Faculty of Law
University of Helsinki

The End of Freedom in Public Places?

Privacy problems arising from surveillance of the European public space.

Jens Kremer

Doctoral dissertation

To be presented for public examination, by due permission of the Faculty of Law at the University of Helsinki in auditorium XIV at the University's main building, on the 24th of March, 2017 at 12 o'clock.

Helsinki 2017

Dissertation

University of Helsinki

Faculty of Law

ISBN 978-951-51-3035-8 (paperback)
ISBN 978-951-51-3036-5 (PDF)

Unigrafia

Helsinki 2017

Abstract

This dissertation analyses specific privacy problems arising from the surveillance of public spaces. It studies the scope and limitations of the human right to privacy and a right to personal data protection in light of advanced surveillance and security technologies. The main research question therefore asks how the existing European fundamental rights to privacy and data protection address increasing surveillance and the unprecedented surveillance capabilities of public spaces in Europe.

This study is divided into two main parts. After introducing the research problem and a descriptive discussion of existing and future surveillance technologies, the first part discusses the theoretical conceptions behind this research, namely the concept of public space, privacy, data protection and security. Part two of this study then discusses four more specific issues in relation to public space surveillance: Individually targeted surveillance, mass surveillance, surveillance done by private actors, automation of surveillance, and incident prediction.

In order to address the research question, this study analyses existing legislation, jurisprudence and specific cases. The overall framework for analyses is derived from a fictional urban surveillance scenario, representing a large European city. This surveillance scenario serves as an anchor point to identify central problems and issues for further fundamental rights based analyses. In that sense, this study uses legal and critical analyses of a specific scenario in order to identify existing, but also potential future legal problems arising from sophisticated public space surveillance.

This study consequently identifies several ways to address public space surveillance from a European fundamental rights perspective. The analyses of a right to privacy and a right to personal data protection show that the European system of fundamental rights protection is very well capable of addressing legal problems arising from public surveillance. However, there is a lack of available case law dealing with complex technological surveillance in Europe. This study therefore distils two main approaches for addressing public surveillance: The first approach is based on individual freedom, relying on the legitimate expectations of legal subjects, the second, which is derived from human dignity and personality rights, challenges the communal effects of

surveillance. Each approach comes with a fundamentally opposite take on public surveillance. Furthermore, this study shows, how data protection functions as a gap-filler between the two approaches. In its conclusion, this study therefore illustrates several ways to address public space surveillance, and it shows that there is a series of legal problems arising from sophisticated technological surveillance, which require a reformulation of legal arguments addressing public place surveillance.

Acknowledgments

This dissertation is the result of several years of research at the Faculty of Law at the University of Helsinki. I am grateful to the many people whose help, both direct and indirect, contributed to this work. I am lucky to have benefited from wonderful colleagues, research communities, friends and family who, in one or the other way, through their support, comments, encouragement, or excellent belay skills, made this dissertation possible.

I would like to especially thank my doctoral supervisor, Kaarlo Tuori, for his mentorship and the many forms of support and encouragement. I am grateful to Professor Iain Cameron for doing me the honour of acting as the opponent and as one of the pre-examiners for this dissertation. Many thanks go to Juha Lavapuro for his contribution as pre-examiner. I also owe a debt of thanks to Tuomas Ojanen and Susanna Lindroos-Hovinheimo for their extremely valuable comments and constructive critique of this work.

I am thankful to Kimmo Nuotio, the Dean of the Faculty of Law, for his continuous support and encouragement. Warm thank you is due to Pia Letto-Vanamo for being a fair, caring and encouraging superior during my employment at the Faculty of Law. I also want to thank Jarna Petman for her role as the coordinator of the discipline of international law, as well as her support and encouragement.

This dissertation could not have been completed without the variety of stimulating research environments and communities that I have had the honour of being a part of during the years.

Particularly the *Centre of Excellence in Foundations of European Law and Polity Research* and its members provided a welcoming research environment and an excellent platform to discuss the first ideas for this work.

I additionally want to thank Sakari Melander and the members of the project *Criminal Law Under Pressure* in Helsinki, Professor Martin Scheinin and the members of the *SURVEILLE-Project* at the European University Institute, the Members of the Research Consortium *Laws of Surveillance and Security (LOSS)* in Helsinki and Turku, the *Young Nordic Police Research Network* in Oslo, the IACL Research Group

Constitutional Responses to Terrorism, and the Research Project *Digital Health Revolution II* at Aalto University. They all provided platforms for presentations and discussions, and fostered the creation of many friendships.

I would like to particularly acknowledge the growing information law community at the University of Helsinki, and here the *Fundamental Rights, Privacy and Security (FUPS)* research group, spearheaded by Tobias Bräutigam, Samuli Miettinen, Niklas Vainio, Olli Pitkänen, Anette Alén-Savikko, and Päivi Korpisaari.

I am very grateful to the Academy of Finland funded Graduate School Law in a Changing World (LCW) at the University of Helsinki, both for funding the majority of this research, as well as for generating a creative research environment for Doctoral Candidates at the Faculty of Law. This work received further financial support from the Research Foundation of the University of Helsinki and the Scandinavian Research Council for Criminology.

A special thanks goes to the colleagues and friends and their invaluable contributions throughout the years, especially Silke Trommer, Søren Berg-Rasmussen, Heikki Marjosola, Suvi Sankari, Fernando Losada, Klaus Tuori, and Eliška Pírková.

Finally, the deepest thanks go to my family and friends for their love and support. To my parents, who have always been supporting me in all possible ways. And to my wife, who brings meaning, motivation, and balance into my life, throughout good and bad times.

Helsinki, 1 March 2017.

Content

Abstract ..... **iii**
Acknowledgments ..... **v**
Content ..... **vii**
Abbreviations ..... **x**

Prelude **1**

1. **Introduction** **3**
   1.1 Background 3
   1.2 Research objectives and main research question 7
   1.3 Methodology 9
   1.4 Structure 16
   1.5 Technology and Surveillance Scenario 18
      1.5.1 Video Surveillance 20
         1.5.1.1 Purposes and Promises of Video Surveillance 22
         1.5.1.2 Smart Surveillance and Video Content Analytics (VCA) 24
         1.5.1.3 Mobile Cameras and Aerial Surveillance 28
      1.5.2 Ubiquitous Sensors and Networks 31
      1.5.3 Biometrics 32
   1.6 The Urban Surveillance Scenario 35

2. **Conceptions of Public Space, Privacy, Data Protection and Security 39**
   2.1 'Private' and 'Public' Physical Space 39
   2.2 Privacy as a Legal Concept 46
      2.2.1 Privacy as the Right to Be Let Alone 46
      2.2.2 Privacy and Torts 49
      2.2.3 Privacy as Control of Information 52
      2.2.4 Privacy as Limited Access to the Self 57
      2.2.5 Intimacy and Secrecy 60
      2.2.6 Privacy, Dignity, and the Right to Personality 65
      2.2.7 Privacy in Public 71
   2.3 Data Protection and Information Law 85
      2.3.1 The Emergence of Data Protection in Europe 85
         2.3.1.1 Data Protection in the International Sphere 91

2.3.1.2 The Sources of Data Protection in Europe 92
2.3.1.3 Data Protection in the EU 94
2.3.2 Data Protection as a Fundamental Right? 96
2.3.3 Conclusion 102
2.4 Security 104
2.4.1 Security and the Law 107
2.4.2 Public Surveillance and Security 109
2.4.3 The Right to Security 109
2.4.3.1 The ECHR and a Right to Security 110
2.4.3.2 The EU and a Right to Security 114
2.4.4 Conclusion 116
2.5 Limiting Mechanisms to Fundamental Rights 118
2.5.1 Limitations of the International Human Right to Privacy and Data Protection 118
2.5.2 Permissible Limitations in the ECHR 126
2.5.3 Permissible Limitations in the EUCFR 133

3. European Fundamental Rights and Public Surveillance 144
3.1 Targeted Public Surveillance 145
3.1.1 The Scope of a Right to Privacy in Public 146
3.1.1.1 Reasonable Expectations of Privacy in Public and the ECHR 153
3.1.1.2 Covert and Overt Public Surveillance 162
3.1.2 Personal Information and Surveillance 166
3.1.2.1 The Definition of Personal Data 169
3.1.2.2 The General Principles of Data Protection 174
3.1.2.3 Data Protection in the Scope of the ECHR 179
3.1.2.4 Data Protection Issues in the Scenario 190
3.1.2.4.1 Systematic Collection 191
3.1.2.4.2 Data Quality 193
3.1.2.4.3 Data Retention 195
3.1.3 Conclusion 197
3.2 Mass Surveillance 200
3.2.1 Distinguishing Mass Surveillance from Targeted Surveillance 202
3.2.2 Mass Surveillance and Privacy 204
3.2.2.1 Admissibility and Victim Status in ECHR Mass Surveillance Cases 205
3.2.2.1.1 Challenging Mass Surveillance *in abstracto* 210

3.2.2.1.2 The Victim-Status Test 212
3.2.2.2 Fundamental Rights Arguments against Mass Surveillance 215
3.2.2.2.1 Mass Surveillance and the Scope of Privacy 215
3.2.2.2.2 Mass Surveillance as a 'Menace to Society' 219
3.2.2.2.3 The Right to Establish Relationships with the Outside World 221
3.2.3 Mass Surveillance and Data Protection 223
3.2.3.1 The Scope of Data Protection 225
3.2.3.2 Big Data 226
3.2.3.3 Big Data, Societal data and Data Protection Principles 232
3.2.3.4 Applicability of EU Data Protection to Mass Surveillance 234
3.2.4 Mass Surveillance and Dignity 239
3.2.4.1 Personal Autonomy and Self-Determination 240
3.2.4.2 Dignity and State Surveillance 243
3.2.4.3 EU, Dignity and Surveillance 246
3.2.5 Conclusion 247
3.3 Private Actor Surveillance Operations 249
3.3.1 Private Actors and Fundamental Rights 249
3.3.2 Private Surveillance Operations in Public Areas 250
3.3.3 Conclusion 260
3.4 Automation and Prediction 262
3.4.1 Automation 262
3.4.2 Prediction 269

4. Concluding Remarks 273

Table of Cases 279
Table of Legislation 285
Bibliography 291
Internet Sources 305

Abbreviations

ACLU	American Civil Liberties Union
ACM	Association for Computing Machinery
ADAPTS	Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces
ANPR	Automatic number plate recognition
App	Application
ARGUS-IS	Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System
Art	Article
Az	Aktenzeichen
BayRS	Bayerische Rechtssammlung
BayStrWR	Bayerisches Straßen- und Wegegesetz
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BND	Bundesnachrichtendienst
BSIA	British Security Industry Association
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CoE	Council of Europe
CUP	Cambridge University Press
D	Deliverable
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DPA	Data Protection Authority
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
ed	Editor
edn	Edition
eds	Editors

esp	especially
ETS	European Treaty Series
EU FP7	European Union Framework Program 7
EUCFR	Charter of Fundamental Rights of the European Union
FCC	German Federal Constitutional Court
fn	footnote
FRA	European Union Agency for Fundamental Rights
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
HRC	UN Human Rights Committee
IA	Intelligent Analytics
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICT	Information and Communications Technology
INDECT	Intelligent information system supporting observation, searching and detection for security of citizens in urban environment
IPS	Intelligent Pedestrian Surveillance System
ISTAG	Information Society Technologies Advisory Group
IVA	Intelligent Video Analytics
MAD	Militärischer Abschirmdienst
MIT	Massachusetts Institute of Technology
NGO	Non-governmental organization
no	Number
OECD	Organisation for Economic Co-operation and Development
OUP	Oxford University Press
PerSEAS	Persistent Stare Exploitation and Analysis System
SIS	Schengen Information System
StVO	Straßenverkehrsordnung
TFEU	Treaty on the Functioning of the European Union
UAV	Unmanned Aerial Vehicles

UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
UNGA	United Nations General Assembly
UNTS	United Nations Treaty Series
US	United States
VCA	Video Content Analyses
VCLT	Vienna Convention on the Law of Treaties
Vol	Volume
WAMI	wide area motion imagery
WP	Working Party
WWW	World Wide Web

Prelude

Imagine a sunny Saturday morning in early September. The sun is shining and a light warm breeze is coming from the seaside, a forerunner of a nice warm late summer day in a city somewhere in Northern Europe. You take a short glimpse at the clock on the kitchen wall, place the empty coffee mug in the dishwasher and prepare to leave your apartment in order to visit the nearest supermarket to get some groceries for the weekend. It is 09:53 am and the supermarkets should be open by the time you get there. You grab your keys, your mobile phone and the small thin leather wallet you got as a birthday present and you leave the house. The door locks behind you, making that familiar short squeaking sound as the small electronic motor locks the safety bolts of the door.

As you walk down the stairs your phone suddenly sounds an alarm. You look at it and read on the screen: 'Attention, you are leaving your home. I have switched off the coffee machine and the light in the bathroom for you.' 'Thanks', you think, and at the same time you open your Application for your car on your phone. Yesterday, when you came home from work, the next available parking spot was over 800 meters away from your door and as you don't feel like walking, you press the 'pick me up'-button to order the car to come by itself.

After a couple of minutes, it arrives, fully charged and ready to take you to the supermarket. 'Good morning, your trip will be 7km, 13min driving time with barely any traffic' sounds from the speakers of the car hi fi system while you enter and shortly after that: 'do you want me to get you there?' You think, 'why not', respond 'yes', and while the car noiselessly accelerates down the road, you open your favourite news application on the main dashboard screen. 'I sense that you are in a good mood, shall I select some music from a relevant playlist for you?' sounds from the car hi fi system. 'Yes', you respond and your favourite music makes you feel even better than before.

As you get closer to the supermarket, some advertising in the news-application catches your eye. 'Fresh mussels from French Bretagne, today only 7.95 per kg'. You always love to prepare fresh mussels, especially when you have a good mood and it is a nice summer day. You start speaking: 'Hey, can you get me those mussels, as well as some fresh celery, carrots, parsley and… is there still some white wine in the fridge?'. The

computer system responds immediately: ‘Yes, there is a bottle of white wine in the fridge and I will order your groceries.’ A couple of seconds later, the system gets back to you: ‘The supermarket confirms your orders, they can be picked up at the drive-by station at exit B of the supermarket parking hall. Thank you for your shopping. Please let me know if you need anything else. Have a wonderful day!’. You lean back and think, what a nice start of a day.

This is science fiction. It is far from clear whether such a scenario will ever be reality. Today, in 2017, and at least this morning, my door lock was still mechanical, my car drives on dirty gasoline and my phone barely understands me when I want ‘Siri’ to text my wife that I’ll be home an hour later this evening. My fridge is still not connected to the internet although it’s been forecast since the 90s and I still have to actually physically walk into a supermarket to check if they sell mussels (which one shouldn’t buy if one is concerned with environmental and health issues). Yet, on the other hand, although my lock is still mechanic, the key carries a digital code which allows the lock to be physically opened. My car knows when its emissions are tested and cheats, and there are actually some electric cars out there which can drive on their own in certain situations – none of which are (yet) affordable for individuals from average income households. Also, my phone and all the installed applications collect large volume of data and although my fridge is not connected to the internet there are about 20 devices connected to my home router including phones, tablets, computers, TV, some receivers and lately even a LED lightbulb that can change colour, controlled bt my mobile phone. It seems, we are getting there.

