide the data subject with ‘further information to enable the exercise of his or her rights’ (e.g., the legal basis for the processing, storage periods).

It seems therefore that with these provisions the LED introduces not only a form of ‘individual’ transparency, that is, related to the right to access information connected to the personal data of a specific data subject, but also a form of ‘general’ transparency, which entails informing the general public as regards the existence of police surveillance practices. This approach, consistent with the provisions of CoE Police Recommendation, is considered to be of ‘fundamental importance’ by the CoE, particularly in the case of infrastructural systems of surveillance, where data subjects may not even be aware of the existence of such measures. This is developed even more explicitly in the Practical Guide adopted in 2018 by the CoE to complement the Recommendation with more workable principles for police forces. This document states that ‘the data controller [should] provide general information to the public on the data processing that it carries out, and to give specific information to data subjects if no restrictions or derogations (…) apply.’

---

202 Law Enforcement Directive, Arts 13, 14, 16. Recital 38 seems to introduce a specific right to receive information and a right to obtain an explanation also in case of automated decision-making. On this, more specific, topic see Sajfert and Quintel (n 168) 9-10.

203 A data controller is defined as ‘the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data’. For the purposes of this thesis, when I refer to controllers/data controllers I mean the police. Law Enforcement Directive, Art 3(8).

204 Law Enforcement Directive, Art 13(1).

205 Law Enforcement Directive, Art 13(2).

206 Police Recommendation (n 137) Principle 6.1. The terms ‘individual’ and ‘general’ are introduced by the author. See also Explanatory Memorandum (n 138) para 34.

207 Explanatory Memorandum (n 138) para 81. See also Explanatory Memorandum (n 138) 44. The difference between the two information duties emerges also from the wording itself of Article 13. On the one hand, controllers have to ‘make [information about data processing] available’ generally to data subjects; on the other hand, in specific cases, controllers have to ‘give’ additional information to data subjects. Law Enforcement Directive, Arts 13(1) and (2).

208 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ‘Practical guide on the use of personal data in the police sector’ (T-PD(2018)01) (‘Practical Guide’).

209 Practical Guide (n 208) (emphasis added).
The right of access requires controllers to provide, upon request, a ‘confirmation’ concerning the existence of processing operations related to the data subject’s personal data, the possibility to access this data and the communication of additional information (e.g., the purposes and legal basis of the processing, the categories of personal data processed, the existence of the right to rectification or erasure).\textsuperscript{210}

The right to information and the right of access can be restricted by quite broad limitations that allows data controllers to curtail the exercise of such rights when this could undermine the purposes of the data processing.\textsuperscript{211} Articles 13(3) and 15 of the LED provide controllers with the possibility to ‘limit not only the rights, but also the information about the refusal to grant a certain right,’ thus making it sometimes ‘very difficult, or even impossible, to challenge such replies before courts.’\textsuperscript{212} Moreover, MSs can adopt legislation determining entire categories of processing for which the exercise of these rights can be restricted.\textsuperscript{213} Following the wording of Article 52 of the EU Charter, such limitations can be implemented only in so far as they constitute ‘a necessary and proportionate measure in a democratic society’ in order to pursue one of a series of legitimate interests, such as protecting public or national security, or avoid obstructing ‘inquiries, investigations or procedures’.\textsuperscript{214}

Because of the possibility of such limitations, it is crucial that data subjects also have the option to exercise their rights indirectly, through supervisory authorities.\textsuperscript{215} In all situations in which data controllers do not comply with data subjects’ requests because these are subject to limitations, data subjects’ will still have the possibility to ask for the intervention of the DPA. In these cases, the supervisory authority ‘shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place.’\textsuperscript{216}

