LAWFUL PROCESSING OF PRIVATELY OWNED CAMERAS

AN ANALYSIS ON THE COMPLIANCE OF PRIVATELY OWNED CAMERAS USED BY DUTCH POLICE WITH THE DUTCH AND EUROPEAN STANDARDS

AUTHOR: FREDERICK PRANGER

DATE: NOVEMBER 1ST 2020

UNIVERSITY: TILBURG UNIVERSITY

FIRST READER: MAGDA BREWCZYŃSKA

SECOND READER: COLETTE CUIJPERS

ACKNOWLEDGMENTS

I would like to thank Magda Brewczyńska, Colette Cuijpers and Bo Zhao for their continuous feedback on this thesis. Furthermore, I would like to thank my family and friends for their support. This thesis would not have been possible without them.

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AP	Dutch Data Protection Authority
CJEU	Court of Justice of the European Union
DPA	Data protection authority
DPIA	Data protection impact assessment
ECHR	European Convention on Human Rights
FRT	Facial recognition technologies
ICT	Information communication technologies
IP	Internal Protocol
GDPR	General Data Protection Regulation
GW	Dutch Constitution (de Grondwet)
LED	Law Enforcement Directive
POC	Privately owned camera
TEU	Treaty on European Union
Wbp	Wet bescherming persoonsgegevens
Wjsg	Wet justitiële en strafvorderlijke gegevens
Wpg	Wet politiegegevens

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Camera's. They are everywhere. On highways, within cities and, more increasingly, on our own property. One may wonder whether we are aware of our lives (potentially) being registered by cameras of others. We are aware of the existence of public camera's, such as used on highways, but we may not be aware of the increasing existence of privately owned camera's that may register much more intrusive images of our lives. Such privately owned camera's, perhaps due to the seeming unawareness of bystanders, register images that public cameras would not. As such, they might be very useful for, for example, criminal investigation purposes. Criminals may be aware of public camera's, but, given the increase in privately owned camera's, it is conceivable that they can run from public camera's, but can't hide from privately owned cameras. Such camera's may, for example, be aimed at registering the front yard and, in the process of doing so, also register a street where no public cameras are placed. If more and more houses would have such camera's, it would ultimately become impossible for the criminals to hide from such cameras' coverage. The increase in privately owned camera's and their potential usefulness has sparked the interest of the Dutch government given that it is in fact increasingly utilizing privately owned cameras, such as private CCTV cameras, to surveille private spaces for criminal investigation purposes.[1]

While this might sound great, one should not forget that it is not only criminals that would be registered on camera. It would also be you who is being filmed while stepping out of your car with groceries, while being with your new lover or while having a fight with a friend. One may wonder whether we are willing to trade less criminality on the street for our private life being filmed and (potentially) having that footage used and analyzed by the police. Furthermore, an image that allows for identification of a natural person must be regarded personal data, which requires legal protection. For that reason, when the police would want to use camera footage of privately owned camera, they must comply with the rules for protection of personal data.

One may wonder whether the police should always be allowed to make use of footage derived from privately owned camera's for crime investigation purposes. Especially given the circumstance that the police would then be able to register private footage of citizens on a large

[1] Sander Flight, 'Politie En Beeldtechnologie: Gebruik, Opbrengsten En Uitdagingen' (Sanderflight.nl, 2016), p.69 <http://sanderflight.nl/wp-content/uploads/2016/08/2016-Flight-beeldtechnologie-Justitiele-Verkenningen.pdf> accessed 26 August 2020.

scale. It might surprise you that the police are already doing so, at least in the Netherlands. The Dutch police has recently introduced a register, named 'Camera in Beeld' (hereafter: the Register), for the registration of privately owned cameras (hereafter: POCs) which can exclusively be accessed by the police.[2] POCs are the umbrella term for various cameras, such as CCTV cameras and even digital doorbells. All POCs are eligible to be registered. POCs are meant to record images of one's private property. At the same time, POCs may also record a part of the public space. An example would be the digital doorbell filming the front garden and possibly a part of the sidewalk. Registration of POCs is still voluntary, but there have already been discussions regarding a mandatory registration of POCs. Some POCs are already automatically registered.[3] Once registered, the police could thus access footage of a privately owned camera that registers images without the individuals on those images being aware of that. For example, a digital doorbell might register everyone walking by the house, while the majority of the people walking by will be unaware of such doorbell registering this.

Given that the police will make use of such footage that people are unaware of, the question can be raised as to whether this would violate our right to protection of personal data. The safeguards regarding our right to protection of personal data in the European Union are laid down primarily in two legal instruments, namely in the General Data Protection Regulation (hereafter: GDPR) and, and for the processing of personal data within a law enforcement context, in the Law Enforcement Directive (hereafter: LED). When processing personal data, the GDPR and the LED both require a lawful basis in order for a processing activity to be lawful. Therefore, important questions that can be raised regarding the processing of POC data by the police are: what is the legal basis for this processing activity? And under what circumstances is the use of POC footage by the police for criminal investigation purposes compliant with the standards of data protection?

1.2 PROBLEM DESCRIPTION

As noted, the LED states that a processing activity must have a lawful basis. For the use of the Register, such lawful basis exists. At least, according to the Dutch police provided that the footage of the Register being processed has "added value" (*daadwerkelijke meerwaarde*) for criminal

[2] 'Verplichte Registratie Privé-Camera's? 'Dan Worden Burgers Verlengstuk Politie' (*Nos.nl*, 2018) <https://nos.nl/nieuwsuur/artikel/2238765-verplichte-registratie-prive-camera-s-dan-worden-burgers-verlengstuk-politie.html> accessed 25 March 2020.

[3] Tijs Hofmans, 'Gratis Deurbellen Tegen Criminaliteit' (Tweakers.net, 2019) <https://tweakers.net/reviews/7524/2/digitale-deurbellen-het-twijfelachtige-effect-en-de-privacyzorgen-andere-gemeenten.html> accessed 28 August 2020.

investigation purposes. It is, however, not clear whether the position of the police is correct. One may doubt whether the criterion of "added value" fully respects the principle of lawfulness as required by the LED. The LED, in any event, does not provide any indications that footage having "added value" for criminal investigation purposes automatically results in having a lawful basis for the processing of such footage. Taking this lack of support for the "added value" criterion in the LED into consideration, the question can be raised whether, or under what circumstances, the "added value" criterion is compatible with the principle of lawfulness of the processing of personal data in accordance with the LED.

1.3 SIGNIFICANCE

The question raised above is relevant, especially given the lack of uniformity as to the application of the "added value" criterion for using the Register with POCs. At present, there are no – official or unofficial – guidelines shedding a light on how the police should determine that POC footage has "added value" for criminal investigation purposes. In the absence of such guidelines, the determination by a police officer whether POC footage has "added value" might differ on a case-by-case. This poses the risk that the police treat similar cases differently. In order to help mitigate this potential dissimilar treatment of similar cases, the purpose of this thesis is to ascertain the extent to which the application of the "added value" criterion would be (in)compatible with the applicable standards of lawful processing. In order to achieve this purpose, this thesis will provide a legal analysis on the lawfulness of the use of POC footage by Dutch police with regards to Dutch citizens' data protection rights enshrined in the EU and Dutch legal framework. Based on the outcome of such an analysis, the lack of uniformity could be mitigated because the analysis should result in guidance as to how "added value" criterion can be applied in a way that is compliant with the principle of lawfulness in the LED. In making the analysis in this thesis, only the usage of data derived from POCs by Dutch police for criminal investigation purposes will be looked into. For this reason, the processing by POC owners under the GDPR, including the question whether the GDPR would be applicable (taking into account, inter alia, the household exemption), will not be analyzed in this thesis. This research is relevant in practice, because it provides insight on the ways in which the Dutch police is allowed to use registered POCs for criminal investigation purposes under the "added value" criterion.

1.4 DEFINITION OF SCOPE

This thesis firstly presents the different kinds of POCs that the police utilize for criminal investigation purposes from the Register. Secondly, it examines the technology in POCs. Thirdly, it assesses the applicable European and Dutch data protection laws regarding the use of POCs for criminal investigation purposes by Dutch police. Finally, the thesis assesses whether the use of POCs by police is compliant with the applicable European and Dutch data protection laws.

1.5 RESEARCH QUESTIONS

This research study answers the following research question:

> *Does the processing of personal data collected through privately owned cameras (POCs) by Dutch police for criminal investigation purposes comply with the principle of lawfulness of data protection (as stated in the Law Enforcement Directive)?*

In order to answer the main research question, the following sub-questions will be answered throughout this thesis:

1. What are POCs and what does the Dutch police use them for?
2. How is the principle of lawfulness defined in the Law Enforcement Directive?
3. How is the principle of lawfulness of processing defined in Dutch law?
4. To what extent does the police's use of POCs comply with the principle of lawful processing?

1.6 LITERATURE REVIEW

The purpose of this thesis is, to examine the extent to which - or under what circumstances – the use of POCs by the Dutch police for criminal investigation purposes, by applying the "added value" criterion, is compliant with the principle of lawfulness of processing. In this respect, it can be noted, at the outset, that the "added value" criterion does not follow from, at the very least, written EU law. In addition, as a preliminary note, the lack of uniform guidance as to the interpretation (and thus application) of the "added value" criterion implies that the criterion can, at least in theory, be dependent from police officer to police officer. Taking this into consideration these two preliminary points, this thesis will essentially examine the extent to which the use POCs for criminal investigation purposes by the governments can be compliant with the principle of lawfulness of data protection. Such examination could then be used to propose uniform guidance for the interpretation (and application) of the "added value" criterion so as to ensure compliance with the principle of lawfulness. With respect to the principle of lawfulness, this principle is laid

down in European and Dutch law. There is, however, no specific guidance as to the application of the principle of lawfulness in respect of the use of POCs for criminal investigation purposes. In addition, few scholars write on this subject. As such, a gap exists on a Dutch and international level.

The existence of such a gap is interesting, especially in light of the increase in the use of POCs in general. Moreover, since 1975, the usage of public as well as private cameras for crime investigation purposes by Dutch police has also increased steadily. The introduction of body cams (small cameras attached to the uniform or body of policemen), drones and helicopter-cameras were the latest addition to the arsenal of visual police aid.[4] With regard to the usage of cameras by Dutch police, the ECHR and Dutch Constitution need to be respected.[5] Individuals have the right to be left alone by the government unless there is a legal ground and it is sufficiently necessary and proportionate to utilize a camera.[6]

A research by Bart Engberts addressed the importance of private cameras in apprehending perpetrators.[7] In case a criminal act is suspected, however severe it may be, private cameras can play a pivotal role in the police investigation. Relevant evidence such as camera footage can be obtained by the police when collaborating with private camera owners, especially in places where there could be a communal purpose of safety. This information aids the more efficient gathering of evidence but more importantly helps ensure a more complete investigation. This may very well point to a specific interest the police have, namely obtaining private camera footage to create a complete investigation and to have sufficient evidence for a possible arrest of the perpetrator.

While the use of POCs may have increased, it is noteworthy that, in an extensive research that has been conducted with regard to the usage of public and private cameras by Dutch police, the added value of these cameras, for criminal investigation or as evidence in court, is still unknown.[8] Knowing this, the justification of the "added value" criterion for the use of POC footage is troublesome. One could wonder if the Dutch police would be allowed to access such footage based

---

[4] Sander Flight, 'Politie En Beeldtechnologie: Gebruik, Opbrengsten En Uitdagingen' (Sanderflight.nl, 2016), p.83-85 <http://sanderflight.nl/wp-content/uploads/2016/08/2016-Flight-beeldtechnologie-Justitiele-Verkenningen.pdf> accessed 26 August 2020.

[5] ibid p.83-85.

[6] ibid p.83-85.

[7] Bart Engberts, 'Sensing Door De Politie En Publiek-Private Samenwerking: Operationele Noodzaak' (Politieacademie.nl, 2016), p. 1-3 <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/92748.pdf> accessed 14 June 2020.

[8] Sander Flight, 'Politie En Beeldtechnologie: Gebruik, Opbrengsten En Uitdagingen' (Sanderflight.nl, 2016), p.88 <http://sanderflight.nl/wp-content/uploads/2016/08/2016-Flight-beeldtechnologie-Justitiele-Verkenningen.pdf> accessed 26 August 2020.

on such a criterion. In any event, at present the Dutch police can only make use of POCs if the "added value" criterion would be met; otherwise, the use of such POCs would be unlawful, Assessing the meaning of "added value", has, however, turned out to be rather difficult.

As is shown in the literature, there are several reasons as to why cameras oppose a larger threat to the right to data protection now more than before.[9] The digitalization has increased the information flow via the deployment of (among other devices) cameras in public and private spaces. Additionally, information communication technologies, or 'ICT's', can facilitate extra information to public spaces. An example is public Wi-Fi, on which users can receive additional information about a city's history. Taking this example one step further, smart cameras can even facilitate extra information to public spaces by means of infrared-technology or augmented reality-technology. While this extra data could be convenient to law enforcement for criminal investigation purposes, it could also oppose threats to the individual's right to data protection if the data is processed unlawfully. Because there is so much more data being processed in modern societies, this data could aid the police in criminal investigations. Therefore, there is an interest for Dutch police to receive as much additional data as possible for an investigation. However, this usage of data must always be done within the data protection standards set in place by the European Union.

On July 10th 2019, the European Data Protection Board (hereafter: the EDPB) has issued guidelines on lawful use of public and private cameras.[10] With regard to the general notions made in these guidelines, the EDPB acknowledges that camera use can be necessary to serve the interests at stake (for example a jewelry store that wants to increase safety measures). However, the use of cameras should only be done when strictly necessary, while always considering other (less intrusive) measures and only if the interests of the data subjects are not neglected.

1.7 METHODOLOGY

This thesis is a result of a theoretical doctrinal legal research.[11] The legal dogmatic methodology entails systematically explaining legal rules and concepts. The written laws in the Netherlands and the European Union (EU) are the subject of this thesis, as in effect on the date of this thesis. Such

[9] Bo Zhao, 'Exposure And Concealment In Digitalized Public Spaces' (*Rug.nl*, 2017), p.150-155 <https://www.rug.nl/research/portal/en/publications/exposure-and-concealment-in-digitalized-public-spaces(ff4c6eb8-0fbe-4428-b985-13b057c7615b).html> accessed 26 August 2020.

[10] 'Guidelines 3/2019 On Processing Of Personal Data Through Video Devices' (EDPS, 2019), <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en> accessed 29 October 2020.