1. Introduction

1.1 Background

This thesis is about surveillance in public spaces. One might rightly ask what the scenario in above has to do with surveillance and furthermore why it is the prelude to this study on surveillance and law. The answer to this question is relatively simple: All those new services described above produce data. Data which essentially contains information of many sorts. This is not necessarily intended but it is just how it works. Computers create data as a 'by-product' in every operation they process. Bruce Schneier describes this phenomenon in his recent book *Data and Goliath*.[1]

If technology, innovation and entrepreneurship strive for a scenario as the one above, a lot more sensors and devices will need to produce, collect, retain and process data. This data also needs to be shared more efficiently. Simply imagine the computer processes that need to happen when one wants to build a functional and safe system that warns one that the coffee machine is on when leaving home. There needs to be a network that enables those devices to somehow communicate. Some sensor needs to identify that the coffee machine is on, some others need to detect that a person is leaving, requiring location information. Then, there needs to be a system that processes those sensor data and makes the right conclusions. Also, the system should be secure, foremost against malfunction but also against external manipulation. In order to technically achieve such an operation, a lot of data needs to be collected and analysed, all automatically and in the background. Similarly, for vehicle automation, but much more complex and a broader scale. Automatic vehicles need to process a large quantity of sensor data and they will probably be networked. Many more examples of data processing in everyday contexts can be found in smart city designs and the digitalization of infrastructure.

Scenarios as the one mentioned above require vast networking and communications between things, devices and people in society. In fact, everyday life will increasingly be accompanied by a vast and invisible web of communications and data flows. Those data flows, have been described as the Internet of Things, ubiquitous computing, and

[1] See Schneier B, Data and Goliath: the hidden battles to collect your data and control your world (W.W. Norton 2015), especially Chapter 1.

smart cities amongst other terms.[2] All of those come with one issue: The data which is produced can be used to gather, retain and process information about individuals. Such information can literally tell everything about a person, including profiling and the prediction of likely future behaviour. In short, all data, even if collected as a by-product, is extremely useful for surveillance purposes.

Surveillance, as a buzzword, has become a major issue for democracies and law not at least with the public debates sparked by the revelations of excessive global surveillance practices through US military and intelligence agencies.[3] David Lyon described such surveillance already in 2001 as '…any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered.'[4] Surveillance therefore comes with the core purpose of controlling and coercing, or in order to gain advantages over an alleged opponent or competitor in the future.

One of the reason why surveillance appears to have become omnipresent is, however, not only due to the ever-expanding capabilities of technologies and data processing, but also because of many alleged and perceived increased security concerns. The increasing fears of terror attacks in crowded public places, for example, have therefore paved the ways for more public surveillance. Both, the variations of attacks and the sophistication of the attackers appear to necessitate a wide array of security counter measures that reach from architectural alterations to the installation of highly sophisticated surveillance systems enabling control over vast public spaces. In fact, today's tools for public surveillance have reached an unprecedented level of sophistication and surveillance capabilities, which promise to improve security perceptions. During recent years, surveillance capabilities have evolved dramatically.

---

[2] See e.g. De Hert P and others, 'Legal Safeguards for Privacy and Data Protection in Ambient Intelligence' (2008) 13 Personal and Ubiquitous Computing 435; Rouvroy A, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence' (2008) 2 Studies in Ethics, Law and Technology 1; Edwards L, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) European Data Protection Law Review 28.

[3] See Greenwald G, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books/Henry Holt 2014); Georgieva I, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR.' (2015) Utrecht Journal of International and European Law 104.

[4] Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001), 2.

Today, modern public surveillance systems include a variety of sensors such as video cameras, hyper sensitive microphones or radiation detectors and their interconnectedness allows for highly sophisticated processing of data. This enables the use of surveillance systems that can automatically detect incidents, recognize gunshots or explosions or track objects in real time. Additionally, they are integrated into modern centrally administered 'smart' cities. Soon, scenarios of such 'smart' surveillance systems could enable total control over public spaces, may that be a parking lot, a railway station or a whole city including its roads, public transport systems, shopping, leisure and commercial areas.

Public places are of special concern for security authorities. With their general accessibility, openness and the inherent freedom in addition to the symbolisms they carry, public places are a focal point for both the bright and dark sides of societal life. Liberations and revolutions, but also atrocities and massacres are often associated with particular public spaces. Breaking highly organized, regulated and functional public spaces can be a tool to question existing or ruling powers in all its forms and shapes.[5] With this, the public space is an area of freedom, the expression of opinion, political protest, but also a space for state violence, massacres or target for terror attacks such as the recent attacks in Paris.

Fifteen years ago, after the 9/11 attacks put terrorism up high on political agendas, a variety of legal exceptions and emergency measures were introduced, *inter alia* in the form of anti-terrorism laws. A whole new regime of security measures was introduced on a global scale, legally enabling unprecedented surveillance of individuals in ever expanding states of exceptions and emergencies.[6] Debates and responses to the recent attacks in Paris indicate that the expansion of surveillance in European spaces has not yet reached its peak.[7]

---

[5] See Burgmer C, 'Warum einen öffentlichen Platz besetzen?' (Deutschlandfunk, Essay und Diskurs, 03.10.2014) http://www.deutschlandfunk.de/protestbewegung-warum-einen-oeffentlichen-platz-besetzen.1184.de.html?dram:article_id=299327 accessed 8 October 2016.

[6] See e.g. Scheppele KL, 'Global Security Law and the Challenge to Constitutionalism after 9/11' (2011) Public Law 352.

[7] The New York Times Editorial Board, 'Mass Surveillance Isn't the Answer to Fighting Terrorism' *The New York Times Online*, (17.11.2015) http://www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html accessed 17.11.2015, also in print: The New York Times, New York Edition, 18.11.2015, p A26.

As the amounts of data have increased, so has the capabilities for analysing them. Technological advancements also led to continuous progress in the capabilities of surveillance technologies up to a point that was unimaginable just a few years ago. The ability to trace individuals with commonly used devices such as mobile phones or RFID-tags is only one example[8], CCTV systems are now part of everyday life and Massively Integrated Multiple Sensor Installations (MIMSI) [9] as well as video analytics and facial recognition systems are available, functional and are being used by security services. While in 2008, for example, automated face recognition technology was only capable of recognizing faces regardless of environmental conditions with an accuracy of 90-95%,[10] in 2015 Google researchers published a paper claiming nearly 100% accuracy for a popular facial recognition dataset.[11]

Modern surveillance systems in public places have come a long way since the first analogue closed-circuit surveillance cameras emerged.[12] Today, smart surveillance systems are digital, networked, retain and analyse surveillance data they obtain from a variety of sensors and sources, and they are deeply integrated into the public environments they control. Video analytics enables the searching of image data in real time, facial recognition can pick out suspects from a vast data pool, behavioural analytics can identify any incident in real time, and the integration of ubiquitous data

[8] Radio Frequency Identification tags are small microchips which store unique information about a single item and which can be read and traced via radio waves.

[9] MIMSIs are surveillance systems that combine different sensors into one connected surveillance system: e.g. when intelligent visual surveillance (that can identify suspicious behavior through e.g. motion analyses) is connected with other types of surveillance technology such as audio analyses (that can automatically identify unusual sounds, such as explosions, shooting or screams). See e.g.: Cannataci, JA, 'Squaring the Circle of Smart Surveillance and Privacy, 2010 Fourth International Conference on Digital Society' in Council of Europe Recommendation R(87)15 & ETS Convention 108, Data Protection Vision 2020: Options for improving European policy and legislation during 2010-2020; Appendix 3, http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf accessed 17.November 2015.

[10] See: e.g.: Gardiner B, 'Engineers Test Highly Accurate Face Recognition' *Wired* (24.03.2008), http://www.wired.com/science/discoveries/news/2008/03/new_face_recognition accessed 17 November 2015.

[11] Florian Schroff, Dmitry Kalenichenko, James Philbin, 'FaceNet: A Unified Embedding for Face Recognition and Clustering.' (v3, 17 June 2015, Cornell University Library, arXiv.org) http://arxiv.org/pdf/1503.03832.pdf accessed 17 November 2015.

[12] See e.g. Webster CWR and others (eds), *Video surveillance: Practices and Policies in Europe* (IOS Press 2012).

streams from the internet of things, the internet, and social media allows profiling, highly targeted surveillance and even theoretically incident prediction.[13]

1.2 Research Objectives and Main Research Question

Today's massive data streams, paired with the constantly improving capabilities of surveillance and security technologies will theoretically enable highly sophisticated surveillance and the control of public spaces. With this, the public space is transforming. It is becoming more surveilled and controlled, and the control mechanisms are becoming more efficient, more responsive and even predictive. In this connection, two legal questions emerge - and both questions address regulations concerning public spaces.

The first, and probably most intuitive legal question concerns the 'regulability' of public space *per se*.[14] How is individual or collective behaviour regulated in a public space? What governs it and how can new issues such as technological developments be addressed? Surveillance and control mechanism in this context are an essential part of enforcement and analyses of the functioning of such regulations.

The second legal question rising from the increased surveillance and control is about governing and regulation of power. What are the counter mechanisms that protect individuals from excessive control of public spaces?

Public spaces in democratic societies are essentially places symbolizing freedom and any state measures restricting that freedom needs to have, at least to some extent, certain recourse mechanisms. In that sense, the second question is about fundamental and human rights in public spaces. What are the rights of individuals in public places? How can surveillance and control be limited? Is there a need to rethink the existing fundamental rights frameworks? Are advancing surveillance and control technologies a concern for fundamental rights?

[13] TrapWire is an early example of an attempt to build such a system. See Botsch RD and Maness MT 'Trapwire. Preventing Terrorism.' (2006) 22 *Crime and Justice International* 95, November/December 2006, 39-41.

[14] The term 'regulability' derives from Lawrence Lessig's work on cyberspace and describes '…the capacity of a government to regulate behavior within its proper reach.' See Lessig L, *Code: and other laws of cyberspace* (Basic Books 1999) p 19.

On the one hand, human rights have developed mechanisms to address the above-mentioned questions, for example, employing a human right to privacy. On the other hand, international human rights conventions and their protection systems seem to be overstrained with increased risks in public places, and the improved surveillance and control capabilities. It can clearly be said that the right to privacy is at stake through increasing state surveillance and anti-terrorism measures [15] and the massive improvements in security technology are adding to yet unprecedented interferences with human and fundamental rights. Furthermore, advanced technologies such as, for example, incident prediction and algorithmic analytics pose new challenges to existing fundamental rights mechanisms.

This study primarily addresses the latter set of questions. It asks how the existing European fundamental rights to privacy and data protection address the increasing and unprecedented surveillance capabilities of public spaces in Europe. For this reason, it primarily focusses on the scope of privacy and data protection in a public sphere increasingly controlled by highly sophisticated surveillance.

In order to answer these questions, this study approaches the topic from the various theoretical perceptions of privacy as a fundamental right. The core thesis of this study lies in a presumed separation between two fundamentally different approaches to privacy as a right: a conception of privacy based on individual liberty and a conception of privacy based on dignity, a right to personality, and a communal element deriving thereof. This distinction is important, because each of the approaches has different answers to the question of the applicability of fundamental rights to public space surveillance and the dramatic improvements of surveillance capabilities. This study will show that both approaches are present in current European jurisprudence on privacy and data protection and will therewith contribute to a better understanding of the 'problem of privacy in public',[16] by discussing a different perspective on privacy

[15] See UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin, A/HRC/13/37, 28.12.2009; Privacy International (2007), 'National Privacy Ranking 2007, Leading Surveillance Societies around the World', http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597&als[theme]=Data Protection and Privacy Laws accessed 17.11.2015.

[16] See e.g. Nissenbaum HF, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.

that produce contradictory results in understanding the rights to privacy and data protection.

1.3 Methodology

This study is based in theoretical analyses of existing legislation, jurisprudence and case analyses. For the latter, the framework for analyses is derived from an urban surveillance scenario. With references to real functional surveillance technology as well as connecting jurisprudence, the surveillance scenario serves as an anchor point to deduct central problems and issues for further analyses. This method is used to cover the uncertainty of future surveillance scenarios and in this way, future legal questions can be identified – as one essential element of this research is the ability to identify emerging legal problems.

There certainly are a variety of methods in law and so are there discussions of that topic.[17] One can, for example, borrow methodologies from the social sciences such as empirical research or socio-legal analyses, but probably the most common method in law is doctrinal legal research as '…the research process used to identify, analyse and synthesize the content of law.'[18] This, of course, presupposes that there is an identifiable content of law. However, assuming that law is an objective concept in reality enables to leave aside fundamental theoretical problems when researching it.

The debates around law and its methods in the social- and natural- sciences have of course always been subject to debates within the respective fields and one of the reasons for these debates is law's very distinct nature from the social sciences and natural sciences. In natural sciences, scientific knowledge is derived from a combination of description and causality. A phenomenon is observed and explained in accordance with the commonly agreed rules of explanations in the specific area of the scientific community. In social science, a variety of theoretical approaches such as, for example, an empirical-analytical or a critical-dialectical approach can construct and deliver scientific knowledge. Legal science, although it can be approached and

[17] See e.g. Watkins D and M Burton M (eds), *Research Methods in Law* (Oxon: Routledge 2013).

[18] Hutchinson T 'Doctrinal Research – Researching the Jury' in D Watkins, M Burton (eds) *Research Methods in Law* (Oxon: Routledge 2013) 9.

combined with methodologies of classical social sciences, has an added component: legal problems are heavily 'event'-based problems. Legal scholars, as Rubin describes it, '…are not trying to describe the causes of observed phenomena, but to evaluate a series of events, to express values, and to prescribe alternatives.'[19] This means that a method in law will have difficulties employing natural science methodologies, and requires turning towards the production of knowledge in social science, on the one hand, but it also means that it should be clear that a purely legally-dogmatic approach concerning the sole interpretation of existing rules has its clear limits.

One possibility to overcome this problem could be to employ a discursive perspective, in which communications in their many different forms play the decisive role. After all, law is communicated through language which allows us to look at law through the lens of discursive theories. Law can then be conceptualized as a self-referential and operatively closed system in Luhmannian terms,[20] for example when certain specialized fields of law are understood '*as* a language' comprising of its own 'grammar'.[21] From this perspective, legal discourses need to adapt and comply with the code and rules of the relevant communicative system. For Koskenniemi, for example, international lawyers need to speak the language and know the grammar of international law in order to build a legal argument that can be successful within the system of reference and therefore, conduct and apply doctrinal research on the surface level, while not losing the bigger picture of legal theoretical problems in the background. One problem with such allegedly critical methodologies, however, is that they barely leave room for theoretical inventions on a doctrinal level within the particularly closed specialized field of law.