\textsuperscript{210} Law Enforcement Directive, Art 14.
\textsuperscript{211} De Hert and Papakonstantinou, ‘The New Police and Criminal Justice Data Protection Directive’ (n 163) 12; De Hert and Sajfert, ‘Police, privacy and data protection from a comparative legal Perspective’ (n 129) 315. Concerning these restrictions, Bäcker and Hornung consider that the wording of Articles 13(3)(b), 15(1)(b), and 16(4)(b) ‘does not require that the criminal offence in question constitute the reason for the data processing. Moreover, it need not even be a criminal offence that the concerned data subject has committed itself or is connected to in any way. On this basis, the duty to notify could be virtually meaningless in practice. This is especially true for investigative measures which form part of an ongoing proactive strategy.’ Bäcker and Hornung (n 124) 631.
\textsuperscript{212} Sajfert and Quintel (n 168) 7.
\textsuperscript{213} Law Enforcement Directive, Arts 13(4) and 15(2).
\textsuperscript{214} Law Enforcement Directive, Arts 13(3) and 15(2).
\textsuperscript{215} Law Enforcement Directive, Art 17(1).
\textsuperscript{216} Law Enforcement Directive, Art 17(3). See also Caruana (n 166) 262. In her article, the author also argues that, unlike in the GDPR, in the LED there is no clear power for DPAs to order controllers to comply with the data subjects’ requests.
According to Sajfert and Quintel the introduction of this ‘two-level approach (…)
significantly improves the situation of data subjects (…) as it introduces another line of
checks by an independent supervisory authority.’\textsuperscript{217} Since it is broadly accepted that there
are situations in which the police have a legitimate interest in not providing certain
information on its surveillance activities – for example because they might frustrate an
ongoing operation – Article 17 of the LED provides for an additional instrument of
guarantee for the data subjects in these cases, as the DPA will still be able to carry out the
necessary checks to ensure that the police is making a legitimate use of those exemptions.
The LED provisions on data subjects’ rights can be considered ‘largely satisfactory’, as
they ‘introduce a number of adequate safeguards.’\textsuperscript{218} In particular, information and access
rights might constitute a useful instrument for the individual to directly control the
activities of the police (transparency downwards). Nevertheless, according to De Hert
and Papakonstantinou, the ‘extensive use’ from MSs of the provisions allowing to limit
their exercise ‘might ultimately render the exercise of all individual rights irrelevant’.
This is true only to a certain extent, as in cases where the restrictions are made use of, the
indirect exercise of rights should guarantee that an independent authority will still check
if the decision made by the police was legitimate and that surveillance powers are
exercised in a lawful way (transparency inwards).\textsuperscript{220}

\textbf{4.4.2 The accountability of data controllers}

The concept of accountability in data protection law\textsuperscript{221} is closely connected to the data
protection reform package approved in 2016 by EU institutions, and in particular to a
debate among European DPAs, in which context ‘accountability is understood as
requiring that organizations not only take responsibility for the data they handle, but also
have the ability to demonstrate that they have the systems, policies, training and other

\textsuperscript{217} Sajfert and Quintel (n 168) 13-14. The authors also note that this approach ‘seems to be inspired by the
relatively recent judgments of the ECtHR \textit{Roman Zakharov v. Russia} and \textit{Szabó and Vissy v. Hungary}’. 
\textsuperscript{218} Marquenie (n 163) 332.
\textsuperscript{219} De Hert and Papakonstantinou, ‘The New Police and Criminal Justice Data Protection Directive’ (n 163)
13.
\textsuperscript{220} Law Enforcement Directive, Art 17(3) read in conjunction with Art 46(1)(g). However, this will depend
ultimately on a number of factors, including the amount of resources DPAs will be able to dedicate to data
subjects’ requests, or the effectiveness of corrective powers given to them by MSs. On this latter point, see
n 216. For a discussion on DPAs’ powers, see Section 4.4.3.
\textsuperscript{221} See Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier, ‘The accountability principle in data
protection regulation: origin, development and future directions’ in Daniel Guagnin and others (eds), 
\textit{Managing Privacy through Accountability} (Palgrave Macmillan 2012); Charles Raab, ‘The Meaning of
“Accountability” in the Information Privacy Context’ in Daniel Guagnin and others (eds), \textit{Managing
Privacy through Accountability} (Palgrave Macmillan 2012).
practices in place to do so." While this concept was developed mainly in the context of data controllers subject to the GDPR, it is also spelled out as a data protection principle in the LED. \(^{223}\)

The principle of accountability places upon data controllers ‘the burden of implementing on their own initiative appropriate data protection measures in relation to the processing they execute’, in order to be able to demonstrate compliance with data protection principles and rules. \(^{224}\) This includes technical and organisational measures, \(^{225}\) such as data protection policies, \(^{226}\) Data Protection Officers, \(^{227}\) and safeguards embedded into the processing activities themselves, such as through data protection by design and by default. \(^{228}\) Controllers will also have to maintain records and logs of their processing activities. \(^{229}\)

A DPIA is required ‘where a type of processing, in particular, using new technologies (…) is likely to result in a high risk to the rights and freedoms of natural persons’. \(^{230}\) This will not only serve to have controllers better assess risks related to the rights and freedoms of data subjects, but it might also increase the transparency of processes leading to the decision to adopt a particular data processing system, and lead to a consequent improved oversight from supervisory authorities. In fact, the LED also introduces an obligation for data controllers to consult the supervisory authority prior to the processing of personal data, when the DPIA ‘indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk’ – or when the use of new technologies ‘involves a high risk to the rights and freedoms of data subjects’. \(^{231}\)