[11] Jan M. Smits, 'What is legal doctrine? On the aims and methods of legal-dogmatic research', Maastricht European Private Law Institute Working Paper (2015) 06, p. 8.

laws predominantly include statutes and case law. In addition, reference is also made to the legal literature in order to obtain a better understanding of such laws.[12]

With respect to the laws taken into consideration in this research, only cases that are relevant in the Netherlands will be considered. As such, the geographical scope of the legal dogmatic methodology in this thesis is limited to the Netherlands. The relevant cases that will be taken into account, based on this geographical scope, are cases of Dutch legal courts, as well as the European Court of Justice. The purpose of defining this geographical scope is to set boundaries within the research of this thesis and to provide a complete answer to the research question with regard to the use of POCs by the police for criminal investigation purposes.

With respect to the relevant literature and scholarly opinions analyzed, the thesis focuses on developing a more in-depth understanding of the current legal frameworks that apply to the use of POCs by the police for criminal investigation purposes.

1.8 THESIS STRUCTURE

The structure of this thesis will be described in this paragraph. Chapter 2 categorizes POCs that are relevant to the crime investigations by Dutch police and identifies what their relevance is. Chapter 3 analyzes the European legal frameworks regarding lawful processing with regard to the use of POCs by Dutch police. Chapter 4 analyzes the Dutch legal framework with regard to lawful processing. Chapter 5 elaborates on if the use of POCs for criminal investigations by the Dutch police is compliant with the European and Dutch standard of lawfulness. The conclusion summarizes the results of the research and provides a clear answer to the research question.

[12] J.B.M. Vranken, 'Kenmerken Van Juridisch Dogmatisch Onderzoek' (2014), hfdstk 8, Asser/Vranken Algemeen <https://www.navigator.nl/document/id5c32ae2109264b1f910d57eab2012098?ctx=WKNL_CSL_1743> accessed 27 October 2019.

CHAPTER 2: THE USE OF PRIVATELY OWNED CAMERAS BY DUTCH POLICE

2.1 PRIVATELY OWNED CAMERAS (POCS) AND RELEVANT TECHNOLOGIES

This chapter will explain what privately owned cameras (POCs) are and what kind of technologies they use. To that end, for the reason of clarity, firstly a possible categorization of POCs will be made. Secondly, the usage of POCs in two camera projects by Dutch police will be discussed.

In order to determine what POCs are, the landscape of cameras in the Netherlands needs to be described. POCs can be categorized in various ways. In this thesis three distinctions between POCs are proposed, namely: [13]

1. Stationary versus portable cameras: stationary cameras are cameras that are immovable and usually attached to property or solid ground. An example is the Closed-Circuit Television (CCTV) camera. Such cameras are often used in public areas such as city center streets or market squares. Portable cameras are cameras that are movable. An example is the GoPro, which is a pocket-sized camera that can be turned on and off with a simple button.

2. Non-smart versus smart cameras: a non-smart camera has only one function typically characteristic for cameras, namely video recording. An example is a CCTV camera. Smart cameras are cameras that in addition to video recording, can also analyze a scene, extract information from that scene and report activities to its user. An example is the digital doorbell. Such a camera does record an environment in the process, but this is not it's only fundamental purpose.[14] A smart camera can extract information from the image that is recorded. Therefore, the output of information from a smart camera is more extensive. Smart cameras are of particular interest to the government due to their use in distributed smart networks. Distributed smart cameras are interesting for governments

[13] 'Cameratoezicht In Nederland; Een Schets Van Het Nederlandse Cameralandschap' (2013), p. 15-29, <https://www.researchgate.net/publication/320555155_Cameratoezicht_in_Nederland_een_schets_van_het_Nederlandse_cameralandschap> accessed 2 April 2020.

[14] Bernhard Rinner, 'Toward Pervasive Smart Camera Networks' (*Www.sciencedirect.com.tilburguniversity.idm.oclc.org*, 2009) <https://www.sciencedirect.com.tilburguniversity.idm.oclc.org/topics/engineering/smart-camera> accessed 22 April 2020.

due to their ability to analyze recorder information from large spaces while the cameras. These cameras can facilitate the work of the police for example by identifying a suspect through a fast and efficient public video sharing platform.[15] When several smart cameras are combined to cover a large space or when algorithms are used to perform a smart camera operation, this is called a distributed smart network.[16]

3. Public versus private cameras: Public cameras are owned and controlled by the government or municipality. An example is license plate recognition cameras placed above city entrances. Cameras that are owned and controlled by private parties, such as individuals or companies are considered private cameras.

The distinction between the categories is not set in stone. This is illustrated by cameras fitting in more than one of the categories described above at the same time. For example, a CCTV camera can be both stationary and smart (due to possible extra functionalities). Another example is the GoPro. This camera is smart (due to its extensive functionalities) and portable.
This thesis focuses primarily on a recently introduced governmental camera projects and the involvement of POCs in this project, namely: Camera in Beeld.[17] This project will be further explained in the next paragraph.[18]

2.2 GOVERNMENTAL CAMERA PROJECTS

[15] Bernhard Rinner, 'Toward Pervasive Smart Camera Networks' (*Www.sciencedirect.com.tilburguniversity.idm.oclc.org*, 2009) <https://www.sciencedirect.com.tilburguniversity.idm.oclc.org/topics/engineering/smart-camera> accessed 22 April 2020. Ring-owners can share any video feed that contains criminal or even suspicious behavior to the public social network called 'Neighbours'. See also: Drew Harwell, 'Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns' (The Washington Post, 2019) <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/> accessed 8 September 2020.

[16] ibid.

[17] 'Cameratoezicht In Nederland; Een Schets Van Het Nederlandse Cameralandschap' (2013), p. 15-29, <https://www.researchgate.net/publication/320555155_Cameratoezicht_in_Nederland_een_schets_van_het_Nederlandse_cameralandschap> accessed 2 April 2020.

[18] It is particularly interesting for the Dutch government to attempt to access these cameras because the access to the footage of the POCs is less restricted. See also; Bart Van Der Sloot, 'Het Gegevensbeschermingsrecht Op De Schop: Noodzaak Of Afbraak?' (*Bartvandersloot.nl*, 2017) <https://bartvandersloot.nl/onewebmedia/Het_gegevensbeschermingsrecht_op_de_scho.pdf> accessed 4 April 2020. In this article the increasing frequency and relevance of governmental data processing through smart cameras is discussed as well. It appears apparent that smart cameras are becoming more relevant in multiple ways. The issues regarding Big Data will not be discussed in this thesis; See also: 'Inzet Van Sensordata Voor Leefbaarheid En Veiligheid | Rathenau Instituut' (*Rathenau.nl*, 2019) <https://www.rathenau.nl/nl/digitale-samenleving/inzet-van-sensordata-voor-leefbaarheid-en-veiligheid> accessed 23 April 2020.

2.2.1 CAMERA IN BEELD

The first governmental camera project that will be discussed is one that the police has initiated: a register named Camera in Beeld. The police are therefore the initiative taker of the project.

The program encourages individuals and private companies, who placed stationary POCs on their property (the camera owners) to register these camera's in the Camera in Beeld register (hereafter: Register).[19] The registration can take place via the website of the Dutch police and requires a POC owner to provide the Dutch police with personal details as well as some information on the camera. This information consists of details on whether the camera is actually filming, how long the footage is stored and if it stores photos of the video feed.

After registration, the police can use the camera footage obtained from the POCs for ongoing investigations. Registered cameras can however only be accessed by Dutch police if the footage has any "added value" for the investigation.

As opposed to placing cameras with the permission of the mayor close to private properties by police, it is less time consuming to make use of POCs. The cameras are already in place and the police can access the footage without requiring additional consent from other authorities or private camera owners when requesting camera footage from these POCs.[20] Private households or companies do not need any kind of consent to place cameras, while they could potentially record (part of) a public place.

Quantitatively, it is estimated that with Camera in Beeld the police would gain access to approximately 230,000 cameras without any intervention from the mayor, of which 88% would capture at least part of a public road.[21]

The police supervise and process all incoming applications by private individuals and companies to register their POC. Other than that, the police are not yet involved in the data processing. According to the police's registration website, there are no requirements that govern what kind of cameras can be installed and registered. It could be a smart camera storing additional data, such as IP addresses of the owner of the camera, in addition to the video and audio data. Only the police

---

[19] "Camera in Beeld" (*Politie.nl*, 2019) <https://www.politie.nl/themas/camera-in-beeld.html?sid=afedd054-0221-49a3-acab-58aa68496ad3> accessed 23 November 2019. National marketing campaigns were initiated by Dutch police to encourage private camera owners to register for the Register.

[20] Concerns have been voiced about this lack of consent in the processing of data by Police. With regard to the Dutch Criminal Code of Procedure, Police do not request footage but order it in accordance with Article 126nd Criminal Code of Procedure and Dutch Supreme Court case law; see also: [2010] Hoge Raad, 08/03502 (Hoge Raad).

[21] Lotte Houwing, 'Hoe De Politie Haar Buitenwettelijke Surveillancenetwerk Uitbreidt' (Joop.bnnvara.nl, 2020) <https://joop.bnnvara.nl/opinies/hoe-de-politie-haar-buitenwettelijke-surveillancenetwerk-uitbreidt> accessed 11 February 2020.

have the authority to access the camera register and are permitted to request and process data from a private camera owner if necessary, for criminal investigation purposes.

2.2.1.1 DIGITAL DOORBELL PILOT

An initiative implemented by the Ministry of Justice and Security in the Netherlands in cooperation with the police, the Department of Criminality Prevention, and the municipalities is the use of Ring digital doorbells.[22] As part of the initiative, the government subsidized municipalities to distribute digital doorbells to civilians (the owners of the camera). The municipalities of Almere, Eindhoven, and Oostbroek (among others) subsidized the purchase of approximately 100 smart doorbells through governmental funds. However, in order to obtain this subsidy, the doorbells had to be automatically registered with Camera in Beeld. This mandatory registration appears to be a way for the police to obtain greater access to POCs in a short period of time. Due to the absence of clear guidelines on the utilization of and access to these doorbells by police, questions were raised by the Dutch parliament regarding the right to protection of personal data and access to this data by police.[23]

Ring is the most prominent smart doorbell. Ring smart doorbells were introduced worldwide in 2015 and quickly became a success.[24] The company's doorbell features a high-definition camera, a motion sensor, and a speaker for two-way conversations between visitors and users. Smart doorbells are useful to civilians and companies for monitoring who is or has been at their door, but they can also provide useful information to police forces due to their ability to, for example, easily identify trespassers in case of a burglary. The potential use of these POCs for the Dutch police force is not merely conceivable; it is already being put into practice in other countries. For example, in the United States Ring has a contractual obligation to relinquish data from the doorbell feed. This obligation could possibly come into effect if the police have reason to believe that the video footage would be of value in a criminal investigation. The possibility that such intrusive obligations would also emerge in the Netherlands cannot be excluded. For now, Ring does not have similar obligations to the Dutch police forces.[25]

---

[22] Rudy Bouma, 'Slimme Deurbel Rukt Op In Strijd Tegen Inbraken, Maar Hoe Zit Het Met Privacy?' (*NOS.nl*, 2020) <https://nos.nl/nieuwsuur/artikel/2318362-slimme-deurbel-rukt-op-in-strijd-tegen-inbraken-maar-hoe-zit-het-met-privacy.html> accessed 13 February 2020.

[23] 'Kamerstuk 28684, Nr. 617' (*Zoek.officielebekendmakingen.nl*, 2020) <https://zoek.officielebekendmakingen.nl/kst-28684-617.html> accessed 23 April 2020.

[24] (Ring Europe, 2015) <https://eu.ring.com/> accessed 13 February 2020.

[25] Arnoud Wokke, 'Tweakers' (Tweakers.net, 2019) <https://tweakers.net/nieuws/156730/ring-heeft-geen-samenwerkingscontracten-met-politie-in-nederland-en-belgie.html> accessed 13 February 2020.

Though Ring currently does not have any contractual obligations to the Dutch police, a similar less intrusive obligation exists in the Netherlands since the Ring cameras involved in the government project were automatically registered with Camera in Beeld. After registration, the doorbell feed can be requested by the Dutch police force if the footage has potential "added value" (described in chapter 4).[26]

The Ring doorbell has potential to be helpful to criminal investigations especially because of its smart functionalities, but that potential is also the downside of the POC. Even though the additional data and functionalities could be helpful to criminal investigations, clear safeguards should be in place to control the access the police have to this data. It remains doubtful if the current safeguards are sufficient.[27]

As mentioned before, questions have been raised regarding access to data by police. The collected data does not only include video and audio data; independent research has shown that Ring doorbells do not only collect data for law enforcement, the doorbell also secretly collects data for analytic companies. [28] This data consists of names, time zone, device model, language preferences on the device, sensor data (from the test device's magnetometer, gyroscope and accelerometer) Internal Protocol (IP) addresses, and mobile networks from the owners.[29] The Electronic Frontier Foundation, an organization defending civil liberties in a digital world, discovered that this additional data stored by the Ring-doorbell was provided to four main analytics and marketing companies, such as Google and Facebook. This data processing takes place without any user notification or user consent and, in most cases, there is no option to retrieve the data or have it deleted from the servers.[30] Because of the scope of this thesis, these privacy implications for the owners of the cameras can only be recalled here, but will not be further discussed.

2.3 CONCLUSION

[26] Rudy Bouma, 'Slimme Deurbel Rukt Op In Strijd Tegen Inbraken, Maar Hoe Zit Het Met Privacy?' (*NOS.nl*, 2020) <https://nos.nl/nieuwsuur/artikel/2318362-slimme-deurbel-rukt-op-in-strijd-tegen-inbraken-maar-hoe-zit-het-met-privacy.html> accessed 13 February 2020.

[27] Tom Mckay, 'Duh: FBI Warned Doorbell Cams Can Also Tip Suspects Off To Approaching Cops' (Gizmodo, 2020) <https://gizmodo.com/duh-fbi-warned-doorbell-cams-can-also-tip-suspects-off-1844911515?utm_source=gizmodo_newsletter&utm_medium=email&utm_campaign=2020-09-01> accessed 4 September 2020.

[28] Bill Budington, 'Ring Doorbell App Packed With Third-Party Trackers' (Electronic Frontier Foundation, 2020) <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers> accessed 8 September 2020.

[29] ibid.

[30] 'Ring Doorbell 'Gives Facebook And Google User Data' (*BBC News*, 2020) <https://www.bbc.com/news/technology-51281476> accessed 23 April 2020.

In this chapter the concept of POCs as used in this thesis has been clarified. In that respect, it has been clarified which POCs are relevant for the Dutch police for criminal investigations purposes and how the police can use these POCs in an ongoing camera project. While the categorization of POCs could show some overlap when examining a certain POC, an attempt has been made to categorize the POCs based on their distinctive traits.

The most prominent Dutch governmental camera project, Camera in Beeld, has been discussed. The Camera in Beeld-project, accompanied by the Ring-project, shows the potential usefulness of POCs for criminal investigation purposes. The criterion applied by Dutch police for the use of POCs and the compliance of this criterion with what the European and Dutch data protection standards try to safeguard will be further investigated in later chapters.