Another theoretical strand is to understand law in connection with its embedded social presuppositions. Here, Kaarlo Tuori's take on a 'hidden social theory' behind legal concepts offers an interesting approach. According to this idea, 'legal concepts and doctrines include at least an implicit or "*hidden social theory*": a conception of the

[19] Rubin EL, 'Law and Society & Law and Economics: Common Ground, Irreconcilable Differences, New Directions' (1997) Wisconsin Law Review 521, 527.

[20] See Luhmann N, *Das Recht der Gesellschaft* (Suhrkamp 1995), 38-41

[21] See Koskenniemi M, *From Apology to Utopia. The Structure of International Legal Argument.* (Reissue with new Epilogue, Cambridge University Press 2005), 568 (emphasis original).

social field under regulation.'[22] With this hidden social theory also comes a certain 'legal culture' as an integral element to the basis of application of law.[23] This means especially, that a specific legal system comes with certain core assumptions of social reality.

This is extremely important for analysing legal issues in connection with surveillance. Assuming that the developments and employment of surveillance technologies are driven by actors and certain systems of security, it is required that the legal regulation of such systems are understood in connection with the presuppositions of the system in place. This phenomenon could be understood in terms of security mindsets, a specific and institutionalized way of approaching security problems.[24] Approaching and solving security problems therewith would depend on the institutionalized understanding of how security problems emerge and how they should be solved.

This particular study choses fundamental rights analyses as a coherent point of approaching security problems in relation to surveillance systems. This naturally presupposes a critical stand towards surveillance as such, however, there are of course other, more systematic, and more critical ways of approach surveillance. In that sense, this study employs a thematic, rather than a systematic way of conducting a problem-based analyses of specific issues deriving from current and future surveillance technologies.

One additional reason for such an approach is that many of the technologies in the security sector have capabilities that have not been subjected to jurisprudence and legal disputes. In addition, many of the technologies do create new legal problems. The question of liability for damages caused by automatically flying Unmanned Aerial Vehicles (UAVs) or of legality of wide-scale surveillance practices of mobile-phone meta-data and location analysis by police forces during political demonstrations could

[22] Tuori K, 'A European Security Constitution?' In Fichera M and J Kremer (eds), *Law and Security in Europe: Reconsidering the Security Constitution.* (Intersentia 2013), 43. See also Tuori K, *Ratio and Voluntas: The Tension between Reason and Will in Law* (Ashgate, Aldershot 2011), 197.

[23] See Tuori's approach to legal culture and '*Vorverständnis*' in Tuori K, *Ratio and Voluntas: The Tension between Reason and Will in Law* (Ashgate, Aldershot 2011), 197.

[24] The idea of security mindsets has been discussed elsewhere: See Kremer J, 'Exception, Protection and Securitization: Security Mindsets in Law.' in Fichera M and Kremer J (eds), Law and Security in Europe: Reconsidering the Security Constitution (Intersentia 2013) and Kremer J, 'Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace' (2014) 23 Information & Communications Technology Law 220.

be two examples. Some of those issues may reach new levels of intrusion with fundamental rights, or even necessitate rethinking whole legal structures such as the recent reform of the EU data protection framework. Consequently, the effects on law and the arising legal questions may be rather broad.

In order to delimit the scope of research, this study takes a scenario-based approach. This means that it will use an exemplary surveillance scenario and test it towards possible legal responses. From this point of view, it will then be possible to identify certain problems and new questions requiring legal responses. From a methodologist point of view, this thesis will hence have a more critical-dialectical background than a normative one. This is probably because underlying this study is the belief that approaches towards surveillance technologies today, due to many factors which will be discussed throughout this text, need to be analysed from a critical perspective, ultimately due to the fact that they run the danger of becoming tools for establishing power imbalances. However, the connecting point between the theoretical discussion and doctrinal approach shall be the use of human rights law as the main reference.

On the one hand, this study takes a theoretical stance in order to analyse the legal theoretical underpinnings behind technology and surveillance. On the other hand, this study attempts to reason doctrinally with the help of the rules and principles for global standards given by international (and European) human and fundamental rights law. It therefore attempts to avoid the many theoretical discussions around the societal and social science aspects of surveillance and control e.g. in its Foucauldian sense,[25] while at the same time giving some room for theoretical discussions about legal arguments on surveillance and control as the subject of this study. Surveillance, technology and control are thereby approached from a critical perspective: in a similar way as human and fundamental rights can be conceptualized as a tool of criticism of control, power and suppression.[26] The social presuppositions underlying societal surveillance and control, paired with their critical-dialectical approach towards the effects of

[25] Much research has been done in the social sciences on the theory, implication and effects of surveillance, up to the point that some may argue for the existence of its own sub-disciplinary field of research labelled 'surveillance studies'. See e.g. Lyon D (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006), Lyon D, *Surveillance Studies: An Overview* (Polity 2007), and Lyon D, Haggerty KD and Ball K (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012).

[26] See e.g. Douzinas C, *The End of Human Rights: Critical Legal Thought at the Turn of the Century* (Hart 2000).

surveillance and control on individual and collective freedoms therefore serve as underlying elements in the search for legal arguments capable of challenging new phenomena, or 'events', deriving from a sophistication of surveillance technologies paired with an increased political will to employ such tools.[27]

In fact, the capabilities and use of technology play a central role in the analysis this study attempts to conduct. And it is here where it chooses to depart from analyses of discourses on surveillance, power and control: technological capabilities play a decisive role for the creation of 'events' which need to be addressed in terms of legal arguments. While those 'events' can very well be understood in terms of power relations and their challenges, it appears that technologies of information collection come with more subtle underpinnings. Particularly holistic surveillance practices often use data sources that are not primarily intended to be panoptical, but have from the outset other purposes in societies. While the Foucauldian panopticon can serve as a method and a model for analyses, a lot of personal data processing does not come with the intention of surveillance of control, but with the purpose to provide a service, conduct business, make profit, or even liberate persons. As often data are essentially by-products of computing, and computing is an essential element of societies, surveillance and control possibilities come as by-products of electronic administration, technological progress and new forms of business and services in modern societies. Consequently, regulation and governance of data processing requires keeping in mind possible responses to disturbances and interferences caused by technologies with surveillance and control capabilities. In order to address the question of compatibility but also suitability for law as a mediating mechanism addressing such effects, this study uses human and fundamental rights as the point of intersection between law and technology, simply because it is interferences with fundamental rights which lie at the centre of the critique of a critique, but also of acceptance of surveillance technologies in European societies.

An additional element of importance in this study is therefore a clear understanding of the function and capabilities of surveillance technologies. In order to analyse legal

[27] Some work has also been done particularly on legal and governance responses to surveillance and control: see e.g. Bennett CJ and Raab CD, *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate, 2003), Bennett CJ, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press 2008).

'events' that may appear as a result of using new technologies, this work employs a fictional surveillance scenario, which is based on a brief analysis of technological capabilities and potential future developments. While the fundamental rights analysis is based on case analyses, the technological part uses a variety of sources both from technical research fields, but also from media and journalism. The surveillance scenario is therefore hypothetical, however, based on existing current technology as well as on prognoses on where developments may lead. In that sense, potential future legal 'events' deriving from surveillance are distilled from an urban surveillance scenario outlined in Section 1.6. Before, however, presenting the scenario, the following sections will briefly discuss terminologies, structure, as well as give an overview that will enable a better understanding of the function, but foremost, the capabilities of surveillance technologies.

***

Terminology and language are essential in law. The mere substance of the subject as such depends on commonly agreed meanings of language and communications. Consequently, it is important to discuss and clarify the meaning of the terms employed in this study, especially because the conceptualizations, notions and meanings of terms in technology and surveillance can be rather broad. Additionally, this study brings together a variety of scientific fields such as the social sciences, technology and law, which may lead to confusion of the terms that are employed in different ways throughout the fields.

The first confusion that may arise in light of this study, is the distinction between public and private. As will be discussed in Section 2.1, this theoretical distinction is highly complex and heavily disputed as well as conceptually problematic. An extensive theoretical discussion of the public/private distinction, however, would exceed the limits of this study. It is therefore important to keep in mind that the term 'public' is mostly used in connection with 'physical' public space. The same applies for all combinations of words containing the term 'public': public sphere, public space or public area relate to physical spaces and zones, if not otherwise described in the context of the discussion. Public surveillance therefore relates to surveillance of public spheres, mostly in its concrete physical, rather than its abstract political sense.

Another issue requires to be mentioned in this context, and that is the use of legal sources. Sources lie, of course, at the core of legal analyses and the particular choice of sources depends on disciplinary considerations. This study employs a variety of legal sources from international law, European law, human rights law and information law. Such as international treaties, sources of EU law, case law and even national law. In some parts, however, this study relies on general legal arguments deriving from the national jurisprudence of EU Member States. Those are employed in order to illustrate different approaches to the problem of privacy in public spaces and naturally do not unfold the same authoritative force on international levels. What matters for the argument in this study, however, is more the theoretical strands of lines of interpretation of surveillance issues in European public spaces. National and constitutional legal arguments are therewith used as a supportive theoretical argument, which function on a different level than international and European legal arguments. It is therefore the focus of possible regulation of European public spaces, rather than the strict focus on a specific field of law which underlies the choice of sources and methodology throughout this study. Additionally, the relationship between legal sources on an international level as such is naturally problematic. The complex relationship between the EU Charter of Fundamental Rights (EUCFR) and the European Convention on Fundamental Right (ECHR) is only one example of essentially different regimes addressing similar issues with similar material and territorial scopes. Those debates, however, would exceed the limits of this study.[28] The combination of focussing on the physical public space (rather than an abstract public sphere) with narrowing the scope of this study (mostly) to a European context, produces the concept of a 'European public space' contained in the title. While it is clear that such a conceptualisation may be challenged, it shall serve as an anchor point for a legal analysis in a globalised world, in which the traditional legal boundaries between jurisdictions and legal systems are more difficult to uphold, particularly when law encounters technologies that operated beyond national and conceptual boundaries.

[28] For further discussions on that issue see e.g. Fischer-Lescano A and Teubner G, *Regime- Kollisionen. Zur Fragmentierung des globalen Rechts* (Suhrkamp 2006); Maduro M, Sankari S and Tuori K (eds), *Transnational Law: Rethinking European Law and Legal Thinking* (Routledge, 2014), Gragl P, *The Accession of the European Union to the European Convention on Human Rights* (Hart Publishing 2013).

1.4 Structure

This study analyses the role and function of the fundamental rights to privacy and the protection of personal data in the context of increasing public surveillance. For this purpose, there are essentially three elements of crucial importance for answering this question.

Firstly, in order to connect the legal analysis to the existing sophistication of surveillance technologies, this study requires an assessment of surveillance technologies and their capabilities and therewith a short description of existing and future surveillance technologies. Secondly, this study discusses questions surrounding the underlying conceptions of privacy (and data protection) as fundamental rights. Thirdly, in order to assess the legal implications of surveillance technologies on the European public space, this study requires a fundamental rights analyses of specific issues that are derived from public surveillance.

Consequently, the structure of this study follows this outline. It is structured into two main parts, where Part One discusses the underlying theoretical frameworks and legal concepts, and part two analyses specific issues in light of fundamental rights protection in the European public space.

This introduction contains an overview of specific surveillance technologies and their capabilities and gives a glimpse into potential near-future application of such surveillance technologies. This includes a description of the development from classic video surveillance systems to sophisticated and highly integrated surveillance networks which analyse vast quantities of data and might even have certain predictive capabilities. It additionally outlines a fictional urban surveillance scenario in order to distil four distinct issues related to the question of fundamental rights applicability in public places and the consequences of different conceptualization: targeted individual surveillance, mass surveillance of public spaces, surveillance through private actors and predictive and automated surveillance.

The first part then starts off by analysing the foundational concept of a European public space and the problem of privacy in public areas in this study. It then turns to the theoretical background of the research question, providing an insight into the legal

theoretical conceptualization of privacy, data protection and security. Within the analyses of a right to privacy, privacy is analysed as a legal concept, outlining the foundation for the distinction between privacy as a concept of liberty and privacy as a concept of dignity and community. It furthermore discussed data protection as a regulatory instrument on the one hand, and as a fundamental right on the other hand. Thirdly, part one of this study analyses security in light of its theoretical complexity, function in surveillance contexts, and in light of the construction of a right to security in Europe. Of particular interest here is the concept of security, including the relationship between security and law as well as the construct of security as a right. Finally, as a fourth issue, part one turns to the more general practical problems of human rights and surveillance, and that is a discussion on permissible limitations to a right to privacy in a global and a European context.

Overall, part one of this study shows that privacy, while originally conceptualized as a liberal individualistic concept, has tendencies in Europe to be understood in terms of dignity and personality and therewith has become a right that forms an essential building block in the ideal of a freedon and dignity based European democratic society.

The Second major part of this study analyses the current European fundamental rights framework in light of the fictional urban surveillance scenario which is based on the technological analyses in the introduction.

The first section in the Second part analyses targeted public surveillance in the sense that surveillance operations here are focused on a particular individual. This is the most classic public surveillance scenario and the analyses draws from the vast body of case law, especially from the perspective of the ECHR.

The second section in part two then turns towards a more detailed analyses of mass surveillance in public places. Here, fundamental rights jurisprudence is analysed towards its capabilities to address and resolve legal disputes arising from the surveillance of large groups or abstract entities.

The third issue addressed in part two focuses on actors, and here particularly on private actors. The public-private divide, the increasing privatization of public spaces as well as increasing possibilities for individuals to acquire and operate surveillance

technologies call for a closer look at the relationship between private surveillance actors and fundamental rights protection.

The fourth and final focus issue in part three then looks at future perspectives: the increased availability of data flows and networks paired with the development of surveillance technologies might have and the consequences of automation as well as the predictive capabilities of future surveillance systems.

Each of the issues therefore addresses separate legal questions in connection to certain fundamental rights aspects. Additionally, beyond mere legal analyses of existing regulations, this part identifies areas of legal uncertainty as well as those that lack regulations and suggests possible solutions. This thesis concludes with a detailed response to the research question outlined in this introduction.

***

The following section will now briefly introduce surveillance technologies. Of particular importance here, is the technological development from classical video surveillance to sophisticated multi-sensor surveillance systems. In that sense, this section will describe different security and surveillance technologies, culminating in a fictional, yet technologically more or less realistic urban surveillance scenario.

1.5 Technology and Surveillance Scenario

Surveillance technology plays a crucial role in this study. One of the core assumptions of this work is that there is a mutual influence between technology and law. New technology requires new regulation, and new regulation influences new technologies. The reason for regulation of technology often derives from the societal effects of technologies, and their potential for changing social life, either for better or for worse. Furthermore, in relation to security, regulation is employed for mediating risks, threats and worst case scenarios.[29] Technology can be very dangerous when seen from this perspective.

For this work, the focal point lies on surveillance and respective technologies enabling surveillance. It explores, how surveillance technology is shaping legal regulation and

[29] See e.g. Sunstein CR, *Worst-case scenarios* (Harvard University Press 2009).

how legal regulation shapes technologies. Foremost, however, the underlying legal sources of this work derive from human and fundamental rights norms, as the overarching norms and principles guiding the regulation of technologies. While this work refrains from a detailed engagement with the relationship between technology and law as such, as well as from a detailed engagement with the philosophical discussions of rights as a concept, it remains important to understand the functionality of security and surveillance technology to assess their impacts on law. Consequently, after outlining the theoretical basis of the affected rights in question, namely the fundamentals of privacy and data protection, this section turns to a more descriptive analysis of the functionality of surveillance technologies. This is important for two reasons: Firstly, to give an overview of the available technologies and their future developments, and secondly, in order to lay the ground for a fictional, but technically realistic surveillance scenario. The surveillance scenario will then enable a legal analysis of specific issues based on the theoretical conceptions of privacy and data protection as rights in the first part.