Moreover, as the DPIA needs to be documented, it can be accessed by DPAs also when

\(^{222}\) Alhadeff, Van Alsenoy and Dumortier (n 221) 14.
\(^{223}\) Law Enforcement Directive, Art 4(4).
\(^{225}\) Law Enforcement Directive, Art 19(1).
\(^{226}\) Law Enforcement Directive, Art 19(2).
\(^{227}\) Law Enforcement Directive, Art 32.
\(^{228}\) Law Enforcement Directive, Art 20.
\(^{229}\) Law Enforcement Directive, Arts 24 and 25.
\(^{230}\) Law Enforcement Directive, Art 27. According to De Hert and Papakonstantinou, the wording of the LED is quite strict in this regard and this provision should apply ‘whenever new technologies are used in the police and criminal justice context’. De Hert and Papakonstantinou, ‘The New Police and Criminal Justice Data Protection Directive’ (n 163) 17.
\(^{231}\) Law Enforcement Directive, Art 28. The language of this and the preceding article seems to be partially circular: on the one hand, the DPIA provision requires an assessment ‘where a type of processing, in particular, using new technologies (…) is likely to result in a high risk to the rights and freedoms of natural person’; on the other hand, Article 28 provides prior consultation where ‘a data protection impact assessment (…) indicates that the processing would result in a high risk’ or where ‘the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects’.
conducting general monitoring or investigative activities,\textsuperscript{232} or when investigating a specific complaint from a data subject. According to some authors, DPIA will play ‘an especially important role in the management of new surveillance and processing technologies.’\textsuperscript{233} These provisions, along with ‘the general obligation to cooperate with supervisory authorities and provide [them] with the necessary information,’ and with ‘the broad involvement of the supervisory authority in the workings and activities of the data controllers,’\textsuperscript{234} seem to strengthen the accountability of controllers \textit{vis-à-vis} supervisory authorities.

But the most promising obligations are probably Articles 24 and 25 of the LED, regarding the keeping of records and logs. The former provision mirrors the correspondent Article 30 GDPR and provides that controllers keep record of various information related to their data processing, to be made available to DPAs upon request. The latter is instead a peculiarity of the LED and requires that, for each processing operation, the time, the identification of the operator accessing the data, the possible recipients, and the justification for the processing operation itself are registered. According to Sajfert and Quintel, ‘as law enforcement databases contain high volumes of information on a large number of individuals, a lot of which are sensitive data, the logs play a central role in ensuring that such databases are not being abused and are only accessed by persons with proper authorization and with valid reasons to access retained data’.\textsuperscript{235} Overall, this improves the transparency of data processing activities, the accountability of controllers and the effective capability for supervisory authorities to oversee data processing.

The logging provision has the potential to greatly increase the transparency of police surveillance activities, as theoretically all digital technologies used by the police should comply with it. This might increase not only event transparency, allowing to check the lawfulness of each and every processing operation, but also, on the long run, process transparency, as an analysis of aggregated data could show if certain events are part of broader institutional behaviours or not. Nevertheless, it is possible that this provision will lead to a vast number of logs being produced, potentially affecting the possibility of this Article leading to effective transparency, depending, among other things, on the feasibility for DPAs to carry out frequent audits of such logs.

\textsuperscript{232} Law Enforcement Directive, Artt 46(1)(a) and (i). See also Law Enforcement Directive, Art 26.
\textsuperscript{233} Marquenie (n 163) 333. Of the same advice are Sajfert and Quintel. Sajfert and Quintel (n 168) 12.
\textsuperscript{234} Marquenie (n 163) 333-34.
\textsuperscript{235} Sajfert and Quintel (n 168) 16.
Overall, compared to previous data protection instruments in the police sector, the LED introduces much stronger accountability for data controllers, increasing inward and downwards transparency in preventative police surveillance. Records and logs should ensure, at least, that event transparency is enhanced. DPIAs, prior consultation requirements, and again logs, provided that they are extensively audited, might also increase process transparency, shedding some light on how the police design and implement such measures.