From this chapter it can be derived that POCs in this thesis are private cameras that possess different traits. However, in the current projects under scrutiny, the POCs relevant to the Dutch police are mainly stationary, private, smart and non-smart.

CHAPTER 3: PRINCIPLE OF LAWFULNESS IN THE LAW ENFORCEMENT DIRECTIVE

3.1 INTRODUCTION

This chapter will look into the principle of lawfulness as laid down in the LED. The purpose of this chapter is to determine under what circumstances processing of personal data by law enforcement authorities can be considered lawful under the LED. In doing so, the scope of the LED will be discussed first. Second, article 8 of the LED, which contains the principle of lawfulness, will be analyzed. Finally, this chapter will end with a conclusion regarding the question under what circumstances processing of personal data by law enforcement authorities meets the conditions of the principle of lawfulness as laid down in the LED.

3.2 THE LAW ENFORCEMENT DIRECTIVE

The general rules regarding the processing of personal data of natural persons within the European Union, are laid down in Regulation (EU) 2016/679, better known as the General Data Protection Regulation (hereafter: GDPR). During the intergovernmental conference which adopted the Treaty of Lisbon in 2007 the Member States acknowledged, by means of Declaration 21, the need for specific rules for personal data relating to judicial cooperation in criminal matters and police cooperation, due to the specific nature of this data.[31] This need was subsequently turned into a legislative act by the adoption of Directive (EU) 2016/680, also known as the Law Enforcement Directive or LED, which lays down the specific rules relating to personal data processed by competent authorities for specific, namely law enforcement, purposes.

The purpose of the LED is to harmonize the rules regarding the processing of personal data relating to the activities by competent authorities.[32] Such activities taken by competent authorities can include the exercise of authority by taking coercive measures such as police activities at large public events. It can also include police or other authorities maintaining law and order to safeguard against and prevent threats to public safety. In order for data processing to fall under the LED, both the personal and material scope have to be met. This entails that processing has to be carried out by a competent authority (personal scope) and processing needs to be carried out for one of the aforementioned purposes (material scope). The scope of the LED is intended to, essentially,

[31] Recital 10 LED.
[32] Recital 15 & 12 LED.

cover all personal data processing that takes place in a law enforcement context, regardless of whether the processing takes places domestically or outside of the borders of the Member State.[33] The purposes that the LED provides include the "prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties."[34] Furthermore, the data processing needs to be conducted by a competent authority. Competent authorities are defined as any authority that can carry out the aforementioned purpose in data processing or any other body or entity entrusted by member state law to exercise public authority.[35] Article 2 (1) states that the data processing must be performed through wholly or partly automated means.[36]

With respect to the scope of the LED, two exclusions are made. Firstly, processing of personal data "*in the course of an activity which falls outside of the scope of Union Law*" is excluded from the scope of the LED.[37] Secondly, processing "*by the Union institutions, bodies, offices and agencies*" is excluded as well.

The LED entered into force on May 5, 2016, and EU member states were obligated to incorporate it into their national laws by May 6, 2018. The LED aims to protect the fundamental rights and freedoms of natural persons, particularly their right to the protection of personal data.[38] The LED has played a substantial role in the development of "an area of freedom, security and justice with a high level of data protection in accordance with the EU Charter [red: of Fundamental Rights]."[39] The GDPR and the LED are heavily related.[40] To exemplify this, the recitals of the LED indicate that when a competent authority processes for other purposes than stated in this Directive, the GDPR applies to that processing.[41] In addition, the LED closely follows the rules and principles enshrined in the GDPR when defining the core principles that should cover data processing.

[33] Paul de Hert, 'The New Police And Criminal Justice Data Protection Directive' (Pure.uvt.nl, 2016), p. 9-11, <https://pure.uvt.nl/ws/portalfiles/portal/19816258/pdh16_vpdirective_corrected_.pdf> accessed 10 September 2020; see also: Article 1 & 2 LED.
[34] Article 1 (1) & 2 (1) LED.
[35] Article 3 (7) LED.
[36] Article 2 (2) LED.
[37] Article 2(3) LED.
[38] Article 1 (2)(a) LED.
[39] M.R. Leiser, The Law Enforcement Directive: Conceptual Challenges of EU Law (2019), p. 1, <https://openaccess.leidenuniv.nl/bitstream/handle/1887/79246/2019_Leiser_en_Custers_Submitted_LED_paper_EDPL.pdf?sequence=1> accessed 28 April 2020.
[40] FRA, Handbook On European Data Protection Law (2018), p.33.
[41] Recital 11 LED.

3.2.1 LAWFULNESS OF PROCESSING

In order for a data processing activity to be lawful, it needs to be based on a legal ground. The LED provides one ground, namely processing that is necessary for the performance of a task carried out by a competent authority.[42] In contrast to the LED, the GDPR provides six grounds, including five grounds for processing that are based on a condition of necessity. Since necessity of the processing is required in most of the grounds in the GDPR, the GDPR can function as an inspiration for further examining the condition of necessity needed for processing in the LED. Furthermore, with respect to processing under the GDPR, processing should be done lawfully, fairly and in a transparent manner. Whereas the GDPR thus refers to three criteria, the LED, in article 4, only states processing should be done lawfully and fairly in article 4. Interestingly, transparency is left out. This can, however, be explained by the specific nature of processing under the LED given that such processing may be done in covert operations or video surveillance.[43] In such cases, having to be transparent about the processing, would defeat the purpose of the processing and thus the operation in itself.

The question when the processing of personal data is compliant with the principle of lawfulness, can be answered by further analyzing article 8 of the LED. This article reads as follows:[44]

*"*1. *Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.*

2. *Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing."*

There are three important elements that can be derived from this provision:

Firstly, the processing of personal data must be *necessary* for the performance of a task carried out by a competent authority (section 3.2.2). Secondly, the processing must be carried out for the *purposes* set out in article 1(1) (section 3.2.3). Thirdly, and finally, the processing must be based on Union or Member State law (section 3.2.4).

[42] Article 8 LED.
[43] Recital 26 LED.
[44] Article 8 LED.

3.2.2 NECESSITY

The first element that needs to be taken into account is the necessity of the processing activity, as stated in article 8 of the LED. With respect to determining how necessity in article 8 of the LED should be interpreted, it should be noted at the outset that there is, up to this date, no case law from the CJEU. In the absence of case law with respect to the term "necessity" in article 8 of the LED, reference shall be made to other sources and their interpretation of the term "necessity". Such sources include the EDPS toolkit, case law on other legal instruments and guidelines issued by several Data Protection Authorities. Given that these sources are not binding upon the CJEU if it would be called to interpret the meaning of necessity in article 8 of the LED, the weight to be attached to such sources is difficult to determine. However, at present, the sources discussed below will nonetheless help shed a light on the way in which the term "necessity" is currently being applied.

3.2.2.1 EDPS TOOLKIT

The first source to which reference can be made in order to shed a light on the meaning of the term "necessity" is article 52 of the Charter. This provision states that any limitation on the exercise of the rights and freedoms recognized by the Charter, such as the right to personal data protection as stated in article 8, must be necessary for an objective of general interest or to protect rights and freedoms of others. The European Data Protection Supervisor, Europe's independent data protection authority (hereafter: EDPS), issued a 'necessity toolkit' to help EU policymakers and legislators to assess the compliance of proposed measures with EU data protection law.[45] In this toolkit, a checklist is presented including the following items:

1. A detailed factual description of the measure is needed;
2. An examination of whether the measure is a limitation on the right to protection of personal data or any other right;
3. The objective of the (contemplated) measure must be examined;
4. The application of the necessity-test, in particular the tests of effectiveness and intrusiveness.[46]

[45] 'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (Edps.europa.eu, 2017) <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 10 September 2020. The EDPS consists of a head supervisor and has a support team of lawyers, IT specialists and administrators.
[46] Ibid p.9.

While the toolkit may provide a checklist, it does not provide a straight forward answer on whether a measure would be compliant with the necessity requirement. It does, however, offer a checklist and legal analysis of the necessity test applied to the processing of personal data.[47] According to the toolkit, necessity implies the need for a fact-based analysis of the effectiveness of the measure for the objective pursued and it requires an assessment on whether the measure in question is a less intrusive measure in comparison to other options for achieving the same objective.[48] Furthermore, the toolkit states that, in line with case law of the CJEU, if the envisaged measure is considered necessary, only then should the measure be tested to be proportionate. [49] In practice, this entails that the competent authority can only deem a measure necessary if the authority can justify that the use of the measure is indeed necessary in the specific circumstances.[50]

As mentioned above, proportionality and necessity are often linked. They are however separate principles. The European Court of Justice (hereafter: CJEU) determined that *"the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives"*.[51]

The principle of proportionality is also addressed in the EDPS toolkit. According to the toolkit, proportionality can be viewed in a broad and narrow sense. Proportionate in a broad sense encompasses both the necessity and the appropriateness of a measure.[52] Proportionality in a narrow sense, *i.e.* the principle of proportionality as enshrined in article 52 of the Charter, means that for a measure to meet proportionality the advantages need to outweigh the disadvantages.

Recital 26 of the LED elaborates on when covert investigations or video surveillance are lawful. It states that such activities can be done "as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate

[47] ibid p.2.

[48] 'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (Edps.europa.eu, 2017), p. 5 <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 10 September 2020.

[49] CJEU, C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para 51.

[50] 'Guidelines 3/2019 On Processing Of Personal Data Through Video Devices' (EDPS, 2019), p. 8-9 <https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en> accessed 29 October 2020.

[51] CJEU, C-62/14, Gauweiler, 16 June 2015, para. 67.

[52] 'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (Edps.europa.eu, 2017), p. 5 <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 10 September 2020.

interests of the natural person concerned". This seems to indicate that necessary is in fact intertwined with the requirement of proportionality.

3.2.2.2 CASE LAW

As mentioned before, the toolkit of the EDPS gives a checklist on how to assess the necessity of a measurement. However, it does not give a clear answer on how to interpret the requirement of necessity in the LED.

Unfortunately, as mentioned above, there is no case law in which the CJEU explained how necessity should be understood within the context of the LED. Therefore, in order to have a better understanding of the necessity-criterion in this context, other legal instruments need to be examined. Such an examination could, by analogy, be relevant for assessing the meaning of the necessity criterion under article 8 of the LED. With respect to examining other sources of EU law, the case law regarding the GDPR does not provide any answer either in how to interpret this criterion. However, before the GDPR was introduced, there were already multiple EU instruments in effect regarding data protection, including Directive 95/46/EC and the Data Retention Directive.[53] Even though these cases are based around older legislation, the cases do give an insight as to how the European Court has interpreted the term necessity in a surveillance context.

With respect to the necessity under the predecessor of the GDPR, Directive 95/46/EC, reference can be made to *Huber*.[54] In this case, the Higher Administrative Court asked the CJEU if personal data processed in a central register for foreign nationals, was compatible with Community law. The CJEU ruled that in order to meet the criterion of necessity, the measure should contribute to a more effective application of the legislation in question.[55]

Moreover, in *Digital Rights Ireland,* with regard to the Data Retention Directive, the CJEU had to rule whether articles 3, 4 and 6 of this directive were compatible with several articles of the Treaty of the European Union.[56] The articles of the directive required *"telephone communications service providers to retain traffic and location data relating to those providers for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State."* It was ruled, inter alia, that 'fighting against serious crime', as stated in this directive, as an objective of general interest does not justify a measure being necessary for that purpose.[57]

[53] Directive 95/46/EC & Directive 2006/24/EC.
[54] CJEU, C-524/6, Huber, 16 December 2008.
[55] CJEU, C-524/6, Huber, 16 December 2008, para 54-62.
[56] CJEU, C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014.
[57] CJEU, C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014, para. 51-65.

Even though both of these cases regarded legislative instruments that are outdated, the interpretation of necessity in a surveillance context by authorities could, by analogy, be relevant for determining the meaning of the term necessity in article 8 of the LED.

3.2.2.3 DATA PROTECTION AUTHORITIES

Besides the Charter and the GDPR, there are no other EU legislative sources in this context that, by analogy, may help assess the necessity criterion under article 8 of the LED. As such, in order to further look into the – potential – meaning of the term necessity under article 8 of the LED, reference will be made to non-legislative sources. With respect to the weight to be attached to such sources, it should be mentioned that the CJEU is, by no means, bound by them and may, in the end, choose a different direction. However, in the absence of any case law of the CJEU in this respect, these non-legislative sources will be addressed below in order to look for direction on how to interpret the necessity requirement. One of these sources are the guidelines issued by the Working Party 29 (hereafter: WP29) (currently replaced by the European Data Protection Board (EDPB)). In their "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", WP29 stated that when conducting a DPIA, one must assess the necessity and proportionality of the measures of the processing, amongst other assessments.[58] This is also stated in article 35 subsection 7 of the GDPR. Even though these guidelines were written for Directive 95/46/EC, the meaning of the word 'necessary' seems to be aligned with the meaning as intended in the GDPR (and the LED as mentioned above). In the second annex of these guidelines, necessity is addressed more extensive. With regard to the GDPR, the guidelines state that measures should be contributing to necessity on the basis of four pillars:

1. specified, explicit and legitimate purposes,
2. lawfulness of processing,
3. adequate, relevant and necessary data and
4. limited storage duration.

Furthermore, the guidelines mention multiple sources on where to find more information on how to conduct a DPIA and thus, how to further interpret necessity.[59]

[58] 'Guidelines On Data Protection Impact Assessment (DPIA) And Determining Whether Processing Is "Likely To Result In A High Risk" For The Purposes Of Regulation 2016/679' (Ec.europa.eu, 2017) <https://ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 12 September 2020.
[59] ibid.

One of these sources mentioned by the WP29 is the guide created by the Information Commissioner's Office (hereafter: ICO), the English Data Protection Authority.[60] The ICO has created this guidance for organizations in order to conduct a DPIA.[61] Noteworthy is that at the time of the issuance of the guide, the UK were still part of the European Union. This guide gives a further explanation on which questions to consider in order to determine the necessity of a processing operation. When assessing the necessity and proportionality, companies are encouraged to answer the following questions, including questions on the compliance measurements:

1. "Do your plans help to achieve your purpose?
2. Is there any other reasonable way to achieve the same result?
3. Is there another way to achieve the same outcome?
4. How will you prevent function creep?
5. How will you ensure data quality and data minimization?
6. What information will you give individuals?
7. How will you help to support their rights?
8. What measures do you take to ensure processors comply?
9. How do you safeguard any international transfers?"[62]

The questions are quite similar to the questions to consider when conducting a DPIA, although when it comes to necessity in terms of a DPIA, the overall 'compliance' with the GDPR seems to play a bigger role.