Surveillance technologies have a long-standing history, and include targeted and non-targeted technologies, but also tactics of espionage and deception.[30] In that sense, classical surveillance technologies were concerned with the gathering of information about specific individuals. Technologies of surveillance have therefore always played a big role in societies, and were especially prominent in repressive regimes in which they were used by the states' security and police authorities. Security and surveillance technologies became more and more sophisticated and efficient, and with the emergence of computers, public registers and bureaucratic administration of public authorities, came the need for technology which could make processing easier and more efficient. While data protection emerged as a tool for regulating states' access to personal information, public surveillance technologies followed different logics than the administrative collection of personal data in registries. Public surveillance is different because it is more offensive surveillance. Unlike the administrative collection of citizens' data, public surveillance is *per se* of a repressive nature. Its very nature is control, not administration.

[30] See e.g. Dandeker C, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Polity 1990).

That said, naturally, security technologies used in public places underwent similar technological improvements as computers and information technologies. In the last 30 years, they became cheap, powerful, efficient and ubiquitous. The driving forces behind those tendencies were digitization[31], miniaturization, the 'sensor revolution' and data processing. As a result, the gathering, storage and analyses of information on persons became easier and more efficient than ever before, a phenomenon which was labelled 'dataveillance' by Clarke already in 1988.[32] In fact, technological advancements have had an enormous impact on public surveillance technologies, and have blurred the borders between the surveillance of public spaces and the surveillance of individuals via data collection, retention and processing. For example, social media data as well as mobile phone communication data can add to the surveillance of a public space equipped with a camera surveillance system. The following Section therefore discusses some of the most prominent technologies and trends in public surveillance.

1.5.1 Video Surveillance

Video surveillance is the first and most obvious surveillance technology in public places and there is probably very few central places in a modern city which are not equipped with video surveillance technology, and today it can be seen as an integrated part of public urban life.[33] Video surveillance first was seen in the 1960s when video cassette recorders enabled the storing of video images and has experienced nothing less but a technological revolution ever since.[34] The simplest technological version of such Closed-circuit Television (CCTV) systems essentially consisted of a monitor which was directly wired to a camera. The monitor then showed an image of an area in real time, much in the same way than if a security person would stand at a corner

[31] For an excellent explanation of the term and its effects see Murray A, *Information Technology Law: The Law and Society* (2nd ed, Oxford University Press 2013), 4-7.

[32] Clarke R, 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498.

[33] See Norris C and Armstrong G, *The Maximum Surveillance Society: The Rise of CCTV* (Berg, 1999), 18; Welsh BC and Farrington DP, 'Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis' (2009) 26 Justice Quarterly 716, 717.

[34] Webster CWR, 'CCTV Policy in the UK: Reconsidering the Evidence Base' (2009) 6 Surveillance & Society 10, 11-12.

and watch an area with her own eyes.[35] Taking electronic images from public places, however, allowed for the integration of additional elements into the CCTV system: Video recorders in order to retain images and for manual review enabled a view back in time, and additional cameras which could be controlled and viewed from a single location enabled the surveillance of larger spaces.

Contemporary video surveillance, however, functions very differently. Three essential elements have changed the core technologies: digitization, integration and the sensor revolution. Digitization essentially means the shift form analogue technology to digital technology which became the technological standard for visual security applications.[36] Digital technology[37] enables more complex surveillance systems as it improves the quality of images as well as the easier and wider distribution of images without quality loss.[38] Furthermore, images can be stored easier and most importantly, enable computers to process visual data, giving rise to an array of new capabilities for visual surveillance systems, for example analysing images.[39] With digitization comes also the capability of integration and networking of surveillance technologies. A surveillance camera which is connected to the internet installed in a home in Finland can be accessed from a mobile phone in Australia. This means also that a variety of controllers in different places can have access to a surveillance system at the same time, and surveillance data of the same surveillance system can be shared and analysed simultaneously in many places.[40] At the same time, an indefinite number of sensors such as video cameras or microphones can be added to the surveillance network, enabling the steady growth and the modifications as well as adding new capabilities and technologies.

---

[35] The argument that being watched by video surveillance in public places is not different than being watched by another person is essentially based on the assumption of a very basic CCTV system.

[36] See Harwood E, *Digital CCTV: A Security Professional's Guide* (Elsevier/Butterworth-Heinemann, 2008), ix- x.

[37] For an excellent detailed explanation of the differences between analog and digital technology, see ibid, 19-37 and Murray A, *Information Technology Law: The Law and Society* (2nd ed, Oxford University Press 2013), 2-14.

[38] Harwood E, '*Digital CCTV: a security professional's guide*' (Elsevier/Butterworth-Heinemann, 2008), 95, 96.

[39] Ibid, 221-223.

[40] Ibid, 99; See also Von Silva-Tarouca Larsen B, *Setting the Watch: Privacy and the Ethics of CCTV Surveillance* (Hart Publishing 2011), 46.

The third element fostering radical change in visual surveillance technologies is the revolution in sensor technologies. Digital image technology is of high quality and the sensors as such became cheaper and more efficient. Many of the digital cameras today are so called dome-or PTZ-cameras (pan-tilt-zoom) which means that they can rotate, tilt and zoon in and out. [41] Actual zoom ranges of such cameras are impressive, when, for example, a camera controller can read a newspaper article on the surveillance monitor over distances of 150m and more.[42]

Consequently, most of contemporary video surveillance systems have developed significantly from the analogue input-output model. Furthermore, video surveillance not only advanced technologically, but also spread at a fast pace: it became a ubiquitous technology in urban public, semi-public and also private spaces.[43] For example in the UK, they have become an 'entrenched' urban feature since the mid-2000s: partnerships between public and private sectors, enormous technical advancements, centrally managed systems as well as a focus from community security to the prevention of terrorism led to a quantitative but also qualitative expansion of security systems.[44] Video surveillance today should be understood more in terms of sophisticated and multi-purpose surveillance networks which embody a wide variety of capabilities, rather than cameras wired to a control room where images are watched by controllers.[45]

1.5.1.1 Purposes and Promises of Video Surveillance

The proliferation of visual surveillance systems often follows an alleged assumption: video surveillance systems somehow would have a positive effect on the environments they observe. The promises of increased video surveillance are manifold and reach from increased public security, over to more efficient security governance to deterrence and the prevention of crime, however, the real and measurable effects of

[41] Ibid, 43.

[42] Ibid.

[43] See Norris C, 'Accounting for the global growth of CCTV' in Lyon D, Haggerty KD and Ball K (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012) 251-258, 252

[44] See e.g. Webster CWR, 'CCTV Policy in the UK: Reconsidering the Evidence Base' (2009) 6 Surveillance & Society 10, 11-12.

[45] For a technological description of networked cameras see Nilsson F and Axis Communications, *Intelligent Network Video: Understanding Modern Video Surveillance Systems* (CRC Press 2008), 21-46.

video surveillance are subject to debate.[46] Studies on the functionality and effects of video surveillance have produced contradicting results. In 2009, for example, a meta-study by Welsh and Farrington found that video surveillance '…is most effective in reducing crime in car parks, is most effective in reducing vehicle crimes, and is more effective in reducing crime in the UK than in other countries.'[47] Beyond the positive effects in car thefts, the study could not find significant impact on other crimes.[48] Also, a 2011 U.S. Department of Justice-funded evaluation of video surveillance systems in Baltimore, Chicago, and Washington D.C. found inconsistent results: while there were measureable reductions of some crimes in some areas, not all the areas showed the same effects:

> Analysis results indicate that cameras, when actively monitored, have a cost-beneficial impact on crime with no statistically significant evidence of displacement to neighboring areas. However, in some contexts and locations these crime reduction benefits are not realized.[49]

Considering the general complexity of crimes as a social phenomenon in public areas, this does not come as a surprise. It should however, be made clear that the assumption of a large positive effect of video surveillance on safety in public spaces is scientifically problematic.

While the studies above primarily focused on the measureable effectiveness of video surveillance in the context of crime, much further research on the impact, perception or function of video surveillance has been conducted in the social sciences. The most recent works address for example the specific analyses on the steady growth and path of success of video surveillance,[50] perceptions and policies of video surveillance

---

[46] See Welsh BC and Farrington DP, 'Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis' (2009) 26 Justice Quarterly 716, 717.

[47] Ibid, 736.

[48] Ibid, 717.

[49] La Vigne NG and others, Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention (Final Technical Report, Urban Institute 2011), http://www.urban.org/sites/default/files/alfresco/publication-pdfs/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.PDF accessed 10 October 2016, 87.

[50] See Norris C and Armstrong G, *The Maximum Surveillance Society: The Rise of CCTV* (Berg 1999), Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge, 2012).

across several European countries,[51] how video surveillance embeds into the core of societies,[52] from a normative and ethical perspective,[53] how video surveillance changes public spaces[54] or video surveillance as a tool for power in surveillance societies.[55] In that sense, video surveillance is often theorized and criticized as a tool of power and suppression and as a tool that has a strong effect in cities, as a tool fostering cities as 'panopticon'.

1.5.1.2 Smart Surveillance and Video Content Analytics (VCA)

The digitization of image technology added another important aspect to the capabilities of surveillance systems: digital images can be processed by computers. This laid the bases for so-called 'smart' security systems in the meaning of '…security augmented by computer-mediated processing.'[56] Computer processing enables detailed and automated analyses of video images in many forms, for example as recognition of patterns or facial recognition. Such video processing technologies are also called 'Video Content Analytics' (VCA), 'Intelligent Video Analytics' (IVA) or just 'Intelligent Analytics' (IA).[57] Digital analytics therefore add capabilities to surveillance systems which previously required time consuming manual analytics. Facial recognition, for example, allows for automatic identification of individuals in public areas, or the search for a certain person in a vast pool of video data. Automated

[51] See Webster CWR and others (eds), *Video surveillance: Practices and Policies in Europe* (IOS Press 2012).

[52] See Kroener I, *CCTV: A technology under the radar?* (Burlington: Ashgate 2014).

[53] See Von Silva-Tarouca Larsen B, *Setting the Watch: Privacy and the Ethics of CCTV Surveillance* (Hart Publishing 2011).

[54] See Koskela H, '"The gaze without eyes" Video surveillance and the changing nature of urban space' in Holmes D (ed), *Virtual Globalization: Virtual Spaces/Tourist Spaces* (Routledge 2001).

[55] See e.g. Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001), 60-68 where the author discusses video surveillance and its relationship to urban consumer spaces.

[56] Ferenbok J and Clement A 'Hidden Changes: From CCTV to 'smart' Video Surveillance' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge 2012), 220.

[57] Video Content Analytics is also sometimes described with the term Intelligent Video Analytics (IVA), see BSIA, 'An Introduction to Video Content Analysis - Industry Guide (BSIA, August 2016), 3 http://www.bsia.co.uk/Portals/4/Publications/262-introduction-video-content-analysis-industry-guide-02.pdf , accessed 15 October 2016; and Ferenbok J and Clement A 'Hidden Changes: From CCTV to 'smart' Video Surveillance' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge 2012), 222-223.

detection of incidents could use movement patterns in order to alert the operators of a surveillance system to certain citations and detect intrusions, hazards, explosions, or unusual behaviour amongst many others. Already shortly after the turn of the century, media reported the employment of behavioural analytics software in the London Underground: Software named 'Intelligent Pedestrian Surveillance System (IPS)' allegedly analysed video data of metro stations and picked out 'unusual' behaviour such as loitering or repeatedly missing trains.[58] The idea behind the software 'Cromatica' developed at London's Kingston University was to identify potential suicidal persons, enabling real-time response and even prevention.[59]

Ever since then, an array of technologies and research projects worked on the sophistication and integration of algorithms for complex video analytics. Other examples of heavily integrated video surveillance analytics are the two EU FP7 funded research projects ADAPTS and INDECT. ADAPTS (Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces) was an FP7 consortium research project from 2009 until 2013 which attempted to develop systems for the detection of 'abnormal' behaviour via video analytics as well as audio analytics.[60] Specifically, the project developed '…visual and acoustical sensor processing and inference mechanisms to automatically detect potentially threatening behaviour of individuals in a group or crowd in large public spaces, e.g., those in relation to public transport or large scale events.'[61] To achieve this, ADAPTS developed a methodology of defining 'abnormal behaviour' on the basis of the academic literature, the analyses of former incidents, the behaviour of video surveillance operators as well as the opinions of experts in the field[62] and distinguished a list of detectable types of behaviour and sound.[63] This was then used in order to develop detection systems in specific

[58] Hogan J, 'Smart software linked to CCTV can spot dubious behaviour' *New Scientist*, 11.6.2003 https://www.newscientist.com/article/dn3918-smart-software-linked-to-cctv-can-spot-dubious-behaviour/ accessed 10 March 2016.

[59] Wakefield J, 'Surveillance cameras to predict behaviour' *BBC News* (1.5.2002) http://news.bbc.co.uk/2/hi/sci/tech/1953770.stm accessed 12 March 2016.

[60] ADABTS, 'Final Report Summary - ADABTS', European Commission, 12 December 2014 http://cordis.europa.eu/result/rcn/153868_en.pdf accessed 12 March 2016.

[61] Ibid, 2.

[62] Ibid, 5.

[63] See ADABTS WP 5 D 5.1 'Vision-based Human Detection and Action Analysis', 21 December 2011,

scenarios, such as terrorism at an airport, crowd behaviour in a stadium and individual behaviour in a city centre.[64]

Following ADAPTS, another FP7 funded research project attempted to achieve similar goals. INDECT, spelled out 'Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment' used a nearly 15 Million EUR research budget in order '…to develop advanced and innovative algorithms for human decision support in combating terrorism and other criminal activities, such as human trafficking, child pornography, detection of dangerous situations (e.g. robberies) and the use of dangerous objects (e.g. knives or guns) in public spaces.'[65] In a similar way as ADAPTS, INDECT attempted to develop the recognition of specific individual behaviours but also added audio analytics to the system and therewith used audio recorded via microphones from public places for the detection of not only 'unusual' behaviours but also 'abnormal sounds.'[66] INDECT, however, went a step further than ADAPTS: it also included a variety of data analytics for criminal forensics and detection in computer networks, which means that INDECT actually attempted to combine real world audio and video surveillance with virtual world data analytics.[67] The project claims that it actually developed a variety of software for police use, for example amongst many others 'high precision crawler technologies navigating the Internet World Wide Web (WWW)', 'software for learning relationships between people and organizations through websites and social networks' and a '…KASS Social Network Analysis system with the functionality dedicated to the analysis of data coming from Internet blogs.'[68] INDECT even

https://www.informationsystems.foi.se/main.php/ADABTS%20D5.1%20Vision-based%20Human%20Detection%20and%20Action%20Analysis.pdf?fileitem=7340162 accessed 16 October 2016, and ADABTS WP5 D 5.2, Task 5.3 and 5.4: 'Sound Source Localization and Analysis', 10 December 2012, https://www.informationsystems.foi.se/main.php/D5.2_Sound_Source_Localization_and_Analysis.pdf?fileitem=7340174 accesssed 16 October 2016.