4.4.3 The role of Data Protection Authorities

Within the data protection framework, the role of supervisory authorities and their independence is of great importance. It is enshrined in EU Treaties and reiterated in the jurisprudence of the Court of Justice.\(^\text{236}\) Moreover, since ‘DPAs generally tend to take their monitoring powers seriously, if not expansively’,\(^\text{237}\) and since ‘effective supervision has increasingly been considered a highly important aspect of data protection (…) to foster accountability, strengthen data subject rights and improve the oversight of data controllers’,\(^\text{238}\) submitting preventative police surveillance to the supervision of DPAs seems to be an essential step in guaranteeing individuals’ privacy.

In the LED, supervisory authorities are vested with several powers,\(^\text{239}\) but there are doubts in literature concerning the adequacy of such powers, particularly if compared to GDPR standards: some of them are excluded, without any justification, while others are ‘more restrictively framed.’\(^\text{240}\) Indeed, Article 47 of the LED requires MSs to provide DPAs with investigative, corrective and advisory powers, but it does not provide for a detailed specification of what these powers should be. It ‘provides for a minimum harmonisation of investigative powers’, granting DPAs the power to access personal data and request information from data controllers, while ‘advisory powers boil down to the prior consultation procedure (in Article 28) and policy advice to the executive and the


\(^{238}\) Marquenie (n 163) 335.

\(^{239}\) Namely, to issue warnings, to order the controller or processor to bring processing operations into compliance, to impose limitations on processing, and to bring infringements of provisions to the attention of judicial authorities and possibly engage in legal proceedings. Law Enforcement Directive, Art 47.

\(^{240}\) Caruana (n 166) 259. See also Marquenie (n 163) 335.
legislative branch of the government’.

Concerning corrective powers, only three examples of what they might entail are provided.

This lack of more specific provisions could lead to some problematic results. For example, the LED requires MSs to lay down rules on penalties, to be imposed on data controllers who do not comply with data protection law. Moreover, it provides that supervisory authorities’ annual activity reports contain, among other things, information on the ‘penalties imposed’ during the year. Oddly enough, though, the power for DPAs to impose penalties is nowhere to be found in the Law Enforcement Directive. This might lead to a situation in which some MSs do not provide for DPAs to impose penalties – possibly providing for another authority to do so – while the language of Article 49 LED would suggest that this should be the case.

As noted earlier, it is understandable that the provisions of a directive are not as detailed as those of a regulation. At the same time, comparing the twenty-six powers provided to DPAs in the GDPR to their under-definition in the LED raises some doubts on the choices made by the legislator. Even more so, since on the capability of DPAs to conduct actual oversight relies a great deal of the possibility for data protection law to provide for effective and not only nominal transparency.

The rules concerning the appointment of DPAs under the LED might also constitute a problematic issue. Whereas the CoE advises that the authorities to supervise the police should be the same as for general data processing, EU law allows MSs to have a dedicated DPA for the LED, which might affect the independence and the effective capability for the authority to oversee the police.

Moreover, from a neorepublican perspective, the fact that the LED allows MSs to provide for the executive to appoint members of the DPA might be problematic. As in most MSs


242 Namely, to issue warnings to data controllers or processors ‘that intended processing operations are likely to infringe’ the LED, ‘to order the controller or processor to bring processing operations into compliance’, and to impose a limitation or ban on data processing. Law Enforcement Directive, Art 47(2).

243 Oddly enough, though, the power for DPAs to impose penalties is nowhere to be found in the Law Enforcement Directive. This might lead to a situation in which some MSs do not provide for DPAs to impose penalties – possibly providing for another authority to do so – while the language of Article 49 LED would suggest that this should be the case.

244 As noted earlier, it is understandable that the provisions of a directive are not as detailed as those of a regulation. At the same time, comparing the twenty-six powers provided to DPAs in the GDPR to their under-definition in the LED raises some doubts on the choices made by the legislator. Even more so, since on the capability of DPAs to conduct actual oversight relies a great deal of the possibility for data protection law to provide for effective and not only nominal transparency.

The rules concerning the appointment of DPAs under the LED might also constitute a problematic issue. Whereas the CoE advises that the authorities to supervise the police should be the same as for general data processing, EU law allows MSs to have a dedicated DPA for the LED, which might affect the independence and the effective capability for the authority to oversee the police.

Moreover, from a neorepublican perspective, the fact that the LED allows MSs to provide for the executive to appoint members of the DPA might be problematic. As in most MSs

245 Also the GDPR does not provide for a specific power for DPAs to impose penalties, while it does provide for a power to impose administrative fines. Under the LED, while MSs have to provide for corrective powers (Art 47(2) LED), it seems they might choose not to provide specifically for sanctioning powers. GDPR, Art 58(2)(i). See Caruana (n 166) 263.