Taking this into consideration, the ICO made an interesting comment in its opinion on the use of live facial recognition technology by law enforcement in public places.[63] While the subject is not the same as the use of POCs, one of the comments made by the Commissioner should also be taken into account when analyzing the necessity requirement of the LED:

[60] At the time of the creation of the template, the UK was a member of the European Union and therefore, the ICO's template is relevant for this thesis.

[61] 'Data Protection Impact Assessments' (Ico.org.uk) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> accessed 12 September 2020.

[62] 'DPIA Suggested Process And Template' (Ico.org.uk) <https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx> accessed 12 September 2020.

[63] 'How Do We Apply Legitimate Interests In Practice?' (Ico.org.uk), p.9 <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> accessed 12 September 2020.

In the Commissioner's view, inconsistency across police forces in terms of necessity and proportionality must be avoided to prevent a lack of clearness and predictability for the public.[64] As mentioned above, a clear meaning of the word necessity is also needed for the public to know when the police might process their personal data. Based on the analysis above, necessity will always be explained by ways of balancing multiple interests and measures. Not providing a clear and predictable explanation.

The ICO also created a guide on processing personal data in a law enforcement context. In this guide, necessity is also discussed. It states that "It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is necessary for the stated purpose."[65]

Another source mentioned by the WP29 is the template for privacy impact assessments, issued by the Commission nationale de l'informatique et des libertés (hereafter: CNIL), the French Data Protection Authority. [66]

The CNIL issued this in-depth template on how to conduct a DPIA. In the template, the CNIL explains how to assess the proportionality and necessity of the processing. According to this template, there are multiple factors to take into account:

1. The justification of the purposes
2. The justification of the lawfulness: is there a legal basis as stated in article 6 of the GDPR?
3. The justification of data minimization
4. The justification of data quality
5. The justification of storage durations

The factors of the CNIL have some overlap with the questions recommended by the ICO when conducting a DPIA, but they do have some differences. As mentioned above, the ICO also recommends a few different questions to take into account when conducting a DPIA. It does give some insight into the interpretation, the guidelines by the national data protection authorities do not give a clear answer on how to interpret the criterion of necessity.

[64] 'How Do We Apply Legitimate Interests In Practice?' (Ico.org.uk), p.9 <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> accessed 12 September 2020.

[65] 'Principles' (Ico.org.uk) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/> accessed 12 September 2020.

[66] 'Privacy Impact Assessment' (Cnil.fr, 2018), p. 5-8 <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf> accessed 15 September 2020.

3.2.2.4 SUMMARY

To summarize, the interpretation of the necessity-criterion has been done in various ways. First, the EU Charter states that any limitation on the rights and freedoms enshrined in the Charter must be necessary for an objective of general interest or to protect rights and freedoms of others. Second, the toolkit focusses on a fact-based analysis of effectiveness as well as an assessment of proportionality in relation to necessity. Third, the case law states that in order to determine necessity of the measure, the application of the legislation should be more effective as a result of the measure. Finally, the ICO and CNIL focus on whether the purpose of the measure is being achieved and whether that purpose is justifiable. Furthermore, the ICO focusses on proportionality as well as an assessment of the chance of function creeping. The CNIL carries on to discuss the other principles enshrined in the GDPR, such as the justification of data minimization, data quality and storage duration.

In comparison, most of these sources seem to focus on the effectiveness of the measure, the proportionality of the measure and the intrusiveness of the measure. While all ways are contributing towards a proper interpretation, the aspects of the toolkit in combination with the case law seem like the most appropriate way to test necessity in this thesis. This is because three aspects are assessed in these sources:

- How effective the measure is to accomplish the purpose;
- how intrusive the measure is with regard to the privacy of the data subject;
- if the measure is proportionate in relation to the infringement of the privacy of the data subject.

3.2.3 LAW ENFORCEMENT PURPOSES

The second criteria that needs to be considered when processing data is that processing has to take place for a specific purpose. As stated before, the purposes under which the competent authorities can process data are set out in Article 1(1) LED. The stated purposes include the "prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties"[67].

Recital 12 of the LED states that activities carried out by police and law enforcement are mainly focused on these purposes.[68] As mentioned before, the recitals provide some examples, such as taking coercive measures such as police demonstrations at public events.

[67] Article 1 (1) & 2 (1) LED.
[68] Recital 12 LED.

Not all data processed by law enforcement authorities falls under the scope of the LED.[69] For example, if a law enforcement agency processes personal data regarding payment of wages of its employees, this processing falls under the GDPR. Even processing activities regarding borders, asylum and migration falls under the scope of the GDPR and not the LED. Data used on crimes that already have taken place (for example, data regarding evidence in court) as well as data used on crimes that still might take place (for example, a crime prediction models used to prevent crime) fall under the scope of the LED. Data is also not limited to criminal events, but also to suspects, criminals, victims, witnesses, testifying law enforcement officers and police informants.

With respect to video surveillance, the EDPS has issued guidelines wherein the purposes are discussed in a law enforcement context. In case of an occurrence of a physical security incident, video recordings can be used for investigative purposes. When that use of video recordings shifts towards a more preventive purpose, meaning the use of video recordings without a physical security incident, it should be used only in exceptional circumstances. To determine whether these uses are permissible and if they need any safeguards requires a case-by-case analysis.[70]

3.2.4 UNION OR MEMBER STATE LAW

The third element that needs to be taken into account when processing data is that the processing needs to be based on Union or Member State law. In other words, processing has to be based on European or national law. Whether there is an obligation to implement by a Member State depends on the type of European law. In case of a directive, the Member State has an obligation to implement the directive into national law. In case of a regulation, this is automatically binding for a Member State and it does not need any implementation.[71]

Recital 33 explains that where the LED refers to Member State law, it does not necessarily need to be a legislative act adopted by a parliament, "as long as it is clear and precise, and its application is foreseeable for those subject to it".[72]

---

[69] Leiser M R, 'The Law Enforcement Directive: Conceptual Challenges Of EU Law Enforcement Directive' (2019), p. 5-7, <https://openaccess.leidenuniv.nl/bitstream/handle/1887/79246/2019_Leiser_en_Custers_Submitted_LED_paper_EDPL.pdf?sequence=1> accessed 28 April 2020.

[70] 'THE EDPS VIDEO-SURVEILLANCE GUIDELINES' (Edps.europa.eu, 2010), p. 20-21 <https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> accessed 10 September 2020.

[71] 'Applying EU Law' (European Commission - European Commission) <https://ec.europa.eu/info/law/law-making-process/applying-eu-law_en> accessed 13 September 2020.

[72] Recital 33 LED.

3.3 CONCLUSION

This chapter has made an attempt to explain the standards of lawful processing under the LED. As described in this chapter, lawfulness of processing consists of three elements, namely: necessity of processing, purposeful processing and processing based on Union or Member State law. In the absence of case law of the CJEU regarding the meaning of the term 'necessary' in the LED, an attempt has been made to interpret the necessity term on the basis of the following other sources: a toolkit designed by the EDPS, relevant case law and guidelines on lawful processing made by various Data Protection Authorities.

Necessity is explained in many different ways but can be captured in the following characteristics: Firstly, necessity implies a fact-based analysis of effectiveness of the measure as well as an assessment of the intrusiveness of the measure. Secondly, necessity implies an assessment of the measure's contribution to being helpful in a better application of the law. Finally, it may include an assessment of whether the measure contributes towards the achievement of the purpose of the measure. Taking into consideration that these three characteristics are most common in the sources analyzed in this chapter, the most appropriate interpretation of necessity, for the purposes of this thesis, contains three elements: the effectiveness of the measure, the intrusiveness of the measure and the relation of proportionality in a case.

CHAPTER 4: PRINCIPLE OF LAWFULNESS IN DUTCH LAW

4.1 INTRODUCTION

This chapter will discuss how the principle of lawfulness derived from the LED has been implemented into Dutch law and how it is applied. The purpose of this chapter will thus be to examine the meaning of this principle under Dutch law. The LED, including its principle of lawfulness, has been implemented into Dutch law in two laws, namely: The Dutch Police Data Act and the Dutch Judicial and Criminal Records Act.[73] For the purposes of this thesis, the implementation of the principle of lawfulness in the Dutch Police Data Act is most relevant. This is because of the fact that the Dutch Judicial and Criminal Records Act is not applicable to the use of POCs for criminal investigation purposes. This is confirmed in the evaluation report of the Dutch Judicial and Criminal Records Act.[74] Therefore, the Dutch Judicial and Criminal Records Act will only be briefly discussed in this thesis. First, the Dutch Police Data Act shall be analyzed. Secondly, the processing of data by Dutch police derived from POCs will be discussed. Finally, the threat of function creeping related to the use of data by Dutch police derived from POCs will also be discussed.

The scope of the Dutch Judicial and Criminal Records Act is limited to the processing of judicial data by the Minister of Finance for the purposes of ensuring a good criminal procedure (*goede strafrechtspleging*).[75] The data to be processed under the Dutch Judicial and Criminal Records Act is processed in so-called judicial documentation. For these purposes, judicial documentation is defined as "a coherent collection of judicial data relating to different persons which is put together by automated means" (article 1(5)). The judicial data that is included in this coherent collection, for individuals, concerns the names, gender, address, place of birth, date of birth, personal identification numbers and nationality (article 6 (1) Decree Judicial and Criminal Records (*Besluit justitiële en strafvordelijke gegevens*). In addition, data relating to the criminal offence and any decisions made in that respect are considered part of the judicial documentation (see article 3 et seq. Decree Judicial and Criminal Records). Taking this into account, the Dutch Judicial and Criminal Records Act does not relate to the criminal investigation. Instead, it is concerned with

[73] Wet Politiegegevens 2007; Wet Justitiele en Strafvorderlijke Gegevens 2002

[74] Ira Helsloot, 'Evaluatie Wet Justitiële En Strafvorderlijke Gegevens' (Wodc.nl, 2013), p.31-32 <https://www.wodc.nl/binaries/2102-volledige-tekst_tcm28-72074.pdf> accessed 5 October 2020.

[75] ibid p.31-34.

ensuring that, after a criminal investigation has been conducted, the judicial documentation is sufficient so as to ensure a good criminal procedure.

4.2 DUTCH LEGAL FRAMEWORK

4.2.1 DUTCH POLICE DATA ACT (WET POLITIEGEGEVENS)

The Dutch Police Data Act (hereafter: Wpg) establishes rules for the processing of police data in relation to the rights and duties of the police and civilians. The scope is defined by article 2 of the Wpg. This article stipulates which processing activities fall under the material scope and which processing activities do not. Based on this provision, only the processing of police data by a competent authority included in a register or intentioned to be included in a register falls under its scope.[76]

The term "police data" is defined in the Wpg as *"all police data that is processed in order to fulfill the police task."*[77] "Processing" is defined in the Wpg as "*all processing activities regarding police data done in an automatic manner or non-automatic manner, such as collecting, structuring or storing of police data.*"

When the LED was implemented into Dutch national law in 2018, it effectively changed the scope of the Wpg in two ways. First, the definition of police data was narrowed down, as established in Article 1 of the Wpg. The definition now excludes several processing tasks carried out by police. Second, the scope of the legislation was extended to data processing by special investigating supervisors (*buitengewone opsporingsambtenaren*). Other processing was excluded from this legislation.[78]

As described in chapter 3, processing is considered lawful if it is based on a legal basis. It is relevant for this thesis to assess the Dutch legal basis for processing of personal data for criminal investigation purposes. The relevant legal basis for processing for criminal investigation purposes is adopted in the Wpg under article 3.[79] With respect to the processing of data under the Wpg,

[76] Article 2 Wpg.
[77] Article 1 Wpg.
[78] 'Wegwijzer Richtlijn Gegevensbescherming Opsporing En Vervolging' (*Rijksoverheid.nl*, 2018), p. 9-11 <https://www.rijksoverheid.nl/documenten/publicaties/2018/12/06/wegwijzer-richtlijn-gegevensbescherming-opsporing-en-vervolging> accessed 9 June 2020.
[79] 'Memorie Van Toelichting Wijziging Wet Politiegegevens En Justitiële En Strafvorderlijke Gegevens' (Rijksoverheid.nl, 2018), p.36 <https://www.rijksoverheid.nl/documenten/rapporten/2018/02/13/tk-mvt-wijz-wet-politiegegevens-en-justitiele-en-strafvorderlijke-gegevens> accessed 6 September 2020.

article 3, subsection 1, corresponds with the principle of lawfulness from article 8 of the LED.[80] Two conditions need to be met for the police to process data lawfully under this law. The processing needs to be necessary under article 3, subsection 1 (section 4.2.1.1) of the Wpg. The processing also has to be for the purposes set out in this law under article 3, subsection 1 (section 4.2.1.2). Both conditions will be further discussed below. The condition of processing that needs to be based on Union or Member State law is implemented into the Wpg and Bpg (Dutch Police Data Decree) as a whole. This entails that processing needs to be compliant with the Wpg. In other words, this condition is met if the processing falls under the scope of the Wpg.

4.2.1.1 NECESSITY WPG

As mentioned above, the criterion of necessity is laid down in article 3, subsection 1, of the Wpg. Pursuant to this provision, data can only be processed if it is necessary to fulfill the police task.[81] When assessing the explanatory report, no specific interpretation of the necessity requirement is given.[82] In order to interpret the term "necessary" correctly, case law could give some further guidance.

With regard to a law enforcement context, the Dutch Council of State deemed in 2018 that in order to assess necessity it should be assessed whether *"the processing of data serves the legitimate purpose of law enforcement."*[83] This could be seen as a test of effectiveness of the measure, one that is also addressed by the European laws and regulations as described in chapter 3 (hereafter: European sources).

In 2019, the Amsterdam District Court deemed that necessity should be assessed based on all relevant facts in combination with the principles of proportionality and subsidiarity, with reference to article 6 of the GDPR.[84] This is in line with the European sources as described in chapter 3.