[64] ADABTS, 'Final Report Summary', (n 60), 6.

[65] INDECT, 'Final Report Summary – INDECT' European Commission, 20 January 2016, http://cordis.europa.eu/result/rcn/175782_en.pdf accessed 17 October 2016, 2.

[66] Ibid, 11.

[67] Ibid, 3.

[68] Ibid, 3.

included a research group on UAVs and their integration into surveillance systems.[69] While the presentation of the project's results appear rather dubious and the project in general has received widespread criticism for its surveillance approaches in the public,[70] the ideas behind such research show a trend towards the integration of a multitude of sensors as well as a rather holistic approach of using real world data as well as data from computer networks for the detection of potential threats.

Returning to visual surveillance, the list of available VCA functions and capabilities is long, however, implementation, practical use and security value vary in quality and usefulness. Nevertheless, a compilation of available algorithms available in 2011 give a glimpse into the surveillance technologies of the future: There exist algorithms for crowd behaviour analyses such as detection of assembly, congestion, dispersion, counting, queuing (waiting time), individual behaviour such as tailgating, loitering, falling/slipping, for creating virtual fences, alarm zones, restricted areas, detecting the direction of a person's movement and dwell time as well as detection of objects i.e. object tracking, abandoned objects, classification, speed, size, vehicle counting, etc.[71] Furthermore, systems can include more complex functionalities such as facial recognition, complex location tracking and automated number plate recognition (ANPR).[72] The usefulness of such a technology for surveillance is obvious: automated analytics of video material and the detection of specific security relevant incidents can make complex visual surveillance systems extremely efficient. Furthermore, such systems can extract information from video and audio material which would either require a large quantity of resources or even be impossible to compile manually.

[69] Ibid, 14.

[70] See e.g. Johnston I, 'EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour"' *The Telegraph*, 19 September 2009, http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html accessed 17 October 2016. Civil society groups and hackers even launched a campaign protesting against the project, culminating in a Europe wide day of protest on the 28th of July 2012, see e.g. the campaign websites http://www.stopp-indect.info accessed 17 October 2016.

[71] See ADABTS, WP3, D 3.1 'Abnormal Behaviour Definition', 23 March 2011, https://www.informationsystems.foi.se/main.php/ADABTS_D3.1_Abnormal_Behaviour_Definition_Public_(PU)_final.pdf?fileitem=7340175 accessed 17 October 2016, 41.

[72] Ibid, 41.

Clearly, such systems have surpassed classical video surveillance, in which the camera was seen merely as an extension of the eye of the observing security guard.

Another important element of VCA in surveillance systems is the ability to search for incidents, persons and object in the retained video material. Theoretically, technologies such as facial recognition or ANPR enable not only the tracking of vehicle in real time but also in the past: with ANPR, for example the location and movement of a suspect prior to an event could be established by programs searching through stored video material.

1.5.1.3 Mobile Cameras and Aerial Surveillance

Projects like ADAPTS and INDECT show that there is an increased interest in developing and employing automated surveillance and detection technologies. However, there are additional factors which could revolutionize surveillance systems further.

Firstly, sensors, including surveillance cameras have become smaller, cheaper and better in terms of quality. Additionally, cameras acquired, as did so many other things, the capability of wireless networking. This means that small and barely recognizable cameras are also much more mobile and connected easily connected to computer networks. Secondly, recent years have also seen a technical revolution regarding robotics: Autonomous vehicles have entered mass markets in all forms and shapes, most prominently as Unmanned Aerial Vehicles (UAVs), so called 'drones'. Drones, furthering the reach of the technology, are ideal carriers of surveillance sensors. F

Regarding the first technological advancement, digital video cameras and the general miniaturization of computer technology led to the appearance of relatively cheap cameras which can be connected to the internet. So-called 'IP cameras', connect either via cable or wirelessly, transmit a video stream without the need to build up separate closed wired or wireless networks.[73] There are now pocket-sized, battery powered cameras with wireless connections to mobile data networks that are highly mobile and difficult to spot. Furthermore, they are widely available on the market and can therefore easily be employed also by private persons. Even a smart phone with the

[73] See Kruegle H, *CCTV Surveillance: Analog and Digital Video Practices and Technology* (Elsevier Butterworth Heinemann 2007), 123.

appropriate piece of software or application can stream video via the internet and can be turned into a surveillance device. This means that it has become very easy to build up relatively cheap surveillance systems both for private as well as public use. Furthermore, mobile cameras allow the ad hoc installation of surveillance networks, for example for a targeted surveillance operation. Networked cameras can also be installed on police cars or worn as body cameras for police officers. Especially body worn cameras have sparked intense discussion about surveillance, police violence and the protection of officers on duty.[74] Mobility, wireless video streaming, and global video access made visual surveillance available to any private individual, any organization, and any government. Sophisticated wide-area surveillance employing analytics should, at least for a couple of years remain a tool for entities with greater resources.

The second technological aspect adding novelty to surveillance systems are UAVs and the possibility to use wide-area aerial perspectives in surveillance systems. While it is still rare that UAV's are elements in static surveillance systems, the possibilities for their use are manifold. Drones equipped with video cameras operating video content analytics technologies could automatically follow targets, or identify suspects and track them, eliminating problems in response times to incident alerts. Furthermore, high resolution cameras could become an all-seeing eye hovering above public spaces.

ARGUS-IS is an example of how such a vision could become reality. In 2009, DARPA issued funding calls for the development of systems for wide area aerial visual surveillance.[75] In the call, DARPA was looking for the development of what they called a 'Persistent Stare Exploitation and Analysis System (PerSEAS)', a system capable of '…automatically and interactively discovering actionable intelligence from wide area motion imagery (WAMI) of complex urban, suburban, and rural environments.'[76] In October 2013, BAE Systems published information about a newly

[74] See e.g Elizabeth J, 'Beyond Surveillance: Data Control and Body Cameras' (2016) 14 Surveillance and Society 133; Moser R, 'As If All The World Were Watching: Why Today's Law Enforcement Needs To Be Wearing Body Cameras' (2015) 7 Northern Illinois University Law Review 1.

[75] See DARPA, Persistent Stare Exploitation and Analysis System (PerSEAS), Broad Agency Announcement (BAA) for Information Processing Techniques Office (IPTO) Defense Advanced Research Projects Agency (DARPA), DARPA-BAA-09-55, 18 September 2009, https://www.fbo.gov/utils/view?id=1d32b1d49cdf59a1e5f8790260c7a350 accessed 17 October 2016.

[76] Ibid, 4.

developed product named 'Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System' (ARGUS-IS), a 1.8 Giga pixel colour camera surveillance system which can be mounted in manned or unmanned aerial vehicle in order to enable persistent detailed surveillance over a 15 square mile area at 20,000 feet (about 6km) hovering height.[77] The produced visual image, clear enough to see moving objects such as cars but also persons, is streamed to the controller, who can zoom into more detailed perspectives both in real time as well as in the recorded data.[78] The usefulness of such systems for urban surveillance are obvious: especially paired with data- and video content analytics, systems such as ARGUS IS and others would be capable of creating persistent real-time visual surveillance from the sky, including the detection of 'anomalies' and the tracking of pre-defined targets.[79] In the US at least, it seems that aerial surveillance has become a standard practice in policing, albeit exact information on the details of the surveillance systems employed are not publicly available.[80]

Persistent surveillance from the sky using sophisticated image technology and data processing adds a new dimension to urban surveillance. Integrating UAVs into complex surveillance systems gives operators another layer of unprecedented public surveillance capabilities.

---

[77] See BAE Systems Columbia, 'Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS)' CS-13-F97-ARGUS-IS-Brochure, 10/2013 http://www.baesystems.com/en-sa/download-en-sa/20151124113917/1434554721803.pdf accessed 15 April 2016.

[78] See Stanley J, 'Drone "Nightmare Scenario" Now Has A Name: ARGUS', American Civil Liberties Union ACLU, 21 February 2013, https://www.aclu.org/blog/drone-nightmare-scenario-now-has-name-argus?redirect=blog/technology-and-liberty-free-speech-national-security/drone-nightmare-scenario-now-has-physical accessed 15 April 2016.

[79] See also Stanley J, 'Report Details Government's Ability to Analyze Massive Aerial Surveillance Video Streams' 5 April 2013 ACLU, https://www.aclu.org/blog/report-details-governments-ability-analyze-massive-aerial-surveillance-video-streams?redirect=blog/technology-and-liberty-free-speech-national-security/report-details-governments-ability-analyze accessed 15 April 2016; Timberg, C 'New surveillance technology can track everyone in an area for several hours at a time' *The Washington Post*, 5 February 2014, https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html accessed 12 April 2016.

[80] On the 6th of April 2016, the internet media company BuzzFeed published a report on aerial surveillance practices. Using aircraft location data from the flight tracking website Flightradar24, the report tracked about 200 surveillance planes operated by the FBI and the DHS between August and December 2015, presenting an overall picture of the extend of aerial surveillance on maps. See Aldhous P and Seife C, Spies in the Sky, BuzzFeed.com, 6 April 2016, http://www.buzzfeed.com/peteraldhous/spies-in-the-skies accessed 12 April 2016.

1.5.2 Ubiquitous Sensors and Networks

Surveillance possibilities have improved dramatically. Naturally, this is due to the development of electronic devices and technological inventions that have been permeating everyday life during the last decades. Smart phones and computer networks are only examples of a row of technologies which have changed ways of work and life in modern societies. Today we are surrounded by an array of devices, microcomputers and sensors that collect, transmit and retain data in many forms and shapes. The European Commission's Information and Communication Technologies Advisory Group (ISTAG) has described this phenomenon as 'Ambient Intelligent Environment', in which 'humans will, (…), be surrounded by intelligent interfaces supported by computing and networking technology that is embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials - even particles of decorative substances like paint.'[81]

In addition, Information and Communication Technologies (ICTs) are '…an integral part of almost anything we do (…) – We have moved from society of human communication only, into a world of Internet of Things – where machine-to-machine communication will be a large part of future communication.'[82]

Apart from this 'internet of things' and ubiquitous digital communication between people and devices, another trend has become visible: One prerequisite of such scenarios and visions is the fact that an increasing number of electronic devices can 'interface' with the real environment. This means that there is an increasing number of sensors of all forms and shapes embedded in people's environments. For example, sensors in mobile phones today include sound and touch sensors and future developments are moving towards the expansion of interface options enabling 'cognitive computing' as devices will be able to learn and adapt to their environments.[83] Other examples show the increasing possibilities to use networked

[81] Stanley J, Drone 'Nightmare Scenario', (n 78), 7.

[82] ISTAG, Working Group on International Cooperation: ICT research and innovation in a globalized world. A contribution for thinking strategically the role of international cooperation in EU ICT research and innovation. March 2012, http://cordis.europa.eu/fp7/ict/istag/documents/ict-research-and-innovation-final-72pp.pdf accessed 3 October 2014, 12.

[83] Lohr S, 'IBM Looks Ahead to a Sensor Revolution and Cognitive Computers.' *The New York Times: Bits*, 17 December 2012, http://bits.blogs.nytimes.com/2012/12/17/ibm-looks-ahead-to-a-sensor-revolution-and-cognitive-computers/ accessed 3 October 2014.

sensors for environmental monitoring[84], or the development and improvement of various sensor types, such as, e.g., the integration of chemical sensors in sensor networks.[85] Hence, today there are more types of sensors, sensors are becoming smaller, cheaper, ubiquitous and networked and this trend is likely to increase in the recent year. This sensor revolution has consequently huge implications for surveillance technologies. Not only are the technical capabilities of sensors specifically built for surveillance technologies, such as, e.g., video cameras, microphones or movement sensors, but more and more networked 'everyday' sensors can be used for surveillance and integrated in complex surveillance systems. Many of the NSA surveillance practices that were revealed by the Snowden-Files in summer 2013,[86] for example, were based on data-stream analytics. Such data streams, however, become more and more available through the proliferation of sensor networks recording information, amongst them sensitive information about individuals such as heart rate, movement profiles, body temperature, mood etc. Body sensors in so-called 'wearables' –electronic devices that embody a variety of sensors, for example smart-watches are complemented with technological developments in smart homes or home automation. Furthermore, wide sensor networks can be installed in wide areas of public space – and they can be integrated into surveillance systems as well. Improved sensors, their networks and proliferation hence dramatically improve surveillance capabilities in many ways.

1.5.3 Biometrics

The term 'biometrics' contains a variety of different technologies, some more relevant for public surveillance than others. In general one way of defining the term 'biometrics' can be as '(…) the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person.'[87] The general

[84] Green H, 'Sensor Revolution: Bugging the World. Soon, sensor networks will track everything from weather to inventory.' *Bloomberg Business Week Magazine*, 24 August 2003, http://www.businessweek.com/stories/2003-08-24/tech-wave-2-the-sensor-revolution accessed 3 October 2014.

[85] Byrne R, Benito-Lopez F and Diamond D, 'Materials science and the sensor revolution' (2010) 13 Materials Today 16, 16.

[86] See Greenwald G, *No Place to Hide,* (n 3).

[87] Jain AK and Ross A, 'Introduction to Biometrics.' in Flynn PJ, Jain AK and Ross AA (eds), *Handbook of Biometrics* (Springer 2008) 1-21, 1.

idea is that 'measureable physical properties'[88] are used to uniquely and securely identify individuals as those attributes –such as for example fingerprints or DNA profiles – do not change during a person's lifetime.[89] As such, biometrics can have many forms and shapes, but they all serve the purpose of enabling reliable identification of persons in various environments. Those forms can roughly be separated between physical biometrics and behavioural biometrics. Physical biometrics include features such as finger- palm- or hand prints, face, iris, retina, signature, gait, voice, ear, hand vein, odour or DNA.[90] Behavioural biometrics can for example include certain special patterns such as a person's signature or specific personal typing pattern on a keyboard.[91]

Biometric systems come with certain technological pre-requisites. First, a sensor needs to take a person's biometric data. This can be for example a fingerprint reader, an iris scanner or a video camera filming a face. Secondly, the data needs to be processed. In more detail, the data quality is assessed, the data is translated into a biometric template and the data is compared to adequate reference data.[92] Thirdly, the data or template is stored in a database, possibly in connection with information on the identifiable individual.[93] It goes without saying that biometric systems are often highly complex and require many different technical blocks and stages in order to function in a reliable and efficient way and it is not the intention of this chapter to provide an exhaustive definition of systems, compounds and their efficiencies.[94]

---

[88] Mordini E, Tzovaras D and Ashton H 'Introduction' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 1-21, 7.

[89] See De Hert P 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions.' in Campisi P (ed), *Security and Privacy in Biometrics* (Springer 2013), 369-413, 370.

[90] Jain AK and Ross A, 'Introduction to Biometrics.' (n 87), 3.