246 On this issue, see De Hert and Sajfert (n 241) 250-53.

247 Law Enforcement Directive, Arts 57, 49. See Caruana (n 166) 259.

248 Explanatory Memorandum (n 138) para 31.

249 Law Enforcement Directive, Arts 41(1) and (3).

250 De Hert and Sajfert (n 241) 248.
the police are part of the executive itself, there is a risk that governments will appoint DPAs that are too sympathetic with police needs. For this reason, it would seem preferable to have only the parliament (possibly with the participation of both majority and minority parties) to make such an appointment. This is a critical aspect, since appointment provisions are closely related to the independence of supervisory authorities and since ‘DPAs are particularly under threat of being held in check by public authorities.’ The provisions on the appointment of DPAs are actually identical to those of the GDPR, but while they might be less problematic in the context of commercial data processing activities – probably less so in the administrative sector – they certainly raise more questions in the law enforcement context.

To conclude, the institution of DPAs in the police sector greatly increases at least nominal transparency, as it ensures that MSs provide for an oversight body for preventative police surveillance, where the judicial supervision is not as strong as in the context of traditional criminal investigations. Their role could be the element that ‘gives life’ to several data protection provisions, such as logging provisions and indirect access right. At the same time, as I have shown, in this context their independence could be less strong than in the context of the GDPR and, even more importantly, they might result not being equipped with sufficiently strong powers to perform their tasks, affecting the effective transparency provided by the LED.

### 4.5 Conclusion

The Law Enforcement Directive represents an important step in increasing the transparency of preventative police surveillance.

Analysing its provisions through the lens of Heald’s anatomy of transparency allows us to see that transparency is not a one-dimensional and static concept, but one that develops

---

251 Lacking a comprehensive comparative research on the police forces of the 28 EU MSs, reference can be made to the information provided by the institutional websites of Interpol (https://www.interpol.int/en/Who-we-are/Member-countries) and OSCE (https://polis.osce.org/index.php/country-profiles). From these sources it emerges that most MSs’ police forces are organised either under the Ministry of Interior (in 14 MSs) or under another Ministry (in 8 MSs), while only in 6 MSs the police are organised in a decentralised way, with different level of involvement of the executive in their organisation and supervision.

252 In a 2010 study, the Fundamental Rights Agency of the EU even found that, in some MSs, DPAs were attached to the Ministry of the Interior. European Union Agency for Fundamental Rights, Data Protection in the European Union: the role of National Data Protection Authorities (Publications Office of the European Union 2010) 8. See also Philip Schütz, ‘Comparing formal independence of data protection authorities in selected EU Member States’ (Conference Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference, 2012) 9-10.

253 Schütz (n 252) 10.

254 See Law Enforcement Directive, Art 43; General Data Protection Regulation, Art 53.
in many directions and along many dimensions. Hence, it can be seen as the linking element among the three concepts at the core of the concept of neorepublican antipower – transparency, accountability and oversight. Sometimes, transparency constitutes an enabling factor to achieve accountability and oversight. Other times, oversight and accountability can be themselves instruments to achieve different dimensions of transparency.

The regime for EU data protection seems therefore to provide for a good starting point to control police activities in this context. If effectively implemented, the right to information and the right of access can strongly improve individuals’ awareness of police data processing. At the same time, the possible limitations lower the level of protection in a number of circumstances. The problem with these limitations is that the reasons that might justify them are framed in a broad way and this, especially if they are applied to entire categories of data processing by MSs, could seriously restrict the impact of these provisions. While in the context of the reactive model these restrictions could be considered less problematic, since surveillance is usually more targeted and other safeguards are already provided by criminal law, in the context of preventative surveillance the possibility to limit information and access rights should be framed in a more restrictive way. A better approach seems to be that of CoE Practical Guide, which states that ‘restrictions or derogations (…) should only apply to the extent necessary and be interpreted narrowly’, and that ‘the response should provide clear justification of the decision making which can be verified by an independent authority or a court.’

At the same time, the provision of the indirect exercise of data subjects’ rights can be considered an attempt of the legislator to balance the need for opacity of law enforcement activities with the protection of data subjects’ rights. This might help ensuring an acceptable level of protection, also when rights are restricted, depending on the effective possibility for DPAs to carry out the necessary checks on police processing activities.

Provisions related to the accountability of data controllers also constitute a promising step towards more transparency, as data controllers will have to document and provide justifications for their processing activities. In general, most provisions seem to point towards event transparency, with data controllers being held accountable for single data points and providing single pieces of information to the data subject. However, a lack of clear and binding auditing provisions risks undermining the effective reach of these rules.