As was described in chapter 3, three aspects of necessity were deemed to be essential to determine whether a processing activity is necessary, namely the effectiveness of the measure, the intrusiveness of the measure and the proportionality of the measure. When assessing the aforementioned Dutch cases, it becomes apparent that although not every aspect is being assessed

[80] 'Memorie Van Toelichting Wijziging Wet Politiegegevens En Justitiële En Strafvorderlijke Gegevens' (Rijksoverheid.nl, 2018), p.36 <https://www.rijksoverheid.nl/documenten/rapporten/2018/02/13/tk-mvt-wijz-wet-politiegegevens-en-justitiele-en-strafvorderlijke-gegevens> accessed 6 September 2020.
[81] N.W. Groenhart, 'Commentaar Op Art. 3 Wpg (Kluwer Navigator, 2019).
[82] 'Memorie Van Toelichting Wijziging Wet Politiegegevens En Justitiële En Strafvorderlijke Gegevens' (Rijksoverheid.nl, 2018), p.60 <https://www.rijksoverheid.nl/documenten/rapporten/2018/02/13/tk-mvt-wijz-wet-politiegegevens-en-justitiele-en-strafvorderlijke-gegevens> accessed 6 September 2020.
[83] [2018] Raad van State, 201601536/1/V3 and 201601554/1/V3, para. 18.
[84] [2019] Rechtbank Amsterdam, C/13/666009, para. 4.6-4.9.

by the Dutch Courts, some of the aspects seem to be interchangeably incorporated into the assessment of necessity of processing by the Dutch Courts. In the case ruled by the Dutch Council of State, effectiveness was tested in order to determine the necessity. In the case described above, ruled by the Amsterdam District Court, proportionality and subsidiarity were examined in order to determine the necessity.[85] Interestingly, it does seem that there is no generally accepted test for necessity in Dutch court.

4.2.1.2 PURPOSES IN THE WPG

Similar to article 8 of the LED, article 3 subsection 1 of the Wpg requires that police data may only be processed for the police task (*politietaak)*.[86] The police task includes the investigation of criminal offenses.[87] Therefore, the POC data processed falls within the scope of the purposes laid down in article 3 subsection 1 of the Wpg. From article 8 Wpg onward, the purposes of processing to which the Wpg applies are stated. An example is processing for the performance of the daily police task (as described in article 8 of the Wpg). If the data would be (further) processed for a different purpose that is not justifiable or compatible with the original purpose of the processing, this leads to unlawful processing.

4.3 DATA DERIVED FROM POCS BY POLICE

In this section the legal basis on which the Dutch police use the Register for criminal investigation purposes is further addressed.

4.3.1 LAWFUL TRANSFER OF POC DATA TO POLICE

With regard to the use of the Register, a request for the transfer of video footage of POCs by the police for criminal investigation purposes translates to an order by the public prosecutor based on Article 126nd of the Criminal Code of Procedure.[88] This is confirmed by the Dutch Supreme Court in 2010.[89] The Dutch Supreme Court decided that a request by the police to receive camera footage intended for the protection of persons, buildings, properties, matter, and production processes is a demand as established in Article 126 of the Dutch Criminal Code of Procedure.[90] Refusing such

[85] ibid para. 4.6-4.9.
[86] N.W. Groenhart, 'Commentaar Op Art. 3 Wpg (Kluwer Navigator, 2019).
[87] Article 1a Wpg & Article 3 Police Act.
[88] Article 126nd Dutch Criminal Code of Procedure.
[89] [2010] Hoge Raad, 08/03502 (Hoge Raad).
[90] ibid [2010] Hoge Raad.

an order would be a felony according to the Dutch Criminal Code of Procedure.[91] The consequences of refusing such an order are large (as denying an order could lead to prosecution as a POC owner) and thus, it would be expected that the POC owner is well informed about these consequences. However, the information provided by police to the POC owner with regard to this order is insufficient. Concerns have been raised by legal experts about the misinformation by Dutch police regarding the use of the Register.[92] However, it was made apparent by the Dutch police that they are not considering to stress the consequences of such a refusal more intensively.[93] With regard to the Register, the particular order for camera data to be ordered by police is not described properly on the police website or in any police press release.

4.3.2 ADDED VALUE CRITERION

To answer the main research question, this paragraph will further discuss the usage of POCs by Dutch police for criminal investigation. As mentioned in paragraph 4.2.1, the Wpg is applicable to processing of police data by a competent authority. Furthermore, the Wpg applies to the processing by a competent authority of police data which form part of a filing system or are intended to form part of a filing system. When processing data derived from POCs, the Wpg is applicable. The source of the data (namely the POCs) is included in a register (namely the Register). Also, it is highly likely that the police include the data derived from POCs into another filing system for criminal investigation purposes, and therefore this is assumed for the purpose of this thesis. However, the Dutch police do not explicitly use the criteria for lawfulness as stated in the Wpg. Based on a conversation with the spokesperson of the Dutch police and information found on their website, the police use "added value" as a criterion to decide whether or not they are allowed to process data from POCs.

As was established above, "added value" is not an established criterion for criminal investigation purposes (or other purposes) in the Wpg. This criterion seems rather vague, leaving quite a significant amount of leeway for a police officer to interpret whether or not he can request data from POCs.

[91] Article 189 Dutch Criminal Code.

[92] Houwing L, 'In beeld van een buitenwettelijk surveillancenetwerk' (Joop.bnnvara.nl, 2019) <https://joop.bnnvara.nl/opinies/in-beeld-van-een-buitenwettelijk-surveillancenetwerk> accessed 28 September 2020; this article links to a tweet sent by the chairman of Dutch Criminal Lawyers voicing his concerns. To this tweet the Dutch police responded by saying the given information on the order as mentioned in article 126nd was sufficient.

[93] The official twitter account of the Dutch police confirmed the information was correct as it was currently presented. To this day, no additional information issued by police is found on this matter.

With regard to the POCs registered in the Register, there is no case law available which sheds any light on how to interpret "added value". Since no case law exists on the interpretation, other reliable sources should perhaps give guidance as to the correct interpretation of this criterion. With regard to authoritative bodies, no guidelines have been issued by the legislator, the Dutch police or the Dutch Data Protection Authority for the interpretation of "added value". In January of 2020 the Dutch parliament did ask some questions in parliament with regard to the requirement of lawful processing. The parliament was curious if the principle of lawful processing was being respected in data being derived from POCs by Dutch police.[94] Namely, the legal basis of data processing with regard to digital doorbells. The Minister of Justice and Security responded by stressing that if the doorbell was registered into the Register, the police could only receive the footage that was stored if it had "actual added value". Interestingly, the criteria of necessity and purposefulness were not addressed in that context nor was the "added value" further explained.[95]

Considering the broadness of the term, the lack of further information on how the term is applied, leaves it uncertain for Dutch citizens when the police will be able to request the data of their POCs. This ambiguity will be further discussed in chapter 5.

4.4 FUNCTION CREEP

When using data derived from POCs registered in the Register, the threat of function creep is conceivable. Function creep in this context is the expansion of a system or technology beyond its original purpose.[96] The threat of function creep is conceivable because it is unclear how to interpret the "added value" criterion correctly. Due to this, discrepancies in the interpretation of when data derived from POCs may be processed by police could occur. This might lead to function creep.

An example of function creep was the use of environmental cameras (cameras that can detect license plates of diesel-powered cars to determine if the car is too old to enter the city center of Amsterdam) by Dutch police. The purpose of the environmental cameras was to detect whether

[94] 'Antwoorden Kamervragen Over Het Bericht Gratis Deurbellen Tegen Criminaliteit Het Twijfelachtige Effect En De Privacyzorgen' (Rijksoverheid.nl, 2020) <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/10/antwoorden-kamervragen-over-het-bericht-gratis-deurbellen-tegen-criminaliteit-het-twijfelachtige-effect-en-de-privacyzorgen> accessed 7 September 2020.

[95] 'Antwoorden Kamervragen Over Het Bericht Gratis Deurbellen Tegen Criminaliteit Het Twijfelachtige Effect En De Privacyzorgen' (Rijksoverheid.nl, 2020) <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/10/antwoorden-kamervragen-over-het-bericht-gratis-deurbellen-tegen-criminaliteit-het-twijfelachtige-effect-en-de-privacyzorgen> accessed 7 September 2020.

[96] Bert-Jaap Koops, 'The Concept Of Function Creep' (Papers.ssrn.com, 2020), p. 1-2, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547903> accessed 15 July 2020.

criminals and stolen vehicles were entering the municipality of Amsterdam.[97] This intended purpose was, however, temporary and limited to the time of the coronation of King Willem Alexander—at least in theory. In practice, the Amsterdam police department continued to use these cameras for criminal investigation purposes after the coronation.[98] The data processed for these criminal investigations were not related to the coronation or processed for a compatible purpose; therefore, this use of cameras seems rather extensive. This use went unnoticed for several years. In 2017, however, the Municipal Privacy Commission (*de gemeentelijke privacycommissie)* determined that such use was not compliant with the applicable Dutch data protection standards.[99] According to literature, function creep is inevitable, especially in law enforcement, because investigators often demand all potential information available to them regarding a specific case.[100] If one were to complain to them about wanting this information, it would create suspicion of criminal behavior.[101]

In a legal context, function creep resonates with the concept of abuse of power. In other words, it is an exercise of authority in the public interest but not for the purpose it was intended for. Though the exercise of authority may be well-intentioned, it is problematic if the authority deviates from the original purpose with regard to a vital concept such as data processing. If such use for other purposes is outside the scope of the purposes laid down in articles 1 LED and article 1 subsection a Wpg, this is not compliant with these acts (article 8 LED and article 3 subsection 1 Wpg). Data protection laws have introduced a compatibility test for data processing in order to keep secondary

---

[97] Kristel Van Teeffelen, 'Privacy Settings' (*Trouw.nl*, 2019) <https://www.trouw.nl/binnenland/politie-amsterdam-loerde-onterecht-in-data-van-milieucamera-s~bba1398a/?referer=https%3A%2F%2Fwww.google.com%2F> accessed 25 March 2020. These environmental cameras were originally used to prohibit old diesel vehicles from entering the city. See also: Gemeente Amsterdam, 'Milieuzone' (Amsterdam.nl, 2019) <https://www.amsterdam.nl/parkeren-verkeer/milieuzone/> accessed 23 November 2019.

[98] ibid.

[99] Gemeente Amsterdam, 'Commissie Persoonsgegevens Amsterdam' (Amsterdam.nl, 2019) <https://www.amsterdam.nl/bestuur-organisatie/organisatie/overige/adviesraden/commissie-persoonsgegevens-amsterdam/> accessed 23 November 2019. The "privacycommissie" advises the municipality in their privacy-related policies.

[100] M.S. De Vries, 'Hoe Waarschijnlijk Is Function Creep?' (2011), p.22, < https://www.wodc.nl/binaries/jv1108-volledige-tekst_tcm28-77152.pdf> accessed 16 January 2020; see also: Chris Pounder, 'Nine Principles For Assessing Whether Privacy Is Protected In A Surveillance Society' (Philpapers.org, 2008), p.1-22 <https://philpapers.org/rec/POUNPF-2> accessed 14 October 2020.

[101] Ruth Halperin, 'A Roadmap For Research On Identity In The Information Society' (Eprints.lse.ac.uk, 2008) <http://eprints.lse.ac.uk/23548/1/A_roadmap_for_research_on_identity_in_the_information_society(LSERO).pdf> accessed 25 March 2020.

use of data in check.[102] However, the aforementioned example above shows that this compatibility test is not always (correctly) performed.

4.5 CONCLUSION

This chapter has made an analysis of the relevant Dutch legal framework regarding lawful processing. Even before the implementation of the LED, the principle of lawful processing was enshrined in the Wpg. Based on the Wpg, two conditions need to be met for lawful processing, namely the necessity and the purpose of the processing. The interpretation of necessity is unfortunately not extensively addressed by the explanatory report of the Wpg, but the case law gives some explanation. In the examples used in this chapter, even though the Dutch Court referred to the European sources as described in chapter 3, it continues to use the criteria of chapter 3 interchangeably without one generally accepted test for necessity.

However, because the Dutch police use a different criterion for the use of POCs, namely "added value", the translation between the lawful processing principle and this "added value" criterion could cause an issue. For the processing to be lawful, it requires a test of necessity and purposefulness. It is questionable if the condition of "added value" for the police to use POCs respects these tests in that same strict sense.

[102] Bert-Jaap Koops, 'The Concept Of Function Creep' (Papers.ssrn.com, 2020), p. 13, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547903> accessed 15 July 2020.

CHAPTER 5: DUTCH POLICE COMPLIANCE WITH EUROPEAN AND DUTCH STANDARD OF LAWFUL PROCESSING

5.1 INTRODUCTION

This chapter will ascertain whether the use of POCs by the Dutch police is compliant with the principle of lawfulness under the LED and the Wpg. In making this assessment, the principles of lawful processing of personal data under the LED (section 5.2) and Wpg (section 5.3) will be discussed. Afterwards, the compliance of the "added value" criterion will be assessed (section 5.4). Based on such assessment, recommendations will be made (section 5.5). This chapter ends with a conclusion (section 5.6).

5.2 EUROPEAN STANDARD OF LAWFUL PROCESSING OF PERSONAL DATA

As described in chapter 3, article 8 of the LED states when processing of personal data by law enforcement authorities is lawful.[103] Based on this article, three conditions have to be met for a processing activity to be lawful: firstly, the processing of personal data must be "*necessary for the performance of a task carried out by a competent authority"*. Secondly, the processing must be carried out for the *purposes* set out in article 1(1) LED. Finally, the processing must be based on Union or Member State law. While these last two conditions are rather clear, the condition of necessity leaves room for interpretation. In accordance with European sources as described in chapter 3, it was determined that in order to assess the necessity as accurately as possible, three aspects have to be taken into account: firstly, the effectiveness of the measure to accomplish the purpose.[104] Secondly, the intrusiveness of the measure with regard to the right to the protection of personal data. Finally, if the measure is proportionate in relation to the infringement of the aforementioned right.

5.3 DUTCH STANDARD OF LAWFUL PROCESSING

As described in chapter 4, article 3 of the Wpg corresponds with the principle of lawful processing as stated in article 8 of the LED. The conditions for lawful processing correspond with the

[103] Article 8 LED.

[104] 'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (Edps.europa.eu, 2017), p. 5 <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 10 September 2020. See also: CJEU, C-524/6, Huber, 16 December 2008 and CJEU, C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014.

conditions in the LED, namely necessity and processing for the purposes set out in 1 subsection a Wpg. With respect to the third element of lawfulness under the LED, i.e. the requirement that processing is based on Member State or Union law, it can be noted that the Wpg is an implementation of the requirement that processing is based on, in this case, Member State law. Again, the term necessity is not clarified in the Wpg leaves room for interpretation. The Dutch Courts attempted on multiple occasions to interpret this term. In accordance with the European sources as described in chapter 3, the Dutch Courts assessed necessity in general unison, but did interchange some of the important aspects when assessing the necessity. In the examples given in chapter 4, the Dutch Courts assessed necessity with regard to the principles of proportionality and subsidiarity as well as with regard to serving the purpose of law enforcement.
Because of the similarity between the Dutch assessment of the necessity and the European sources as described in chapter 3, the use of POCs by Dutch police for criminal investigation purposes will be assessed using the three conditions mentioned in chapter 3: effectiveness, intrusiveness and proportionality.