[91] Ibid, 4. For a list and explanations of popular biometric modalities see also Jain AK and Kumar A 'Biometric Recognition: An Overview.' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 49-80, 50-54.

[92] See Jain AK and Ross A, 'Introduction to Biometrics.' (n 87), 5.

[93] Ibid, 4-6.

[94] For further literature on specific biometric systems and discussions on their various technical issues see Flynn PJ, Jain AK and Ross AA, *Handbook of Biometrics* (Springer 2008), Modi SK, *Biometrics in Identity Management: Concepts to Applications* (Artech House 2011), Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), Campisi P (ed), *Security and Privacy in Biometrics* (Springer 2013)

Today, biometric technologies appear in all kinds of systems and devices and they can play an important role in modern surveillance systems. Biometrics or biometric authentication[95] are applied, for example, in access control, passports, criminal investigations, border control, video surveillance, employees time tracking, identity management and unlocking mobile phones, amongst many others. As such the use of biometric technologies can be classified in different usage groups: Commercial, government, forensics,[96] and personalization.[97] In forensics, biometrics such as fingerprints or DNA samples are used to identify perpetrators or corpses. Governmental application includes identity management for ID documents, border controls, healthcare, public administration, etc. Commercial application encompasses many commercially distributes application of biometric technologies such as access control, employee tracking, personal identification and authentication in banking and consumption, including a strong need to reliably identify individuals in online commercial activities. Today, biometrics are also used in private security applications where they are already a standard, such as for example many smart-phones and computers can use finger prints to identify users. In addition to the forensic, governmental and commercial use of biometrics, Shimon Modi adds what he calls future 'Personalization/context-aware applications'.[98] Those are systems that connect certain personal biometric features to personal adjustable systems, such as, for example, a car seats automatically adjusting to a specific driver, a car security system recognizing tiredness, or a smart home activating a preferred light setting by an inhabitant connected to a finger print. Many of those, however, would also fall into the category of commercial applications.

Today, one can envision an endless amount of possible uses for biometrics for a myriad of purposes. Biometric technologies have advanced dramatically in recent years in their distribution, application and efficiency and they will continue to advance. Together with the sensor revolution, biometrics will continue to improve and will proliferate. In addition, biometrics will increasingly be found in large-scale

[95] See Jain AK and Ross A, 'Introduction to Biometrics.' (n 87), 1-2, fn 4 for remarks on the term.

[96] Ibid, 12.

[97] Modi SK, *Biometrics in Identity Management: Concepts to Applications* (Artech House 2011), 12-13.

[98] Ibid, 13.

applications such as national ID systems, e-commerce and an array of security applications.[99]

Generally, biometrics can play a crucial role in large-scale surveillance systems. Naturally, some of the systems and traits are more suitable for surveillance then others. So are fingerprint or DNA samples less relevant for surveillance systems than facial recognition or certain personal pattern recognition. Biometrics have always played an important role in surveillance and forensics for example when it is necessary to identify a perpetrator on a video tape. The improvements of biometric technologies, however, have made it possible to integrate certain biometric recognition technologies into surveillance systems to enable real-time recognition of persons.[100] Facial recognition is the most prominent example of how surveillance capabilities have improved in the recent years, but also pattern recognition such as keystrokes or gait could be used to identify individuals in a surveillance context.

1.6 The Urban Surveillance Scenario

In order to illustrate the theoretical capabilities of such modern smart surveillance systems, this study will use an urban surveillance scenario. Although the scenario as such is fiction, many of the technologies exist, function, and are part of many smart-cities projects all over the globe.

The scenario takes place in the city of Helberg somewhere in Northern Europe. Helberg is a capital of country X with a little over 1.5 million citizens, the seat of the government including many ministries, the legislative including a parliament. Helberg is situated on the coast and has a large passenger and industrial harbour as well as a large airport. Due to this, Helberg is the political, cultural, industrial and commercial centre of the country. Helberg ranks average in terms of crime statistics as well as social stratification. Helberg has a touristic town centre including many culturally and historically valuable sites. Helberg runs a centralized video surveillance system.

---

[99] Jain AK and Ajay Kumar 'Biometric Recognition: An Overview.' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 65.

[100] See Tistarelli M, Barrett SE and O'Toole AJ, 'Facial Recognition, Facial Expression and Intention Detection' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 229, 230.

The system is installed in the city centre; the boundaries are the inner ring road of the city. The city centre is equipped with 10000 state-of-the-art PTZ cameras, enabling coverage of almost 95% of public spaces within the inner surveillance zone. Furthermore, those cameras are equipped with microphones that can access sounds close to the cameras. Third, the centre is equipped with 500 radiation sensors. In addition to the fixed cameras, all police vehicles are equipped with permanently recording mobile video cameras.

Furthermore, the police authorities operate several unmanned aerial vehicles (UAVs) which fly above the city in 12 hour shifts. Those UAVs are equipped with an Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), a surveillance system capable of tracking moving objects such as cars and persons by filming and recording around 100 square km of city area form the air. The ARGUS Imaging System is controlled from the police surveillance centre and is used for real-time tactical police operations such as in mass events or for investigations and forensics, for example in cases of major traffic accidents or crimes.

All the surveillance sensors are connected via fibre-optic cables to a central control centre operated by the police. The control centre retains all collected data for 30 days and is equipped with powerful computers running various types of video analytic software. The surveillance system is therefore capable of automated number plate recognition (ANPR), facial recognition, person and object tracking as well as motion analytics and a wide array of Video Content Analytics (VCA) technologies. The system can also be configured to set different surveillance intensities to specific areas.

For example, the system operates behavioural analytics software in all central car-parks which can automatically identify behaviour typically related to car theft such as the loitering of a group of people and subsequently alert the security centre staff. Furthermore, the system also monitors drivers' compliance with parking regulations in the inner city. Generally, the system operates on an alert-on detect basis. This means that it constantly analyses the incoming sensor data stream and alerts security personnel when a pre-programmed event appears. The levels of sensitivity and the 'anomalies' and 'incidents' which the system detects can be adjusted and set by the operator.

In order to achieve a high level of coverage within the city, public authorities have entered into a variety of public private partnerships in the security field: as a consequence, much of the surveillance data comes from sensors operated by private stakeholders, for example cameras in car parks and shopping malls. Furthermore, a majority of data is collected by private security companies that operate surveillance systems in large areas such as the stations, metro trains, trams, and busses of the city's public transport system.

The system is therefore capable of aiding the execution of a high level of control over vast public areas in the city. The scenario illustrates surveillance and control capabilities, which if implemented, come with a variety of concerns, particularly for the right to privacy of citizens.

This surveillance scenario is hypothetical. The following Sections will identify elements of the scenario with core relevance for a legal analysis. The technological descriptive analyses above have shown that modern urban surveillance no longer is merely about one technology, but about an accumulation of several technologies combining sensors, hardware and software and about complex data analytics and data processing operations. In that sense, modern urban surveillance is not somebody watching a screen and others being watched, but about complex algorithms that automatically and independently control and regulate spaces.

With this, urban surveillance systems have the potential to shift from being rather independent and autonomous 'closed circuit'- systems towards meta-systems that access the treasure troves of big data, social media, smart-city data and the wide variety of available sensor data in order to surveil areas and individuals, control spaces and even forecast events. Recursively, such surveillance systems can feed back data into the variety of other smart city systems that control for example traffic flows, public transport systems or the electronic grid.

Consequently, modern public surveillance will not merely conduct surveillance for reasons of security, but will be a highly complex combination and networks of technologies and sensors that simultaneously administer, regulate, control and surveil large urban spaces.

With this, the borders between classical security surveillance systems and smart administrative and regulative systems become blurred and distorted. In fact, access to data, data mining and methods of data processing are playing an increasingly important role in our capabilities to control public spaces.

The consequences of this are manifold, but there are certain issues that need to be re-thought when approaching this from a legal perspective. The following sections will analyse certain aspects and tendencies of such overarching surveillance that appear in this urban scenario from a fundamental rights perspective, particularly a right to privacy and data protection and their conceptualizations between human dignity/personality and individual liberty. A special focus will be directed towards the gaps and missing connections in the current jurisprudence of European Courts on the issue.

The analysis is structured along the lines of legal issues arising in the scenario and does not necessarily follow classical schemes of testing fundamental rights intrusions. As many problems in the scenario dealing with uncertain legal grounds and a lack of jurisprudence, much focus will be on the applicability and scope of current European fundamental rights. The following analyses is structured in a thematic rather than a schematic way.

2. Conceptions of Public Space, Privacy, Data Protection and Security

This section addresses the theoretical conceptualizations of privacy and the fundamental conceptual antagonisms one must face when engaging with privacy in public places. The question what does privacy in a public context mean, necessitates a deeper theoretical engagement with privacy as a concept on the one hand, and the public private distinction on the other. Yet, certainly a lot of those stories have already been told and will not be told again here. Nevertheless, some of the theoretical foundations do need mentioning because they play a fundamental role in the questions that appear when dealing with privacy and control in public spaces in light of an analyses of the scenario above.

2.1 'Private' and 'Public' Physical Space

One of the core underlying issues in his study derives from the distinction between public and private spaces. In that sense, referring to the scenario above, much of the surveillance happens in physical public spaces in the city of Helberg, and in that sense in areas that can be somehow distinguished from 'private' spaces. One of the first questions deriving from the surveillance scenario requires a distinction between physical 'public' and physical 'private' spaces.

In many ways, much of the theoretical work on privacy draws on the distinction between spaces: it appears intuitive that the privacy framework is different depending on the physical space in which an issue is located. In a private bathroom, privacy appears to work differently than in the centre square of a town. In a similar way, the distinction between public and private does play a role in the legal assessments of surveillance technologies. The applicable legal frameworks vary, depending on the physical space: Surveillance systems operated on a public space appear less intrusive than in a private space, consequently they might be regulated differently.

This section will look at conceptualization of public spaces and its legal ramifications. Furthermore, the distinction between public and private have consequences for the underlying conceptions of privacy. The right to be let alone comes with a distinct interpretation of space than the concept of control of information. Yet, most of the privacy approaches distinguish between a public or a private, an inner and an outer

sphere. Controlling one's personal information, for example, means controlling the zones through which information shifts from a personal into a public sphere. Those concepts will be discussed in Section 2.2 below.

While the relationship between privacy and publicity is naturally not easy to delineate, the question arises to what extend a distinction between physical public and private space can be approached from a legal perspective. In fact, there are many ways of legally defining public space, and all come with their own problems and weaknesses.

The Venice Commission, for example, defines public areas as

> …a place which can be in principle accessed by anyone freely, indiscriminately, at any time and under any circumstances. Public areas are open to the public. In principle anyone at any time can have the benefit of this area. A person benefits freely from public areas. Public areas are governed by public authorities whose power to enforce the law and intervene are wider than within private property.[101]

At first sight, this definition makes sense. Public areas are spaces, which are publicly accessible as well as publicly controlled, governed and administered. However, it is also obvious that there are public places today that are somehow public and yet come with restricted access. Train stations and airports are such examples of a public space, which could be owned and administered by a public entity but yet where access is restricted to those holding a travel ticket. In addition to this, there are also spaces that are publicly accessible, however, only during certain times (e.g. city libraries) or that are even privately owned (such as shopping malls, supermarkets or restaurants. In fact, modern urban spaces today are composed of a variety of publicly or privately owned or administered physical spaces that are only accessible upon the fulfilment of certain conditions. In that sense, strictly speaking, the above-mentioned Venice Commission definition does not cover areas that are not indiscriminately open to the public, or that are not open at all times. If indiscriminate and unrestricted openness is problematic as a criterion, how else could 'public areas' be distinguished from 'private' areas?

Gary Marx gave a nuanced private and public space distinction: he emphasized the need to understand the distinction rather as multi-dimensional and fluid than as fixed and rigid and laid out a list of dimensions of the public-private distinction, such as

[101] European Commission for Democracy through Law (Venice Commission), Opinion on Video Surveillance In Public Places by Public Authorities and the Protection of Human Rights, 23 March 2007, Study No. 404/2006, CDL-AD(2007)014, para 8.

geographical locations, information, communication, expectation and social role and status.[102]

One of Marx's elements for a legal definition of physical public space, however, was that public spaces were 'geographical places as determined by law'.[103] Marx emphasized that the distinction here depended on the accessibility of space from a formal legal perspective and that while public space could be entered or left without constraints, the accessibility of a private space could legally be regulated by the private owner.[104] It is interesting that this definition relies on the formal legal status of a physical space in order to define its 'private' or 'public' nature. This definition, however rests on the legal right to access. However, even here, the distinction is legally tricky. Access to public spaces can be legally restricted, for example when there is a curfew. Public parks can have very strict rules for access and behaviour and public bathrooms do have a very strict element of accessibility restrictions, if they are occupied. Marx therefore rightly noted that many public areas still could be very difficult to access, for example, a jungle or the peak of a mountain.[105]

Hence, besides the accessibility criteria, the legal status appears to be an important element when distinguishing 'public' from 'private' physical areas. In that regards, also the Venice Commission definition contains an element of legal scope: 'Public areas are governed by public authorities whose power to enforce the law and intervene are wider than within private property.'[106] In that sense, scope and applicability of law play an important, if not a decisive part in defining what is a physical 'public' area.

It is striking, though, that legal definitions of what constitutes a physical public space are in practice either avoided or defined in relation to its opposites. In the CJEU *Ryneš* case, for example, the Court conceptualized public space as the space which is not private: The fact that camera surveillance was directed to the space outside of the private area was decisive in the decision concerning the 'household exemption' of

[102] Marx G, 'Murky conceptual waters: The public and the private' (2001) 3 Ethics and Information Technology 157, 160, 161.

[103] Ibid, 161.

[104] Ibid.

[105] Ibid 161, 162.

[106] Venice Commission, Opinion on Video Surveillance, (n 101), para 8.

article 3(2) of the European Data Protection Directive.[107] In the CJEU Judgement, public space was therefore defined through its explicit distinction from the private space.

Examples of legal definitions in relation to public spaces can also be found in many national jurisdictions. In the UK, for example, a 'public place' pursuant to the 1936 Public Order Act, includes, '…any highway (…) and any other premises or place to which at the material time the public have or are permitted to have access, whether on payment or otherwise.'[108] Here, public places are defined through accessibility, although the fact that entrance fees or other restricting mechanisms can prevent entry are not decisive for separating a public place from a private one.

In France, 'public places' required definition for a law prohibiting the concealment of one's face in public.[109] In article 2, the law states that '…l'espace public est constitué des voies publiques ainsi que des lieux ouverts au public ou affectés à un service public.'[110] This means that, besides accessible roads and places, the law also bans the concealment of one's face in areas assigned to a public service. In a Prime Minister's Circular of 2nd of March 2011 on the law, places open to the public include both unrestricted and conditional access areas, in so far as 'as any person who so wishes may meet the requirement (for example, by paying for a ticket to enter a cinema or theatre).'[111] Here, the comment explicitly includes privately owned areas of commercial use into the scope of public places, as well as 'banks, stations, airports and the various means of public transport'.[112] Furthermore, places assigned to a public service in the meaning of the law

> …are the premises of any public institutions, courts and tribunals and administrative bodies, together with any other bodies responsible for providing

[107] See Case C‑212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, Judgement, Court (Fourth Chamber), 11 December 2014, ECLI:EU:C:2014:2428, para 33.