---

255 Practical Guide (n 208) 7.
as ‘relying solely on self-monitoring would prevent the full exercise of different investigative or corrective powers of the supervisory authorities.’

Ultimately, I find two main issues which might undermine the possibility for the current data protection regime to provide for an antipower in the context of preventative police surveillance.

The first element consists in the minimum harmonisation provided by the LED. Even if this is understandable, given the sensitivity of the field and existing difference in MSs’ laws regulating the law enforcement sector, it risks creating a situation where provisions are incoherently applied throughout MSs, possibly leading to low levels of protection. This is true not only because of the ambiguity of some terms, or due to the freedom left to MSs to implement certain provisions, but also because of the lack of precision in certain others.

The second element concerns the role of DPAs, which are, as previously noted, a fundamental element in European data protection law. The problems highlighted regarding their independence and the divergences with the GDPR concerning their powers could seriously undermine their oversight capabilities, to the result that their ability to oversee preventative police surveillance might not be enough to constitute an antipower.

---

257 Sajfert and Quintel (n 168) 17.
258 Although, as previously noted, the guidance from the EDPB and the jurisprudence of EU Courts can hopefully lead to more legal certainty, and help ensuring a high level of protection.
5. Conclusion

The main research question of this thesis originated from the necessity to provide for new means of protection in the context of preventative police surveillance. When states provide police forces with broad surveillance powers to prevent crime and manage risks to public security, the normative choices of determining the possibility for the State to intrude upon individuals’ private sphere have already been made. For this reason, there is a need to provide for additional transparency tools, to channel and control these broad powers.

As explained at the beginning of the third chapter, data protection seems to be a rather fitting and useful instrument to provide for an increased level of transparency of such practices. Before analysing data protection safeguards, though, there was a need to assess if European data protection law is, indeed, applicable to preventative police surveillance. Dealing with this matter entailed a discussion on the terminology of security-related concepts used in CoE and European legal texts to define the scope of application of the law. In European law, terms such as public security, public order, and public safety are never clearly defined and often juxtaposed, so that determining with certainty the scope and the limitations of European data protection instruments in the police sector is a rather difficult task. Nevertheless, the fact in itself that the legislator included terms such as crime prevention, public order and public security in the scope of the legal texts analysed led me to tentatively conclude that these laws were indeed designed also to be applied to the prevention of crime and the management of public security.

This provisional conclusion allowed me to take up the task, in the fourth chapter, of determining how European data protection law can provide for legal protection in the analysed context. The neorepublican concept of antipower provided me with some guidance on what kind of safeguards could be useful to avoid that the police, and hence the State, exercise domination towards individuals within preventative police surveillance. Additionally, Heald’s anatomy of transparency allowed me to better describe what kind of transparency the different safeguards provided by the EU Law Enforcement Directive provide.

All these elements now allow me to answer the main research question of this work.

How is it possible to provide for individuals’ legal protection in the context of preventative police surveillance?

We can provide for individuals’ legal protection in the context of preventative police surveillance by applying European data protection legislation for the police sector to these
surveillance activities. Data protection provides for legal protection by submitting such surveillance activities to a series of procedural safeguards which increase the transparency of police actions. First of all, individuals are assigned rights in order to become aware of police surveillance practices generally, and of data processing related to them individually. They also have rights in order to challenge such surveillance practices before data controllers, in court or in front of supervisory authorities. The police, in their position of data controller, have duties to document and justify each data processing activity, so that compliance with data protection rules can be demonstrated, and their practices can be checked by supervisory authorities. These authorities oversee police operations to make sure that surveillance activities comply with data protection law and they assist individuals in exercising their rights.

In particular, the LED is an important step in raising data protection standards for the police sector in Europe, as it provides for more specific rules than preceding legal texts and it produces direct legal effects in national legal systems, so that also national courts will be able to enforce it. Moreover, this new legal text brings data protection in the police sector under the jurisdiction of the Court of Justice of the European Union. Given recent case law and the link with ECtHR standards, we can expect this to further strengthen the legal protection of individuals and, hopefully, to solve some of the legal issues highlighted in this work. Considering all these elements, it would seem that data protection can indeed provide for a suitable system of legal protection in the context of preventative police surveillance.

However, there are still many issues that might impair this capability. Firstly, there is a risk that MSs might broaden the concept of national security to avoid applying the LED to preventative police surveillance. Secondly, the fact that certain surveillance tools might be used both for police purposes and national security could make it practically impossible to apply different data protection standards to the same processing. Thirdly, the limitations to data subjecta’ rights, which can be considered less problematic in the context of the reactive model, might substantially lower the level of protection in the context of preventative surveillance. Fourthly, the LED provides only minimum harmonisation, and while some MSs may provide for higher data protection standards, others might make full use of the exceptions provided, leading to low levels of protection.