5.4 ASSESSMENT OF COMPLIANCE

The Dutch police's use of POCs for criminal investigation purposes can be compliant with the European standard of lawfulness if the use is necessary and used for a purpose stated in the Wpg (as described above). However, the Dutch police use "added value" as a criterion to determine whether or not they can process data derived from POCs. Therefore, it needs to be analyzed whether this criterion is compliant with the necessity-requirement as laid down in the European and Dutch principle of lawfulness and the purpose limitation-requirement that is linked to this principle.

5.4.1 NECESSITY

Based on the analysis in the previous chapters, the three following assessments need to be carried out to conduct a proper 'necessity-test': a test of the effectiveness of the processing activity, a test of the intrusiveness of the processing activity and a test of the proportionality of the processing activity. Firstly, it needs to be assessed whether the criterion of "added value" contains a test of the effectiveness of the processing activity to achieve the purpose determined by the police. Because the processing must have some effect on achieving the purpose of criminal investigation, it appears that the criterion of "added value" contains a test of effectiveness of the processing of

personal data. Based on the findings in the previous chapters, it is not necessary for the processing to be the most effective measure to achieve the purpose.

Secondly, it needs to be assessed if the criterion of "added value" contains a test of the intrusiveness of the processing activity. In other words, the level of intrusiveness of the processing of personal data with regard to the privacy of the data subject needs to be assessed.[105] The test whether the processing of personal data has "added value" does not take the intrusiveness of the processing activity into account. It appears that "added value" is formulated in a positive sense, meaning that the police assess whether the processing *may* lead to important information for the investigation. However, the test of intrusiveness intends to analyze whether the processing of the personal data is the least intrusive measure with regard to the right to the protection of personal data of the data subject involved. Here, the criterion of "added value" delineates from the principle of lawfulness. Before the processing of the data, in other words before the police analyzes the POC footage, the police are not able to determine what kind of personal data the footage contains. Taking this into account, when processing POC footage the Dutch police will most likely process personal data of multiple data subjects, most of which they will not need for the criminal investigation purpose. To protect the right to the protection of personal data of these data subjects, it is desirable that a test of intrusiveness is always applied when using data derived from POCs.[106] Because of the possible breach of the right to protection of personal data of multiple data subjects, the use of POC data should only be used when it is the least intrusive measure at hands, or when it is the only measure left to achieve the purpose of the criminal investigation.

Lastly, it needs to be assessed if the criterion of "added value" contains a test of proportionality of the processing activity. This test of proportionality should always be incorporated in police conduct if fundamental rights are infringed upon.[107] Whether the processing of personal data is proportionate in relation to the infringement of the privacy of the data subjects involved, will most likely rely on the severity of the crime under investigation. It is conceivable that the interest of the

---

[105] 'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (Edps.europa.eu, 2017), p.16 <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 10 September 2020

[106] 'THE EDPS VIDEO-SURVEILLANCE GUIDELINES' (Edps.europa.eu, 2010), p. 17-19 <https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> accessed 10 September 2020.

[107] Dorien Taeymans, 'EDPB: Richtlijnen Over De Verwerking Van Persoonsgegevens Door (Bewakings)Camera'S' (Navigator.nl, 2020) <https://www.navigator.nl/document/id3072568749b44eeeb2d5ef847b3ff273?h1=(camera),(%27s),(rechtmatigheid),(politie)&ctx=WKNL_CSL_26&idp=LegalIntelligence> accessed 16 October 2020. See also: Sander Flight (Sanderflight.nl, 2016), p. 83 <http://sanderflight.nl/wp-content/uploads/2016/08/2016-Flight-beeldtechnologie-Justitiele-Verkenningen.pdf> accessed 16 October 2020.

police to solve a murder will outweigh the infringement of the right to the protection of personal data of the data subjects shown on the POC footage. However, when a small misdemeanor is under investigation, such as not removing fecal waste deposited by dogs, it is likely that the right to the protection of personal data of the data subjects should be respected more. The criterion of "added value" does not seem to incorporate such an assessment. No distinction has been made by Dutch police between the severity of crimes with regard to the processing of data derived from POCs. Therefore, the criterion appears to only assess whether the processing might lead to more information to solve the investigation, no matter the severity of the crime, a felony or a misdemeanor. It has to be stated that it is troublesome for the police to correctly assess the different types of interests of POC owners and data subjects, since these interests seem to have a different weight to them. One interest should prevail more often than another. For example, in case of a murder the interest in public safety will most likely have more value than the interest in the protection of personal data. In other case, where the value of the interests at stake are not as clear, the right outcome could be difficult to determine. This issue has been confirmed by the CJEU.[108] Based on the arguments above, it can be concluded that the criterion of "added value" is not in compliance with the necessity requirement of the principle of lawfulness.

5.4.2 PURPOSE

It needs to be addressed whether the criterion of "added value" ensures that the processing of footage of POCs will only be used for the purposes of article 1(1) LED. Given that Member States are required to provide for processing to be lawful only if and to the extent that such processing is carried out for the purposes set out in article 1(1) LED (article 8(1) LED), using POC footage would be unlawful if it is used for purposes other than article 1(1) LED. In that respect, it has been indicated that the Dutch police solely processes POC footage in case of a police investigation.[109] Considering that article 1 (1) refers to the processing of personal data by competent authorities for the purposes of the investigation of criminal offences, it would seem that the application of the criterion of "added value" by the police will be for purposes of article 1(1) LED. Taking this into

[108] Bart Custers, 'Nieuwe Online Opsporingsbevoegdheden En Het Recht Op Privacy: Een Analyse Van De Wet Computercriminaliteit III' (Openaccess.leidenuniv.nl, 2018), p. 112 <https://openaccess.leidenuniv.nl/handle/1887/67699> accessed 15 October 2020; see also: CJEU, C-293/12 and C-594/12, Digital Rights Ireland, 8 April 2014.

[109] "Camera in Beeld" (Politie.nl, 2019) <https://www.politie.nl/themas/camera-in-beeld.html?sid=afedd054-0221-49a3-acab-58aa68496ad3> accessed 4 October 2020. See also the purpose as mentioned on the website of the police and therefore the purpose that the police want to achieve is a purpose of 'criminal investigation'.

account, the “added value” criterion is compatible with article 8(1) LED in the sense that it ensures that the POC footage will only be processed for purposes as laid down in article 1(1) LED.

5.5 RECOMMENDATIONS

In this section certain recommendations for the four relevant actors in this thesis are made. These actors are: the Dutch police, the POC owners, the Dutch legislator and the camera manufacturers.

5.5.1 DUTCH POLICE

Firstly, it needs to be made clear to POC owners by Dutch police what the data protection implications are when registering a POC for the Register. A POC owner cannot refuse an order by police for footage, as further explained in chapter 4. Therefore, the Dutch police should be obliged to provide POC owners with extensive information about the implications that are present when registering their POC into the Register and what this might mean for their right to data protection and that of other data subjects. Additionally, the Dutch police should issue strict guidelines for the use of POCs for their criminal investigation purposes in order to create legal certainty for POC owners and data subjects.

5.5.2 THE POC OWNERS

Secondly, POC owners should be more careful when registering their camera for the Register. The interest of POC owners when installing such a camera could be an interest that is not directly compatible with the interest the Dutch police has. When POC owners are well informed, they should assess whether in any occasion they are comfortable with letting the public safety prevail above their own interest, when they installed their camera. This is especially relevant when considering the fact that data subjects recorded on the POCs also could have their right to protection of personal data infringed when POC footage is processed by police. However, this can only be done properly, after receiving extensive information from the police as mentioned above in paragraph 5.4.3.1.

5.5.3 DUTCH LEGISLATOR

Thirdly, the Dutch legislator has to improve the legal certainty by means of legislation. The use of POCs by police for criminal investigation purposes should be bound to certain rules in the criminal domain. An example of this would be to introduce a law or amend the Wpg in such a way that it

states under what circumstances the Dutch police should be able to use POCs for these purposes. For example, it should state what the minimum penalty of custody of a crime under investigation should be, whether all other means need to be exhausted etc.

5.5.4 THE CAMERA MANUFACTURERS

Finally, camera manufacturers play a role in the use of POCs as well. The lack of knowledge about how to use and place a camera by consumers can result in camera footage that may be unnecessarily intrusive with regards to the right to data protection of data subjects other than the POC owners. This could lead to POC footage that cannot be lawfully processed by the police for criminal investigation purposes under the principle of lawfulness. As such, the unawareness of consumers can potentially limit the effectiveness of the Register for criminal investigation purposes. Therefore, manufacturers could inform consumers about the privacy implications of using POCs and how to limit these e.g. how to prevent recording a public road. This could lead to less intrusive footage that is more useful for criminal investigation purposes.

5.6 CONCLUSION

This chapter has ascertained whether the use of POCs by the Dutch police is compliant with the principle of lawfulness under the LED and the Wpg. In assessing this compliance, the principles of lawful processing of personal data under the LED and Wpg have been briefly set out. After having done so, it became apparent that the Dutch data protection standards, as laid down in the Wpg, are similar to the data protection standards under EU law. Such similarity relates to the requirement of necessity and the circumstance that processing can only be done for exercising the police task. With respect to the third element of lawfulness under the LED, i.e. the requirement that processing is based on Member State or Union law, it can be noted that the Wpg is an implementation of the requirement that processing is based on, in this case, Member State law. Taking into consideration the similarities of the criterion of necessity and the purposes for which data can be processed, the test whether the use of POC footage is compliant with these two elements under the LED and the Wpg is, essentially, the same.

When assessing the use of POCs by Dutch police for criminal investigation purposes, the starting-point is that the Dutch police uses the criterion of “added value”. In this chapter it has been concluded that the use of POC footage will be compliant with the purposes set out in the LED and the Wpg. More interesting is the conclusion that the criterion of necessity is not properly included in the “added value” criterion. This is due to the circumstance that the intrusiveness and

proportionality tests are not necessarily integrated properly, in the sense that there are no safeguards in the application of this criterion that ensure that such tests are incorporated in making the assessment whether to use POC footage or not. The consequence of this uncertainty regarding the incorporation of the intrusiveness and proportionality tests is that the "added value" criterion is not necessarily compliant with the principle of lawfulness. As such, it is conceivable that the "added value" criterion is met too easily without taking the infringement of the right to the protection of personal data of the data subjects into account.

Having concluded that it is, at present, uncertain whether the use of the "added value" criterion results in outcomes that are compatible with the requirement of necessity under the principle of lawfulness, recommendations have been made for the Dutch police, the POC owners, the Dutch legislator and the camera manufacturers. Such recommendations could be made by means of (formal) guidelines to be issued for the use of POCs by the Dutch police. Moreover, the legislator could introduce laws that clarify the application of the "added value" criterion. The purpose of such guidelines or clarifications should be to ensure that the tests of intrusiveness and proportionality are incorporated in the criterion of "added value". Finally, with respect to the possibility of increasing the use of POCs for criminal investigation purposes, another recommendation was that camera manufacturers should inform consumers in order to ensure that the POC footage is less intrusive.

CHAPTER 6: SUMMARY AND CONCLUSION

The research question of this thesis was:

> *Does the processing of personal data collected through privately owned cameras (POCs) by Dutch police for criminal investigation purposes comply with the principle of lawfulness of data protection (as stated in the Law Enforcement Directive)?*

In answering this research question, the first step has been to describe the different type of POCs that may be used by the Dutch police. In particular the Register has been described.
The next step has been to examine the principle of lawfulness under the LED and the Wpg. The LED was discussed in chapter 3, the Wpg in chapter 4. With respect to the principle of lawfulness under the LED, three conditions have to be met in order for processing to be lawful: necessity of processing, the processing must be done for purposes as set out in article 1(1) LED, and the processing must be based on Member State or Union law. With respect to the condition of necessity, three aspects are relevant: effectiveness, intrusiveness and proportionality of the measure. This means that, under the necessity requirement, processing must occur in such a way that it is effective, not too intrusive and applied in a proportionate way.
Besides the LED, also the Wpg has been taken into account. The Wpg incorporates the European principle of lawfulness in its provisions. This principle of lawfulness corresponds with the principle of lawfulness under the LED, as confirmed in the explanatory report of the Wpg. Similarly to the LED, the requirement of necessity also applies, while the processing must also be done for specifically listed purposes in the Wpg. With respect to the requirement of necessity, it has been concluded that the interpretation of such requirement under the Wpg is similar to the interpretation given to the requirement of necessity under the LED. Taking this into consideration, it seems that the principle of lawfulness under the Wpg corresponds with the same principle in the LED.
Additionally, chapter 4 also describes under what circumstances the Dutch police will process POC footage. In that respect, it has become apparent that the main criterion for the Dutch police to determine whether POC footage of the Register can be accessed (and thus processed) is whether such POC footage has "added value" (*daadwerkelijke meerwaarde*) for criminal investigation purposes. With respect to this "added value" criterion, it has been concluded that it is not derived from the LED or the Wpg. Given the lack of legal basis in the LED and the Wpg for the "added

value" criterion, the compliance of the "added value" criterion with the principle of lawfulness is, essentially, dependent on an assessment of the interpretation and application of such criterion in practice.

Having established the legislative framework for determining whether the processing of data through POCs by Dutch police for criminal investigation purposes complies with the principle of lawfulness of data protection, chapter 5 assessed such compliance. In doing so, the application of the criterion of "added value" was compared with the principle of lawfulness under the LED (and the Wpg). In that respect, it has been concluded that the criterion of "added value" does not necessarily comply with the principle of lawfulness under the LED because the aspects of intrusiveness and proportionality are not necessarily part of the way in which the "added value" criterion is applied. As such, the "added value" is not compliant with (two aspects of) the necessity criterion of the principle of lawfulness under the LED.

Taking into account the findings of chapter 5, the answer to the research question must be that the processing of data through POCs by Dutch police for criminal investigation purposes does not necessarily comply with the principle of lawfulness of data protection (as stated in the LED).

In order to fix the potential incompatibility of such processing with the principle of lawfulness under the LED, recommendations have been made in chapter 5.

BIBLIOGRAPHY

LEGISLATION

General Data Protection Regulation (EU) 2016/679

Law Enforcement Directive (EU) 2016/680

EU Charter on Fundamental Rights of the European Union

Grondwet

Wetboek Van Strafrecht

Politiewet

Wet politiegegevens

Wet justitiele en strafvorderlijke gegevens

BOOKS

George Orwell, 1984 (Enwikabooks 1949)

'The Right To Property Under The European Convention On Human Rights' (Rm.coe.int 2007)

C Kelk and F. de Jong, Studieboek Materieel Strafrecht (5th edn, Kluwer 2013)

FRA, Handbook On European Data Protection Law (2018)

BOOK SECTIONS

Lilian Edwards and Charlotte Waelde, Law And The Internet (Hart 2008)

Prof. J.B.M. Vranken, 'Kenmerken Van Juridisch Dogmatisch Onderzoek' (Asser/Vranken Algemeen 2014)

Mr. H.L.C. Maessen, Handboek Strafzaken (2015)

P. Mevis, Parlementaire Geschiedenis Modernisering Wetboek Van Strafvordering (Boom 2017)

CASE LAW

Dutch Supreme Court 1995, Zwolsman, NJ 1996, 249 (Hoge Raad)

Dutch Supreme Court 2010, 08/03502 (Hoge Raad)

Dutch Supreme Court 2017, 16/02186 (Hoge Raad)

Dutch Council of State 2018, 201601536/1/V3 and 201601554/1/V3 (Raad van State)

Central Court of Appeal 2018, 16/6346 WSFBSF (Centrale Raad van Beroep).