[108] See UK Public Order Act 1936 (1 Edw 8 and 1 Geo 6, Chapter 6), Section 9.

[109] See Loi no. 2010-1192 du 11 Octobre 2010: interdisant la dissimulation du visage dans l'espace public. JORF no 0237, 12 October 2010; The law was subject to scrutiny by the ECtHR in S.A.S. v France concerning the ban on full-face veils in France. See *S.A.S. v France*, App no. 43835/11, Judgment, Court (Grand Chamber) 01.07.2014.

[110] Article 2 I. 'public places comprise the public highway and any places open to the public or assigned to a public service'.

[111] See *S.A.S. v France*, App no. 43835/11, Judgment, Court (Grand Chamber) 01.07.2014, para 31.

[112] Ibid.

> public services. They include, in particular, the premises of various public authorities and establishments, local government bodies and their public establishments, town halls, courts, prefectures, hospitals, post offices, educational institutions (primary and secondary schools, universities), family benefit offices, health insurance offices, job centers, museums and libraries.[113]

Consequently, in France, and regarding concealment of one's face, public places are defined as vast areas of life and daily activities, excluding only the mere sphere of an individual's own apartment or private residence. In such conceptions, it appears that everything comprises public space, except physical spaces that are walled in, shielded and locked off.

Another example of how to address the complex nature of public space for legal purposes, can be found in German jurisdiction: Here, a public road becomes a public space through official labelling, following an administrative procedure.[114] Once a street is constructed and officially labelled, it becomes a public area on which general public traffic regulations apply as regulated in the 'road traffic order' (Strassenverkehrsordnung, StVO).[115] According to the administrative act on the 'road traffic order', however, public traffic regulations also apply in areas which are not labelled by a public authority but on which the holder of the right to disposal has accepted or tacitly tolerated public traffic.[116] This means that public traffic regulation only does not apply in an area, if that area is clearly and effectively blocked from all sorts of public traffic.

In this example, public areas are delineated from private areas by *de facto* accessibility and an administrative designation. In that sense, the law distinguishes between public areas, semi-public areas and private areas. Public and semi-public space then share the same rules, only strictly private areas might be subject to exemption from such regulation. What matters here, is the intended or unintended openness and accessibility, hence the character of the space.

---

[113] Ibid.

[114] This is regulated in the several laws of the federal states (Länder), see e.g. Bayerisches Straßen- und Wegegesetz (BayStrWG), BayRS V, S. 731, 5 October 1981, Art 6.

[115] See Straßenverkehrs-Ordnung (StVO) (Road Traffc Order), Verordnung vom 06.03.2013 (BGBl. I S. 367), in force since 01.04.2013, (BGBl. I S. 1635, m.W.v. 30.10.2014).

[116] See Allgemeine Verwaltungsvorschrift (General Administrative Order) zur Straßenverkehrs-Ordnung (VwV-StVO), vom 22. Oktober 1998, in the version of 11 November 2014, para 2 (zu §1 II).

These example show some formulations of definitions of public spaces in law. While many of the definitions are limited, it is clear that the relationship between concepts of privacy and legal definitions of space are important for legal arguments addressing the surveillance of public spaces. Especially crucial here is the application of the legal scopes: territorial, personal and material scopes of laws are crucial particularly for fundamental rights arguments.

Regarding public surveillance, the legal distinction between physical public and private space is important for two reasons. Firstly, the categorization of physical space is important for the scope and applicability of laws. Secondly, the definition of public and private spaces has a significant effect on the applicable legal arguments regarding surveillance practices. This will be discussed in more detail in relation to the legal conceptions of privacy below.

For now, it is important to conclude that there are many legal definitions of physical public and private space, containing different elements, such as accessibility, openness, legal designation, or ownership and governance. In connection with the urban surveillance scenario of Helberg above, this raises a variety of issues. Firstly, much of the sophisticated surveillance technologies are directed at physical public spaces that fall under at least one of the public space definitions above. This means that persons that place themselves outside of their own secluded and locked spaces will necessarily expose themselves to some of the described surveillance technologies. Some of the described surveillance technologies additionally might even reach into the physically secluded spaces of a locked off and principally inaccessible 'private' physical spaces. Mobile phone tracking, or holistic aerial surveillance, for example, potentially produces location data of persons also once they are inside allegedly secluded private physical spaces. The potential different treatment of surveillance practices in relation to the location of its target is problematic, as individuals in Helberg might be subject to surveillance regardless where they roam, may that be inside a privately-owned shopping mall, a public library during opening hours, a metro station or even inside their private vehicles on a motorway.

This study therefore employs a rather wide conception of physical public spaces, a conception based on accessibility of space and corresponding effects of surveillance. The conception of 'public space' for the purpose of this study therefore contains all

areas and spheres in which individuals can be subject to surveillance and affected by the surveillance technologies described above. As already indicated above, however, for the detailed legal analyses, the territorial scope of this study shall be limited to Europe, and therefore European public spaces. Although it is limited, for the purposes of this study, public space shall therefore be understood as an open and accessible physical space in which individuals are *de facto* subject to the surveillance technologies describes in the scenario.

The following section turns to the legal conceptualization of privacy, before this study discusses different aspects of the application of privacy in physical public spaces.

2.2 Privacy as a Legal Concept

The second important concept underlying this study on surveillance of public places, is the legal concept of privacy. This section therefore requires a discussion of the concept of privacy and its application and function as concerns public spaces. This discussion is important, particularly because it lies at the core of questions associated with the relationship between surveillance of a public space and surveillance of private spaces. In fact, the legal reasoning on interferences through and justification of surveillance of public spaces depend on the underlying understanding and conceptualization of privacy. This section therefore discusses several concepts of privacy and analyses their relationship and applicability to public space surveillance, leading to a discussion of privacy in public.

Of course, presenting a unique and holistic classification would quickly stress the frame of this study. Many attempts have been made to grasp privacy in all its forms and classify its many components from a variety of disciplinary perspectives. It is important to stress that a legal conception of privacy may vary significantly from philosophical concepts of privacy, and that legal typologies tend to be specific to a particular legal system or legal culture.[117] This section nevertheless focusses on privacy as a legal concepts, namely privacy as a right in order to address the conceptual issues of privacy in public spaces, in an attempt to understand privacy in public from a perspective of international – or transnational law and therewith through the lenses of privacy as a human right.[118]

2.2.1 Privacy as the Right to Be Let Alone

A legal conceptions of privacy following the lines of the common narratives, starts off with Warren and Brandeis' 1890 conception of a right to privacy as a 'right to be let

[117] See Koops B-J and others, 'A Typology of Privacy' (2016) University of Pennsylvania Journal of International Law, Forthcoming; Tilburg Law School Research Paper No. 09/2016, https://ssrn.com/abstract=2754043 accessed 10 January 2017, 5.

[118] Many scholars have developed conceptualizations, typologies and taxonomies of privacy. See especially Solove DJ, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087 and Solove DJ, *Understanding privacy* (Harvard University Press 2008), Finn L, Wright D and Friedewald M, 'Seven Types of Privacy' in Gutwirth S and others (eds), *European Data Protection: Coming of Age* (Springer 2013), Allen AL, *Unpopular Privacy: What must we hide* (Oxford University Press 2011) and very recently Koops B-J and others, 'A Typology of Privacy', (n 117). For a philosophical analysis of privacy, see Richardson J, *Law and the philosophy of privacy* (Routledge 2016).

alone'.[119] There is not much academic writing on the right to privacy that does not refer to Warren and Brandeis' article. Published in 1890 in the Harvard Law Review, the article today often counts as the historical starting point of a legal right to privacy.

The storylines behind the article vary, but the authors' main motives appear to be rooted in the emergence of aggressive and invasive practices of journalism in the US from the midst-19th century onwards. Technological advancements such as mass print media and photographs contributed to the proliferation of newspapers, especially between 1850 and 1890, when the number of readers in the US increased from 800.000 to 8 Million.[120] In their article, Warren and Brandeis argued for a new right to privacy and conceptualized it as the right 'to be let alone', deriving from Thomas Cooley's definition of personal immunity.[121] In 1880, Cooley conducted a classification of legal rights, in which he conceptualized amongst others the right to immunity from attacks and injuries and the right to life as 'personal rights'.[122] He understood personal immunity as '[t]he right to one's person may be said to be a right of complete immunity: to be let alone.'[123]

In their 1890 article, Warren and Brandeis took up the concept of inviolate personality and argued in favour of the introduction of a new right – the right to privacy. They argued that especially due to the spread of print media and photography, individuals were in need for better protection against harms.[124] According to them, the protection of the individual necessitated the formulation of a new right, simply because existing mechanisms of protection such as against slander or libel, copyright violations or the protection of property were not sufficiently developed in that regard. While the right to life protected from physical assault and the threat of death, while slander and libel protected individuals from direct assaults, and while the right to property protected tangible and intangible forms of possessions, there was consequently also a need to

[119] Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 194.

[120] See Solove DJ and Schwartz PM, *Privacy, Information, and Technology* (3rd edn, Wolters Kluwer Law & Business 2011), 11.

[121] See Cooley TM, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Chicago 1880), 29.

[122] Ibid, 24.

[123] Ibid, 29.

[124] Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 194, 195.

expand those concepts and form a right that would protect individuals from being exposed to a public audience, from having letters opened and read[125] and from their portraits being published.[126] As a consequence, Warren and Brandeis grasped the right to privacy as personal injuries done to individuals by another party, on the same level with '…the right not to be assaulted or beaten, the right not to be maliciously prosecuted, the right not to be defamed.'[127] In addition, the authors added that this did not derive from legal principles surrounding private property, but from the 'inviolate personality' of the affected person.[128]

Warren and Brandeis hence argued, that Common Law Courts in the US had already been applying certain realms of protection that fell into the scope of a right to privacy, however, by subsuming them under expanded versions of other rights, such as the right to life or copyright. Consequently, a new formulation of a right to privacy would enable better protection against individual harm. What is interesting is that the right to privacy was conceptualized from a private law perspective. Warren and Brandeis did not primarily see the state and its agents as causing interferences with an individual's right to privacy, but rather other individuals or the press. Privacy was therefore conceptualized as a right to be let alone, not exclusively by the state, but also by other individuals.

Additionally, Warren and Brandeis relied strongly on the concept of a personality right, when they defined the right to privacy as a '…more general right of the individual to be let alone'[129] which was in fact very similar to Cooley's conception of personal immunity as the 'right to one's person'.[130]

Generally, Warren and Brandeis' article has been discussed in countless publications on the issue, and is not only seen as the starting point of the story of privacy but probably one of the most cited legal publication in the history of legal privacy

[125] Ibid, 211, 212.

[126] Ibid, 213, 214.

[127] Ibid, 205.

[128] Ibid.

[129] Ibid.

[130] Cooley TM, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Chicago 1880), 29.

research. Hence, it would not serve any purpose for this work to overly engage with the early conceptions of privacy, as this has been done elsewhere.[131] However, it is interesting to realize how much technological and social developments have influenced already early legal works on privacy. Parallels can be drawn between the role of technologies such as photography and print-media at the turn of the 19th century and today's debates on social media, data protection, information law and the necessity for new interpretations of 'old' civil and fundamental rights. In fact, one of the core assumptions of this work is that modern surveillance practices and technologies in public places come with an enormous potential for societal and legal changes. Interestingly, while social and legal changes have always been part of history, modern surveillance technologies have the potential to control and hamper changes and developments. The legal protection of liberty and change might very well lie at the core of the debate. The right to privacy conceptualized as the right to be let alone, however, did not remain the sole conception of privacy.

2.2.2 Privacy and Torts

In 1960, the dean of the University of California Berkley, William Prosser published an article in the California Law Review, in which he further developed Warren and Brandeis' privacy tort. While Warren and Brandeis' right to be let alone was the starting point for the conceptualization of privacy, Prosser was '…the law's chief architect.'[132] Prosser, after reviewing the extensive body of jurisprudence since the Warren/Brandeis 1890 article, described privacy as consisting of four tort categories:

The first category included cases where somebody gathers information, trespasses, hounds, pries, and hence somehow intrudes either in the private affairs or the chosen seclusion or solitude of others.[133] Important to mention in this context is that this does require the existence and delineation of a clear zone or area of seclusion. Prosser stressed that '[o]n the public street, or in any other public space, the plaintiff has no

[131] This is also a debate primarily within a US constitutional context See e.g. Solove DJ and Schwartz PM, *Privacy, Information, and Technology* (3rd edn, Wolters Kluwer Law & Business 2011), 10-23, Mills JL, *Privacy: The Lost Right* (Oxford University Press 2008), 5-6. For alternative perspectives see e.g. Etzioni A, *The Limits of Privacy* (Basic Books 1999), Solove DJ, *Understanding privacy* (Harvard University Press 2008).

[132] Richards NM and Solove DJ, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 California Law Review, 1888.

[133] Prosser WL, 'Privacy.' (1960) 48 California Law Review 383, 389.

right to be alone, and it is no invasion of his privacy to do no more than follow him about.' [134] Further categories of Prosser's four privacy torts were the '[p]ublic disclosure of embarrassing private facts…', '[p]ublicity which places the plaintiff in a false light in the public eye' and the '[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness.'[135]

According to Prosser's first category, being in a public place contradicts actively searching for solitude. Therewith, an individual enjoys less, if even any, privacy when in a public space. At the same time, however, liabilities could also occur in a public scenario. For example, taking a picture of an embracing couple in public isn't as such an invasion into privacy for Prosser, even if that image may be published. However, if the image would be published with a negative connotation and with an intention to slander or insult the couple, the invasion could fall into the third 'false light in the public eye' –category by which a plaintiff would have a case.[136] With his article, Prosser hence clarified and categorized the right to privacy conveniently for many US lawyers at the time. At the same time, Prosser's conceptions have been subject to many debates and criticism and there are indeed several problems with them: One is, for example, that the Prosser's torts appear to be only a swansong for existing remedies against specific pre-existing torts, or, as Bloustein, argues:

> …the right to privacy is reduced to a mere shell of what it has pretended to be. Instead of a relatively new, basic and independent legal right protecting a unique, fundamental and relatively neglected interest, we find a mere application in novel circumstances of traditional legal rights designed to protect well-identified and established social values.[137]

Indeed, looking at the four tort categories 'intrusion', 'disclosure', 'false light in the public eye' and 'appropriation', this criticism makes sense. There are barely any unique or new forms of invasions in those torts, rather an accumulation of categories that are based on existing torts. This essentially disregards Warren's and Brandeis' idea that privacy should rely on the concept of an inviolate personality as an essential

[134] Ibid, 391.

[135] Ibid, 389.

[136] Ibid, 407.