259 Marquenie (n 163) 328.
260 According to Bäcker and Hornung, the Law Enforcement Directive could also increase the impact of the ECHR and the ECtHR indirectly, due to the fact that the ECHR is part of the EU acquis and the Court of Justice ‘possesses de facto the power to set aside domestic statutes of the Member States due to the supremacy of Union Law.’ Bäcker and Hornung (n 124) 633.
for data subjects. Finally, the issues regarding the independence and the powers of DPAs could weaken their oversight capabilities.

Ultimately, whether the provisions of the LED will constitute an antipower that can effectively prevent the State from ‘subjugating’ individuals through preventative police surveillance, will depend on MSs’ implementing legislation and on the interpretation of the law provided by the EDPB and EU courts, in particular concerning the independence and the powers of DPAs, which are critical elements to provide for effective transparency. Hence, some recommendations can be made for future legislative interventions:

- The legislator, in this case both at CoE and EU level, should more clearly define the scope of data protection law, in particular clarifying the boundaries between different security-related domains – national security, public security, and public order – to ensure legal certainty and a high level of data protection in the police context.

- Concerning the LED, the EU legislator should follow the approach of CoE Practical Guide and draft restrictions in a narrower way, to make sure that they are employed only when necessary for specific reasons (e.g., the necessity to safeguard an ongoing criminal investigation) and that their use is properly justified.

- The EU legislator should at least provide for a minimum, but specifically defined, set of powers for DPAs. These powers could then be extended by MSs, so that in all MSs supervisory authorities can effectively fulfil their tasks, and to avoid lowering the level of protection below standards set by the CJEU in leading case law.

Finally, some considerations on the academic literature analysed and possibilities for further research.

During the gathering of literature for this thesis, it was quite striking to find few sources analysing preventative police surveillance from a legal perspective. While literature on mass surveillance, and in general on surveillance by secret intelligence services, abounds, I found very few sources dealing with the regulation of the use of specific technologies by the police to manage public security and public order. For this reason, I believe that further research could be conducted on how different European jurisdictions regulate police surveillance powers in the preventative context and outside criminal investigation, and on how the police effectively use surveillance tools for related purposes.

Caruana (n 166) 251-52; Marquenie (n 163) 329; Sajfert and Quintel (n 168) 22.
Another issue that seems to be under-researched is that of data protection in the police sector. Starting from the report for the 25th year of the Police Recommendation, some research could be done on how Contracting Parties implement data protection in this context. It would be particularly interesting also to observe how EU MSs have implemented the Law Enforcement Directive, to see if some of them have made remarkable legislative choices to solve the uncertainty of some provisions, as well as to analyse, in the coming years, the guidance emerging from the EDPB, and DPAs’ case law.
Bibliography

Table of cases

Court of Justice of the European Union

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12, C-594/12) [2014] ECLI:EU:C:2014:238

European Commission v Federal Republic of Germany (C-518/07) [2010] ECLI:EU:C:2010:125

European Commission v Republic of Austria (C-614/10) [2012] ECLI:EU:C:2012:631

Maximillian Schrems v Data Protection Commissioner (C-362/14) [2015] ECLI:EU:C:2015:650

European Court of Human Rights

Malone v The United Kingdom (1984) Series A no 82


Table of legislation

European Union Law


**English law**

Criminal Justice and Public Order Act 1994


Police and Criminal Evidence Act 1984

**Italian law**

Codice di procedura penale

Decreto Legge 18 agosto 2000, n 267, in materia di ‘Testo unico delle leggi sull'ordinamento degli enti locali’

Decreto Legge 20 febbraio 2017, n 14, in materia di ‘Disposizioni urgenti in materia di sicurezza delle città’

Decreto Legge 4 ottobre 2018, n 113, in materia di ‘Disposizioni urgenti in materia di protezione internazionale e immigrazione, sicurezza pubblica, nonché misure per la funzionalità del Ministero dell'interno e l'organizzazione e il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata’

Decreto Legge 4 ottobre 2018, n. 113, in materia di ‘Disposizioni urgenti in materia di protezione internazionale e immigrazione, sicurezza pubblica, nonché misure per la funzionalità del Ministero dell'interno e l'organizzazione e il funzionamento dell'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata’