Dutch Lower Court 2019, C/13/666009 (Rechtbank Amsterdam)

Dutch Lower Court 2019, UTR 18/2879 (Rechtbank Midden-Nederland)

Dutch Lower Court 2019, 18/1556 (Rechtbank Midden-Nederland)

CJEU 2003, Bodil Lindqvist, C-101/01

CJEU 2003, C-101/01, Bodil Lindqvist

CJEU 2008, C-524/6 Huber

CJEU 2011, C-468/10 ASNEF

CJEU 2014, C-212/13 Ryneš

CJEU 2014, C-293/12 and C-594/12, Digital Rights Ireland

CJEU 2015, C-62/14, Gauweiler

ARTICLES

'Cameratoezicht In Nederland; Een Schets Van Het Nederlandse Cameralandschap' (2013) <https://www.researchgate.net/publication/320555155_Cameratoezicht_in_Nederland_een_schets_van_het_Nederlandse_cameralandschap> accessed 2 April 2020

Caruana M, 'The Reform Of The EU Data Protection Framework In The Context Of The police And Criminal Justice Sector: Harmonisation, Scope, Oversight And Enforcement' (*Www-tandfonline-com.tilburguniversity.idm.oclc.org*, 2017), <https://www-tandfonline-com.tilburguniversity.idm.oclc.org/doi/pdf/10.1080/13600869.2017.1370224?needAccess=true> accessed 7 June 2020

Colin J Raab C, 'Revisiting The Governance Of Privacy: Contemporary Policy Instruments In Global Perspective' (*Onlinelibrary-wiley-com*, 2018) <https://onlinelibrary-wiley-com.tilburguniversity.idm.oclc.org/doi/full/10.1111/rego.12222> accessed 14 June 2020

Engberts B, 'Sensing Door De Politie En Publiek-Private Samenwerking: Operationele Noodzaak' (*Politieacademie.nl*,

Custers B 'Nieuwe Online Opsporingsbevoegdheden En Het Recht Op Privacy: Een Analyse Van De Wet Computercriminaliteit III' (Openaccess.leidenuniv.nl, 2018), <https://openaccess.leidenuniv.nl/handle/1887/67699> accessed 15 October 2020 2016) <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/92748.pdf> accessed 14 June 2020

Finch K and Tene, O, 'Smart Cities: Privacy, Transparency, And Community' (Papers.ssrn.com, 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3156014> accessed 23 November 2019

Galič M, 'Surveillance, Privacy And Public Space In The Stratumseind Living Lab: The Smart City Debate, Beyond Data' (*Papers.ssrn.com*, 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435518> accessed 14 June 2020

Groenhart N W , 'Commentaar Op Art. 3 Wpg (Kluwer Navigator, 2019)

Hert P de, 'The New police And Criminal Justice Data Protection Directive' (Pure.uvt.nl, 2016), <https://pure.uvt.nl/ws/portalfiles/portal/19816258/pdh16_vpdirective_corrected_.pdf> accessed 7 June 2020; see also: Article 8 (1) Law Enforcement Directive

Hartzog W, 'Inefficiently Automated Law Enforcement' (Digitalcommons.law.msu.edu, 2015), <http://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1149&context=lr> accessed 17 July 2020

Jasserand C, 'Subsequent Use Of GDPR Data For A Law Enforcement Purpose: The Forgotten Principle Of Purpose Limitation?' (ssrn.com, 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230347> accessed 12 June 2020

Koekkoek A K, 'De Grondwet: Een Systematisch En Artikelsgewijs Commentaar' (Tilburg University Research Portal, 2000) <https://research.tilburguniversity.edu/en/publications/de-grondwet-een-systematisch-en-artikelsgewijs-commentaar> accessed 22 February 2020

Koning M, 'Het Recht Op Bescherming Van Persoonsgegevens In De Europese En Nationale Rechtsorde Na Lissabon' (Merelkoning.nl, 2017), https://merelkoning.nl/wp-content/uploads/2017/12/Het-recht-op-bescherming-van-persoonsgegevens-in-de-Europese-en-nationale-rechtsorde-na-Lissabon-m.koning.pdf accessed 29 February 2020

Koops B J, 'Beschouwing Rapport Commissie-Koops: Strafvordering In Het Digitale Tijdperk - Recht.Nl' (*Recht.nl*, 2019) <https://www.recht.nl/nieuws/strafrecht/170190/beschouwing-rapport-commissie-koops-strafvordering-in-het-digitale-tijdperk/> accessed 14 June 2020

Koops B J, 'The Concept Of Function Creep' (Papers.ssrn.com, 2020), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547903> accessed 15 July 2020.

Kulk S 'Juridische Aspecten Van Algoritmen Die Besluiten Nemen Een Verkennend Onderzoek' (Wodc.nl, 2020), <https://www.wodc.nl/binaries/2947_volledige_tekst_tcm28-452340.pdf> accessed 26 August 2020

Leiser M R, The Law Enforcement Directive: Conceptual Chalenges Of EU LAW Enforcement Directive' (2019), <https://openaccess.leidenuniv.nl/bitstream/handle/1887/79246/2019_Leiser_en_Custers_Submitted_LED_paper_EDPL.pdf?sequence=1> accessed 28 April 2020

Moerman E, 'Burgers In Het Digitale Opsporingstijdperk' (*NJB*, 2019) <https://www.njb.nl/magazines/njb-2-(2019).30847.lynkx> accessed 21 January 2020

Nissenbaum H 'Privacy As Contextual Integrity' (NYU Scholars, 2004) <https://nyuscholars.nyu.edu/en/publications/privacy-as-contextual-integrity> accessed 26 August 2020

Pounder C 'Nine Principles For Assessing Whether Privacy Is Protected In A Surveillance Society' (Philpapers.org, 2008), <https://philpapers.org/rec/POUNPF-2> accessed 14 October 2020

Prenzler T, 'Public-Private Crime Prevention Partnerships' (2012), <https://www.researchgate.net/publication/304790628_Public-Private_Crime_Prevention_partnerships?enrichId=rgreq-5050e1235377443b67566a98ca7da189-XXX&enrichSource=Y292ZXJQYWdlOzMwNDc5MDYyODtBUzo1Mjg4ODU0MDMxMzE5MDRAMTUwMzEwNzUxNDc1Mw%3D%3D&el=1_x_3&_esc=publicationCoverPdf> accessed 24 April 2020

Rinner B, 'Toward Pervasive Smart Camera Networks' (*Www-sciencedirect-com.tilburguniversity.idm.oclc.org*, 2009) <https://www-sciencedirect-com.tilburguniversity.idm.oclc.org/topics/engineering/smart-camera> accessed 22 April 2020

Rooij A E van, 'De Gemeentestem, Privacy In Het Semipublieke Domein' (*Navigator.nl*, 2017), p. 700, <https://www.navigator.nl/document/idd60d403da63c4864916de6fdb8f3819e/de-

gemeentestem-privacy-in-het-semipublieke-domein?ctx=WKNL_CSL_29> accessed 24 April 2020

Sajfert J and Quintel T, 'Data Protection Directive (EU) 2016/680 For police And Criminal Justice Authorities' (*Papers.ssrn.com*, 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873> accessed 5 April 2020

Schuilenberg M, 'Politie-Webcrawlers En Predictive Policing' (*Marcschuilenburg.nl*, 2016), <http://marcschuilenburg.nl/wp-content/uploads/2017/06/Politie-webcrawlers.pdf> accessed 11 June 2020

Schutgens R J B, "De algemene taakomschrijving van de politie en de waarde(n) van het legaliteitsbeginsel' (*Repository.ubn.ru.nl*, 2015), <https://repository.ubn.ru.nl/bitstream/handle/2066/149852/149852.pdf?sequence=1> accessed 28 April 2020

Sloot B van der 'How To Assess Privacy Violations In The Age Of Big Data? Analysing The Three Different Tests Developed By The Ecthr And Adding For A Fourth One' (Bartvandersloot.com, 2015), <https://bartvandersloot.com/onewebmedia/How_to_assess_privacy_violations_in_the.pdf> accessed 29 August 2020

Sloot B van der, 'Het Gegevensbeschermingsrecht Op De Schop: Noodzaak Of Afbraak?' (*Bartvandersloot.nl*, 2017) <https://bartvandersloot.nl/onewebmedia/Het_gegevensbeschermingsrecht_op_de_scho.pdf> accessed 4 April 2020

Sloot B van der, "The practical and theoretical problems with balancing', (*Bartvandersloot.com*, 2016) <https://www.bartvandersloot.com/onewebmedia/Balancing.pdf> accessed 7 June 2020

Sloot B van der, 'Where Is The Harm In A Privacy Violation?' (Bartvandersloot.com, 2017), <https://bartvandersloot.com/onewebmedia/where%20is%20the%20harm.pdf> accessed 26 August 2020

Smits J, "What is legal doctrine? On the aims and methods of legal-dogmatic research', Maastricht European Private Law Institute Working Paper (2015) 06

Taeymans D 'EDPB: Richtlijnen Over De Verwerking Van Persoonsgegevens Door (Bewakings)Camera'S' (Navigator.nl, 2020)

<https://www.navigator.nl/document/id3072568749b44eeeb2d5ef847b3ff273?h1=(camera),(%27s),(rechtmatigheid),(politie)&ctx=WKNL_CSL_26&idp=LegalIntelligence> accessed 16 October 2020

Timan T Newell B and Koops BJ 'Privacy In Public Space (Bookdepository.com, 2017) <https://www.bookdepository.com/Privacy-Public-Space-Tjerk-Timan/9781786435392> accessed 26 August 2020

Vries M S de, 'Hoe Waarschijnlijk Is Function Creep?' (2011), <https://openaccess.leidenuniv.nl/bitstream/handle/1887/18313/jv1108compleet.pdf?sequence=6> accessed 16 January 2020

Wagner B, 'Liable, But Not In Control? Ensuring Meaningful Human Agency In Automated Decision-Making Systems' (2019), <https://onlinelibrary.wiley.com/doi/pdf/10.1002/poi3.198> accessed 31 March 2020

Welsh B and Farrington D 'Crime Prevention Effects Of Closed Circuit Television: A Systematic Review' (2002) accessed 26 August 2020

Završnik A, 'Criminal Justice, Artificial Intelligence Systems, And Human Rights' (*Springer Link*, 2020) <https://link.springer.com/article/10.1007/s12027-020-00602-0> accessed 2 April 2020

Zhao B 'Exposure And Concealment In Digitalized Public Spaces' (Rug.nl, 2017) <https://www.rug.nl/research/portal/en/publications/exposure-and-concealment-in-digitalized-public-spaces(ff4c6eb8-0fbe-4428-b985-13b057c7615b).html> accessed 26 August 2020

REPORTS

'Opinion Of The European Data Protection Supervisor On The Amended Proposal For A Regulation Of The European Parliament And Of The Council On The Establishment Of 'EURODAC' For The Comparison Of Fingerprints For The Effective Application Of Regulation' (*Edps.europa.eu*, 2012), <https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf> accessed 11 June 2020

'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (2017), <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf>

'Wegwijzer Richtlijn Gegevensbescherming Opsporing En Vervolging' (*Rijksoverheid.nl*, 2018), <https://www.rijksoverheid.nl/documenten/publicaties/2018/12/06/wegwijzer-richtlijn-gegevensbescherming-opsporing-en-vervolging> accessed 9 June 2020

'Handleiding Algemene Verordening Gegevensbescherming En Uitvoeringswet Algemene Verordening En Uitvoeringswet Algemene Verordening Gegevensbescherming Gegevensbescherming' (Autoriteitpersoonsgegevens.nl, 2018), <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf> accessed 9 June 2020

'Inzet Van Sensordata Voor Leefbaarheid En Veiligheid | Rathenau Instituut' (*Rathenau.nl*, 2019) <https://www.rathenau.nl/nl/digitale-samenleving/inzet-van-sensordata-voor-leefbaarheid-en-veiligheid>

'Guidelines 3/2019 On Processing Of Personal Data Through Video Devices' (*Edpb.europa.eu*, 2019) <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf>

Boogers J, '101 Vragen Over Opsporingsbevoegheden' (Politieacademie.nl, 2003), <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/5445.pdf> accessed 27 July 2020

Delacroix S, 'Algorithms In The Criminal Justice System' (*The Law Society*, 2019), <https://www.lawsociety.org.uk/support-services/research-trends/documents/algorithm-use-in-the-criminal-justice-system-report/> accessed 12 June 2020

Flight S 'Politie En Beeldtechnologie: Gebruik, Opbrengsten En Uitdagingen' (Sanderflight.nl, 2016), <http://sanderflight.nl/wp-content/uploads/2016/08/2016-Flight-beeldtechnologie-Justitiele-Verkenningen.pdf> accessed 26 August 2020

Hagenaars P, 'De Kracht Van Privaat-Publieke Samenwerking' (*Gemeente.nu*, 2017) https://www.gemeente.nu/content/uploads/2017/03/2017-Whitepaper-de-kracht-van-privaat-publieke-samenwerking.pdf

Helsloot I 'Evaluatie Wet Justitiële En Strafvorderlijke Gegevens' (Wodc.nl, 2013), <https://www.wodc.nl/binaries/2102-volledige-tekst_tcm28-72074.pdf> accessed 5 October 2020

Kuijken K, 'Evaluatie Politiewet 2012 Doorontwikkelen En Verbeteren' (*Wodc.nl*, 2017), <https://www.wodc.nl/binaries/2747_Evaluatie-Politiewet-2012_tcm28-289414.pdf> accessed 11 June 2020

Kruijf J de, 'Een Evenwichtig Bestuurde Politie?' (*Rug.nl*, 2017) <https://www.rug.nl/research/portal/files/64129093/2747a_Deelstudie_Juridische_Status_tcm28_289415.pdf> accessed 12 June 2020

La Vigne N, 'Using Public Surveillance Systems For Crime Control And Prevention' (*Urban.org*, 2011), <https://www.urban.org/sites/default/files/publication/27551/412402-Using-Public-Surveillance-Systems-for-Crime-Control-and-Prevention-A-Practical-Guide-for-Law-Enforcement-and-Their-Municipal-Partners.PDF> accessed 5 July 2020