Decreto Legislativo 30 luglio 1999, n 300, in materia di ‘Riforma dell'organizzazione del Governo, a norma dell'articolo 11 della legge 15 marzo 1997, n. 59’

Legge 1 aprile 1981, n 121, in materia di ‘Nuovo ordinamento dell'Amministrazione della pubblica sicurezza’

Regio Decreto 18 giugno 1931, n 773, in materia di ‘Approvazione del testo unico delle leggi di pubblica sicurezza’

**International treaties**

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS 108
Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [2018] CETS 223

Secondary sources

Official documents

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ‘Practical guide on the use of personal data in the police sector’ (T-PD(2018)01)


Council of Europe, ‘Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector’

Council of Europe, ‘Recommendation on the use of personal data in the police sector’ (R (87) 15, adopted by the Committee of Ministers on 17 September 1987)


Books

De Pauw E, and others (eds), Technology-led policing (Maklu 2011)
Garner BA, Black's Law Dictionary (Ninth edition, West 2010)

Gibson N, Criminal Justice – A beginner’s guide (Waterside Press 2014)


Hijmans H, The European Union as Guardian of Internet Privacy (Springer 2016)

Leigh LH, Police powers in England and Wales (Butterworths 1985)


Smits JM, The Mind and Method of the Legal Academic (Edward Elgar 2012)


Tonini P, Manuale di procedura penale (Giuffrè 2015)


Contributions within books


Alonso Blas D, ‘First Pillar and Third Pillar: Need for a Common Approach on Data Protection?’ in Serge Gutwirth and others (eds), Reinventing Data Protection? (Springer 2009)


Cape E, and others, ‘Procedural rights at the investigative stage: towards real commitment to minimum standards’ in Ed Cape and others (eds), Suspects in Europe. Procedural Rights at the Investigative Stage of the Criminal Process in the European Union (Intersentia 2007)


Darbyshire P, ‘Criminal Procedure in England and Wales’ in Richard Vogler and Barbara Huber (eds), Criminal Procedure in Europe (Duncker and Humblot 2008)

De Hert P, Gutwirth S, ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’ in E Claes, A Duff and S Gutwirth (eds), Privacy
[https://works.bepress.com/serge_gutwirth/5/]


Dobinson I, Johns F, ‘Qualitative Legal Research’ in Mike McConville and Wing Hong Chui (eds), Research Methods for Law (Edinburgh University Press 2007)


Hildebrandt M, ‘Criminal Law and Technology in a Data-Driven Society’ in Markus D Dubber and Tatjana Hörnle (eds), The Oxford Handbook of Criminal Law (Oxford University Press 2014)

Hutchinson T, ‘Doctrinal research” in Dawn Watkins and Mandy Burton (eds), Research Methods in Law (Routledge 2013)


Perrodet A, ‘The Italian system’ in Mireille Delmas-Marty and JR Spencer (eds), European Criminal Procedures (Cambridge University Press 2002)

Raab C, ‘The Meaning of “Accountability” in the Information Privacy Context’ in Daniel Guagnin and others (eds), Managing Privacy through Accountability (Palgrave Macmillan 2012)


Vervaele J, ‘Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?’ in S Gutwirth, R Leenes and P De Hert (eds), Reloading Data Protection (Springer 2014)


Journal articles


De Hert P, Papakonstantinou V, ‘The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for’ (2009) 25 Computer Law & Security Review 403


Fonio C, ‘The silent growth of video surveillance in Italy’ (2011) 16 Information Polity 379


Schafer B, ‘Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill’ (2016) 40 Datenschutz und Datensicherheit 592

Scott PF, ‘Secrecy and surveillance: lessons from the law of IMSI catchers’ (2019) 33 International Review of Law, Computers & Technology 1


Sheldon B, ‘Camera surveillance within the UK: Enhancing public safety or a social threat?’ (2011) 25 International Review of Law, Computers & Technology 193

Spencer JR, ‘Adversarial vs inquisitorial systems: is there still such a difference?’ (2016) 20 The International Journal of Human Rights 601

Tzanou M, ‘Data protection as a fundamental right next to privacy? “Reconstructing” a not so new right’ (2013) 3 International Data Privacy Law 88


**Research, conference, and working papers**


Schütz P, ‘Comparing formal independence of data protection authorities in selected EU Member States’ (Conference Paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference, 2012)

**Reports**


**Other secondary sources**


CPDP Conferences, ‘CPDP 2019: law enforcement and data subjects' rights’ (31 February 2019) 30:42-32:24 comments by Vagelis Papakonstantinou <https://www.youtube.com/watch?v=b8ab7oU4ZC0>