Nimwegen T, 'De Belgisch-Nederlandse Strafrechtelijke Samenwerking - Websitevoordepolitie' (*Websitevoordepolitie*, 2018) <https://www.websitevoordepolitie.nl/de-belgisch-nederlandse-strafrechtelijke-samenwerking/>

Schemer B, 'Handleiding Algemene Verordening Gegevensbescherming En Uitvoeringswet Algemene Verordening Gegevensbescherming' (*Iab.nl*), <https://www.iab.nl/images/downloads/HandleidingAlgemeneVerordeningGegevensbeschermin g-1.pdf>

Steden R van 'Publiek-Private Samenwerking In Tijden Van Diffuse Dreiging' (*Fsw.vu.nl*, 2018) <https://www.fsw.vu.nl/nl/Images/117020-PPS-in-tijden-van-diffuse-dreiging_tcm249-894219.pdf>

WEBSITES

Gemeente Amsterdam, 'Milieuzone' (Amsterdam.nl, 2019) <https://www.amsterdam.nl/parkeren-verkeer/milieuzone/> accessed 23 November 2019

'Het Nieuwe Aangiftesysteem Voor Bewakingscamera's Is Beschikbaar | Drupal' (Besafe.be, 2019) <https://www.besafe.be/nl/nieuws/het-nieuwe-aangiftesysteem-voor-bewakingscameras-is-beschikbaar> accessed 23 November 2019

"Camera in Beeld' (*Politie.nl*, 2019) <https://www.politie.nl/themas/camera-in-beeld.html?sid=afedd054-0221-49a3-acab-58aa68496ad3> accessed 23 November 2019

'Cameratoezicht Op Openbare Plaatsen' (*Autoriteitpersoonsgegevens.nl*) <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameratoezicht-op-openbare-plaatsen> accessed 11 January 2020

'Autoriteit Persoonsgegevens Publiceert Beleidsregels Cameratoezicht' (*Autoriteitpersoonsgegevens.nl*, 2016) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht#subtopic-1727> accessed 11 January 2020

Wetten.Nl - Regeling - Wet Politiegegevens - BWBR0022463' (*Wetten.overheid.nl*) <https://wetten.overheid.nl/BWBR0022463/> accessed 11 January 2020

Politie En OM Lanceren App Voor Burgeronderzoek' (*Politie.nl*, 2019), "Burgeronderzoek door pedojagers', <https://www.politie.nl/nieuws/2019/mei/27/00-politie-en-om-lanceren-app-voor-burgeronderzoek.html> accessed 21 January 2020

'London's Met police Switches On Live Facial Recognition, Flying In Face Of Human Rights Concerns' (*Techcrunch.com*, 2020) <https://techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facial-recognition-flying-in-face-of-human-rights-concerns/> accessed 13 February 2020

'Jaaroverzicht 2015 Slim Bekeken: Bijna 40 Nieuwe Cameraprojecten' (*Centrum voor Criminaliteitspreventie en Veiligheid (CCV)*, 2016) <https://hetccv.nl/nieuws/jaaroverzicht-2015-slim-bekeken-bijna-40-nieuwe-cameraprojecten/> accessed 27 March 2020

(Ring Europe, 2015) <https://eu.ring.com/> accessed 13 February 2020

'Verplichte Registratie Privé-Camera's? 'Dan Worden Burgers Verlengstuk Politie' (*Nos.nl*, 2018) <https://nos.nl/nieuwsuur/artikel/2238765-verplichte-registratie-prive-camera-s-dan-worden-burgers-verlengstuk-politie.html> accessed 25 March 2020

'Opsporingsbevoegdheden Hebben Wettelijke Basis - Bewijs In Strafzaken' (*Bewijs in strafzaken*) <https://bewijs-in-strafzaken.nl/uitgangspunt-opsporingsbevoegdheden-hebben-wettelijke-basis/> accessed 2 April 2020

'Landen | Europese Unie' (*Europese Unie*) <https://europa.eu/european-union/about-eu/countries_nl> accessed 5 April 2020

'What Is Considered Personal Data Under The EU GDPR? - GDPR.Eu' (*GDPR.eu*) <https://gdpr.eu/eu-gdpr-personal-data/> accessed 5 April 2020

'How Do We Apply Legitimate Interests In Practice?' (*Ico.org.uk*) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/> accessed 5 April 2020

"Handhaving' (*Politie.nl*, 2020) <https://www.politie.nl/themas/handhaving.html> accessed 6 April 2020

'Ring Doorbell 'Gives Facebook And Google User Data' (*BBC News*, 2020) <https://www.bbc.com/news/technology-51281476> accessed 23 April 2020

Publiek-Private Samenwerking Bij De Opsporing Van Criminaliteit' (*Sdu.nl*, 2017) <https://www.sdu.nl/blog/publiek-private-samenwerking-bij-de-opsporing-van-criminaliteit.html> accessed 24 April 2020

"Hoe Onveiliger, Hoe Meer Acceptatie Cameratoezicht" (*Centrum voor Criminaliteitspreventie en Veiligheid (CCV)*, 2019) <https://hetccv.nl/nieuws/hoe-onveiliger-hoe-meer-acceptatie-cameratoezicht/> accessed 29 April 2020

'Data Protection In The EU' (*European Commission - European Commission*) <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en> accessed 7 June 2020

'Understanding The Difference Between EU Directives And EU Regulations—Certification Experts' (Certification-experts.com) <https://certification-experts.com/understanding-the-difference-between-eu-directives-and-eu-regulations/> accessed 9 June 2020

'Controllers And Processors' (Ico.org.uk) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/> accessed 17 July 2020.

'Politie' (Autoriteitpersoonsgegevens.nl) <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/politie> accessed 22 July 2020

'Antwoorden Kamervragen Over Het Bericht 'Gezichtendatabase Van Politie Bevat Foto's Van 1,3 Miljoen Mensen' (Rijksoverheid.nl, 2019) <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/09/10/antwoorden-kamervragen-

over-het-bericht-gezichtendatabase-van-politie-bevat-foto-s-van-1-3-miljoen-mensen> accessed 7 September 2020

'Antwoorden Kamervragen Over Het Bericht Gratis Deurbellen Tegen Criminaliteit Het Twijfelachtige Effect En De Privacyzorgen' (Rijksoverheid.nl, 2020) <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/01/10/antwoorden-kamervragen-over-het-bericht-gratis-deurbellen-tegen-criminaliteit-het-twijfelachtige-effect-en-de-privacyzorgen> accessed 7 September 2020

'Assessing The Necessity Of Measures That Limit The Fundamental Right To The Protection Of Personal Data: A Toolkit' (Edps.europa.eu, 2017) <https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf> accessed 10 September 2020

'THE EDPS VIDEO-SURVEILLANCE GUIDELINES' (Edps.europa.eu, 2010), <https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> accessed 10 September 2020

'Guidelines On Data Protection Impact Assessment (DPIA) And Determining Whether Processing Is “Likely To Result In A High Risk” For The Purposes Of Regulation 2016/679' (Ec.europa.eu, 2017) <https://ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 12 September 2020

'Guidelines On Data Protection Impact Assessment (DPIA) And Determining Whether Processing Is “Likely To Result In A High Risk” For The Purposes Of Regulation 2016/679' (Ec.europa.eu, 2017) <https://ec.europa.eu/newsroom/document.cfm?doc_id=47711> accessed 12 September 2020

'DPIA Suggested Process And Template' (Ico.org.uk) <https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx> accessed 12 September 2020

'Honderden Beveiligingscamera's In Nederland Niet Goed Beveiligd' | NU - Het Laatste Nieuws Het Eerst Op NU.Nl' (Nu.nl, 2020) <https://www.nu.nl/tech/6025759/honderden-beveiligingscameras-in-nederland-niet-goed-beveiligd.html> accessed 16 October 2020.

Binversie K, 'How Agencies Can Utilize Private Camera Surveillance Systems - In Public Safety' (*In Public Safety*, 2019) <https://inpublicsafety.com/2019/10/how-agencies-can-utilize-private-camera-surveillance-systems/> accessed 5 July 2020.

Bouma R, 'Slimme Deurbel Rukt Op In Strijd Tegen Inbraken, Maar Hoe Zit Het Met Privacy?' (*NOS.nl*, 2020) <https://nos.nl/nieuwsuur/artikel/2318362-slimme-deurbel-rukt-op-in-strijd-tegen-inbraken-maar-hoe-zit-het-met-privacy.html> accessed 13 February 2020

Bowcott O, 'police Use Of Facial Recognition Is Legal, Cardiff High Court Rules' (*the Guardian*, 2019) <https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules> accessed 13 February 2020

Budington B 'Ring Doorbell App Packed With Third-Party Trackers' (Electronic Frontier Foundation, 2020) <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers> accessed 8 September 2020

Engelfriet A, 'De Toegevoegde Waarde Van Een Bodycam Voor De Politie En De Maatschappij - Ius Mentis' (Ius Mentis, 2019) <https://blog.iusmentis.com/2019/05/07/de-toegevoegde-waarde-van-een-bodycam-voor-de-politie-en-de-maatschappij/> accessed 21 July 2020

Gaal W van, 'Gezichtsherkenning Op De Nederlandse Straten: Moeten We Dat Willen?' (*Vice*, 2019) <https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen> accessed 23 April 2020

Haan R, 'Publiek' (*Centrum voor Criminaliteitspreventie en Veiligheid (CCV)*) <https://hetccv.nl/onderwerpen/cameratoezicht/publiek/https://hetccv.nl/onderwerpen/cameratoezicht/publiek/> accessed 28 February 2020

Haan R, "Privaat' (*Centrum voor Criminaliteitspreventie en Veiligheid (CCV)*) <https://hetccv.nl/onderwerpen/cameratoezicht/privaat/https://hetccv.nl/onderwerpen/cameratoezicht/privaat/> accessed 28 February 2020

Haan R, 'Publiek-privaat' (*Centrum voor Criminaliteitspreventie en Veiligheid (CCV)*) <https://hetccv.nl/onderwerpen/cameratoezicht/publiek-privaat/https://hetccv.nl/onderwerpen/cameratoezicht/publiek-privaat/> accessed 28 February 2020

Harwell D 'Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns' (The Washington Post, 2019) <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/> accessed 8 September 2020

Houwing L, 'Hoe De Politie Haar Buitenwettelijke Surveillancenetwerk Uitbreidt' (Joop.bnnvara.nl, 2020) <https://joop.bnnvara.nl/opinies/hoe-de-politie-haar-buitenwettelijke-surveillancenetwerk-uitbreidt> accessed 11 February 2020

Houwing L, 'Minister Komt Met Zorgwekkende Antwoorden Op Kamervragen Over CATCH' (*Bits of Freedom*, 2019) <https://www.bitsoffreedom.nl/2019/09/11/minister-komt-met-zorgwekkende-antwoorden-op-kamervragen-over-catch/> accessed 13 February 2020

Huijbregts J, 'Nederlandse Politie Begint Met Gezichtsherkenning Bij Opsporing' (*Tweakers.net*, 2016) <https://tweakers.net/nieuws/119105/nederlandse-politie-begint-met-gezichtsherkenning-bij-opsporing.html> accessed 23 April 2020

Kaltheuner F, 'Facial Recognition Cameras Will Put Us All In An Identity Parade | Frederike Kaltheuner' (*the Guardian*, 2020) <https://www.theguardian.com/commentisfree/2020/jan/27/facial-recognition-cameras-technology-police> accessed 11 February 2020

Klaassen N, 'Politie Krijgt Steeds Vaker Beelden Privécamera' (*Ad.nl*, 2018) <https://www.ad.nl/binnenland/politie-krijgt-steeds-vaker-beelden-privecamera~a2ad54d1/> accessed 25 January 2020

Peers S, 'Bringing Data Protection Home? The CJEU Rules On Data Protection Law And Home CCTV' (Eulawanalysis.blogspot.com, 2014) <http://eulawanalysis.blogspot.com/2014/12/bringing-data-protection-home-cjeu.html> accessed 27 July 2020

Rombout B, 'Security Management' (Securitymanagement.nl, 2019) <https://www.securitymanagement.nl/registratie-digitale-ogen-ja-of-nee/> accessed 23 November 2019

Teeffelen K van, 'Privacy Settings' (*Trouw.nl*, 2019) <https://www.trouw.nl/binnenland/politie-amsterdam-loerde-onterecht-in-data-van-milieucamera-s~bba1398a/?referer=https%3A%2F%2Fwww.google.com%2F> accessed 25 March 2020

Tomesen W, (*Autoriteitpersoonsgegevens.nl*, 2016) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_saunas_cameratoezicht.pdf> accessed 25 March 2020

Vries E de, 'Privacyweb' (*Privacy-web.nl*, 2019) <https://www.privacy-web.nl/artikelen/avg-gelden-nu-overal-in-de-eu-dezelfde-privacyregels-1> accessed 4 April 2020

Wokke A, 'Tweakers' (Tweakers.net, 2019) <https://tweakers.net/nieuws/156730/ring-heeft-geen-samenwerkingscontracten-met-politie-in-nederland-en-belgie.html> accessed 13 February 2020

PARLIAMENTARY PAPERS

European Union, 'TOELICHTINGEN (*) BIJ HET HANDVEST VAN DE GRONDRECHTEN' (European Union 2007)

Kamerstuk 28684, Nr. 617' (*Zoek.officielebekendmakingen.nl*, 2020) <https://zoek.officielebekendmakingen.nl/kst-28684-617.html>

Tweede Kamer, 'Antwoorden Kamervragen Over Het Bericht 'Gezichtendatabase Van Politie Bevat Foto's Van 1,3 Miljoen Mensen' (2019)

Tweede Kamer, 'Wijziging Van De Wet Politiegegevens En De Wet Justitiële En Strafvorderlijke Gegevens Ter Implementatie Van Europese Regelgeving Over De Verwerking Van Persoonsgegevens Met Het Oog Op De Voorkoming, Het Onderzoek, De Opsporing En Vervolging Van Strafbare Feiten Of De Tenuitvoerlegging Van Straffen' (2017)

'Nota Van Toelichting Politiewet', (*Zoek.officielebekendmakingen.nl*) <https://zoek.officielebekendmakingen.nl/blg-868244.pdf>

'Kamerstuk 29440, Nr. 3' (*officielebekendmakingen.nl*, 2004) <https://zoek.officielebekendmakingen.nl/kst-29440-3.html>

THESIS

Lorca Van de Putte, 'Onder Het Oog Van De Camera: Een Kritische Analyse Van Cameratoezicht In De Publieke Ruimte' (*Lib.ugent.be*, 2014) <https://lib.ugent.be/fulltxt/RUG01/002/162/969/RUG01-002162969_2014_0001_AC.pdf>