[137] Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962, 965-966.

building block.[138] Bloustein used this argument to state that privacy should in fact be based on '…the individual's independence, dignity and integrity' as the essence of human self-determination.[139] This illustrates the existence of two fundamentally opposed understandings of privacy which will be essential for the analyses of modern public area surveillance in this work: an understanding of privacy based on dignity and an understanding of privacy based on a liberal conception of the individual, on harms and on individual expectations.[140]

Additionally, in Richards' and Solove's reading, Prosser's privacy torts face yet another criticism:

> Like a deer caught in the headlights, the privacy torts froze after Prosser's beam focused upon them. Prosser codified the torts in the *Second Restatement of Torts,* effectively locking them into their current form. The result is that the privacy torts are woefully inadequate to address the privacy problems we face today.[141]

It is crucial to note here that Warren and Brandeis, but especially Prosser, understood and discussed privacy with a strong connection to tort law – which as such is a very limited perspective. In fact, such criticism is deeply rooted in the debates around privacy as a general personality right: it can be regarded as problematic to conceptualize privacy merely as a tort law issue because tort law only activates a mechanism of sanction in case of interferences with a general personality right, but does not contribute to a definition and a legal conceptualization of privacy as a part of personality.[142] In other words, if privacy is reduced to a sanctioning mechanism, it is difficult to argue its essential contribution to forming and sustaining personality. The importance of privacy as a personality right will be discussed further below in this study.

---

[138] Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 194, 205.

[139] Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (n 137), 971.

[140] This will be discussed below.

[141] Richards NM and Solove DJ, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 California Law Review, 1924.

[142] See Schwerdtner P, *Das Persönlichkeitsrecht in der deutschen Zivilrechtsordnung: Offene Probleme einer juristischen Entdeckung* (Schweitzer 1976), 80.

2.2.3 Privacy as Control of Information

While Warren and Brandeis as well as Prosser derived their conceptualizations of privacy at least more or less through tort law, and therewith as civil wrongs occurring to individuals, Alan Westin developed a radically different approach to privacy. In his book from 1967 *Privacy and Freedom*, Westin conceptualized privacy as an intrinsic necessity for human beings, opposing the perception that it was a relatively new legal concept.[143] He defined privacy as '…the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others.'[144]

Consequently, for Westin, privacy related firstly to individual self-determination, and secondly, to control over the sharing of personal information. This perspective constituted a new and major aspect of a legal understanding of privacy with immense relevance for modern information law: privacy could now be grasped as informational self-determination and therewith as people's control of information about themselves.[145]

Westin, however, based his ideas on privacy on an anthropological argument and hence derived privacy from a certain nature of human beings which he categorized into the 'animal world', in the 'primitive world' and in 'modern societies'.[146] While such cultural anthropological simplifications are problematic, Westin's 'states' of individual privacy in Western Democracies are worth mentioning in this context. Westin defined what he calls 'four basic states of individual privacy' as 'solitude, intimacy, anonymity and reserve'.[147] Employing those states, he described the basic relationship between an individual and society, and set out a distinction between the privacy and public sphere.

---

[143] See Westin AF, *Privacy and Freedom* (Bodley Head 1967), 7.

[144] Ibid, 7.

[145] The German Federal Constitutional Court (FCC), for example, developed a similar concept of a right to 'informational self-determination' in its Public Census Judgment, which will be discussed further below due to its importance for a more European understanding of privacy and data protection. See [Germany] FCC, BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil, Census Judgment).

[146] Westin AF, *Privacy and Freedom* (Bodley Head 1967), 8, 11, 21.

[147] Ibid, 31.

In the state of *solitude*, individuals are separated from others and completely free from observation through other persons.[148] In the state of *intimacy*, individuals are placed in small, close and intimate units, such as a circle of friends, a marriage or a family. Such units consist of secluded individuals forming close relationships without which, '…a basic need for human contact would not be met.'[149] On the one hand Westin hence described the individual need for solitude as a fundamental part of human existence, while, on the other hand, he recognized the need for social interactions and community.

In describing the third state of individual privacy, Westin moved more and more towards the individual in the public sphere.

> The third state of privacy, *anonymity*, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance.[150]

While in a public place, one does not necessarily expect to be identified, although, of course, everybody could gather certain information about other individuals. Westin further noted that '[k]nowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.'[151]

Such an argumentation is crucial for emphasizing the importance of privacy in public spaces. In backing up his argument, Westin was certainly right when he referred to the special personal openness of individuals in public and towards strangers, as a result of having to fear less recourse than if that openness was given to closely related persons, a phenomenon described in and deriving from Simmel's excursus on the stranger.[152] In that sense, while humans in public spaces can be observed, they at the same time enjoy a clear sense that their behaviour and expressions do not have the same consequences as if they would be conducted among a group of people of close relationship. Strangers, indeed, as Westin put it, were '…able to exert no authority or

[148] Ibid.

[149] Ibid.

[150] Ibid, (emphasis added).

[151] Ibid.

[152] Ibid. 31, 32; Georg Simmel, *Soziologie* (Duncker & Humblot, Berlin 1908), esp. Kapitel IX: Der Raum und die räumlichen Ordnungen der Gesellschaft, Exkurs über den Fremden, 509-512.

restraint over the individual.'[153] This is certainly an important contribution to a different understanding of privacy and will be followed up later in the discussion on privacy in public space.

The fourth state of privacy as defined by Westin is called 'reserve'. With this, he described a certain '…psychological barrier against unwanted intrusion;' which occurs '…when the individual's need to limit communication about himself is protected by the willing discretion of those surrounding him.'[154] This means that information shared between individuals in close relationships generally are not carelessly made public or spread in order to safeguard an individual's personality. This self-restraint '…expresses the individual's choice to withhold or disclose information – the choice that is the dynamic aspect of privacy in daily interpersonal relations.'[155] Once again, Westin drew the idea from Simmel and his identification of constant tension between self-exposure and self-constraint.[156]

Westin additionally took a rather functionalist approach to privacy as a concept in society: for him, the distinction between different privacy states and the distinction between the functions of individuals in society serve as tools to further develop law in a modern democratic state.[157]

In addition, another important contribution of Westin's work were the analyses of new technologies and their effect on individual privacy through surveillance. He thoroughly examined, for example, location tracking, listening devices, physical surveillance and psychological surveillance through public and private actors.[158] Already in 1967, Westin excessively speculated about the future capabilities of privacy invasive technologies; and his predictions concerning small vibration or acceleration sensors carried on the body, miniature microphones or miniaturization of cameras come surprisingly close to the modern mobile phone.[159] He noted that while

[153] Westin AF, *Privacy and Freedom* (Bodley Head 1967), 32.

[154] Ibid.

[155] Ibid, 32.

[156] Ibid.

[157] Ibid, 32, 33.

[158] Ibid, 69-168.

[159] Ibid, 86.

most of the mechanism of surveillance, control and manipulation go a long back in history, '…[w]hat is new today is the marriage of advanced scientific technology to these classic surveillance methods.'[160] It appears that this certainly still applies today, probably even more than ever before.

While engaging with Westin's work, it does not come as a surprise that he has been hugely influential in creating a distinct categorization of privacy, which does not primarily derive from private law and tort law, but from the social sciences, anthropology and sociology. Subsequently, one of the many conceptualizations of privacy today revolves around Westin's idea of privacy as control over personal information. Many other scholars have since then analysed or developed the idea of privacy as control over personal information,[161] and the idea built the foundation of many current understanding of privacy and data protection rights, from the German 'right to informational self-determination' to the right to request access to one's data held by others in the new European General Data Protection Regulation (GDPR).[162] Furthermore, Westin's concept of information control by individuals has played a very important role in the development of privacy management in information law, e.g., in the concept of implied and explicit consent as well as 'notice and choice' for consumer data processing.[163] With this, Westin's privacy as control of personal information strongly depends on an individual's will and choice to share information or not. Hoofnagle and Urban have therefore rightly described Westin's conceptions as deeply dependent on the sovereignty of individuals and their choices, hence as 'privacy homo economicus'.[164] Westin's assumptions are problematic, firstly because it appears that his conception of individual rational choice does not hold up to thorough testing[165] -

[160] Ibid, 68.

[161] See e.g. Solove DJ, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1109, 1110 fn 112; For detailed analyses of Westin's contribution, see Margulis ST, 'On the Status and Contribution of Westin's and Altman's Theories of Privacy' (2003) 59 Journal of Social Issues 411; Fried C, 'Privacy' (1968) 77 Yale Law Journal 475, 482.

[162] For a further discussion on the right to informational self-determination see Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S and others, (eds), *Reinventing Data Protection?* (Springer 2009), 45-76. See Regulation (EU) 2016/679, (GDPR), (n 303), Art 15.

[163] See Hoofnagle CJ and Urban JM, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest Law Review 261, 261, 262.

[164] Ibid, 268-270.

[165] Ibid, 270.

understandable when one thinks of how careless consumers often accept e.g. the privacy policies of a mobile phone application – and secondly, because conceptualizing privacy on the bases of individual choice is too reductive. Solove, for example, rightly remarks that privacy '…is not simply a matter of individual prerogative; it is also an issue of what society deems appropriate to protect.'[166] Westin's privacy conception appears to be centred on individuals rather than communities, and privacy might often need to be contextualized differently, especially when the individual choice theory, for one or the other reason, does not keep its promises.

Problems with conceptualizing privacy as control over information arise especially when the definition of personal information as such is problematic: What actually falls into the realm of personal information and what does it actually mean to 'control' such information?[167] When privacy is understood as control over personal information and dependent on an alleged rational choice, information easily becomes proprietary. The connection between privacy and property, however, is deeply problematic. Solove puts this nicely:

> [W]hen theorists attempt to define what "control" entails, they often define it as a form of ownership, making the conception falter in a number of respects. Finally, conceptions of information control are too narrow because they reduce privacy to informational concerns, omit decisional freedom from the realm of privacy, and focus too exclusively on individual choice.'[168]

This critique is especially directed towards understanding privacy under the auspices of a liberal common law society, such as in the US, where most of the legal privacy debates unfold around interferences with privileges held by intellectual and financial elites. The connection between early conceptions of privacy with high social status, possessions and property in a liberal capitalist society becomes certainly visible in Warren's and Brandeis' right to be let alone by the press and the State. Also, Prosser's four torts of intrusion into chosen solitude, libel and slander and disclosure or

[166] Solove DJ, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087, 1111; For a further discussion on privacy, information, and property, see Alén-Savikko A and Pitkänen O, 'Rights and Entitlements in Information: Proprietary Perspectives and Beyond' in Bräutigam T and Miettinen S (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia 2016), 3-33.

[167] Solove DJ, 'Conceptualizing Privacy', ibid, 1115.

[168] Ibid.

appropriation of information on individuals, carry a strong scent of a liberal individualist understanding of privacy, and Westin has repeatedly, as discussed above, been criticized for his liberal conception of a 'privacy homo economicus'.[169]

So far conceptions of privacy discussed here included the right to be let alone, privacy as a legal tort and privacy as control over personal data, but there are, of course, further nuanced understandings in legal and theoretical writings worth discussing in this context.

2.2.4 Privacy as Limited Access to the Self

Daniel Solove has repeatedly analysed another category of privacy theories, namely privacy as 'limited access to the self'.[170] Ruth Gavison, in this context, argued that privacy boils down to the accessibility of individuals by other individuals or entities. In her understanding, 'accessibility' means '…the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.'[171] '…[I]n perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X. Perfect privacy is, of course, impossible in any society.[172] Similarly, Gross argued that '…privacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited'[173] and Solove summarized limited access theories as '…the individual's desire for concealment and for being apart from others.'[174] He furthermore interpreted those views as a further sophistication of the right to be let alone, and in that sense as a right reaching beyond mere solitude:

> Solitude is a component of limited-access conceptions, as well as the right-to-be-let-alone conceptions, but these theories extend far more broadly than

[169] Hoofnagle CJ and Urban JM, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest Law Review 261, 268-270.

[170] See Solove DJ, 'Conceptualizing Privacy' (2002) 90 Cal L Rev 1087, 1102, Solove DJ, *Understanding Privacy* (Harvard University Press 2008),18, Solove DJ and Schwartz PM, *Privacy, Information, and Technology* (3rd edn, Wolters Kluwer Law & Business 2011), 46.

[171] Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421, 423.

[172] Ibid, 428.

[173] Gross H, 'The Concept of Privacy' (1967) 42 New York University Law Review 34, 35, 36.

[174] Solove DJ, *Understanding Privacy* (Harvard University Press 2008), 18.

> solitude, embracing freedom from government interference, as well as from intrusions by the press and others.[175]

Indeed, Gavison's understanding of accessibility goes beyond individual solitude or to be left alone: for her, privacy comes with an inherent value:

> …the reasons for which we claim privacy in different situations are similar. They are related to the functions privacy has in our lives: the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society.[176]

Privacy, in this understanding, becomes '…a complex of three independent and irreducible elements: secrecy, anonymity, and solitude' as a short form of '…the extent to which an individual is known, the extent to which an individual is the subject of attention, and the extent to which others have physical access to an individual.'[177] Gavison criticized the idea of privacy as control over information on the basis of the difficult notion of 'control'. On the one hand, control is a difficult concept, because '…a voluntary, knowing disclosure does not involve loss of privacy because it is an exercise of control, not a loss of it.'[178] Yet, on the other hand, '…voluntary disclosure is a loss of control because the person who discloses loses the power to prevent others from further disseminating the information.'[179]

Gavison is right in her analyses. 'Control' indeed contains an element of choice and hence runs the danger of a reductionist and choice-centric perception of privacy. Choice is in fact a very weak element of privacy protection, when understanding privacy as access to one's self: there are countless ways available that one can think of scenarios where information is voluntarily disclosed, but then still used in order to gain access to the person. Furthermore, the element of individual choice, inherent in the Westin's conception of privacy as control over information, would require rational and informed individual decision making capabilities which leads back to Hoofnagle and Urban's critique of a 'privacy homo economicus'.[180] Making those choices would

---

[175] Ibid, 19.

[176] Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421, 423.

[177] Ibid, 433,434 and 433 fn 40.

[178] Ibid, 427.

[179] Ibid.

[180] Hoofnagle CJ and Urban JM, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest Law Review 261, 268-270.

require a level of individual rationality, technical skills, knowledge and wisdom that not many people in today's networked world have the means to acquire.

Gavison further rightly pointed out that privacy choices as such cannot be evaluated if a conception of privacy solely depends on individual choice.[181] An individual might for example be criticized for uploading exercise and health data to a server through a fitness or health application on a phone on the basis of not choosing the 'right' kind of privacy behaviour. Through this, privacy becomes a value that reaches beyond individual choice. And this value does not depend on individual choice. Consequently, privacy conceptualized as limited access to the self carries an overarching value of privacy while it is able to point out concrete losses of privacy for individuals. Solove, however, criticised Gavison's conception as it seems to exclude what is often called 'informational privacy', meaning the importance of privacy in connection to the collection, retention and processing of data in computerized databases.[182]

Defining privacy as control over information and conceptualizing privacy access to the self does, however, not seem to be as far separated as some suggest. While the element of choice in the control-conceptualization can be criticized as an illusionary liberal concept, so can the idea of inaccessibility. In fact, defining privacy as something that an individual controls, possesses and even might lose, is one of the core elements of liberal rights theories.[183] Allen stated that liberal conceptions relied on three basic 'privacies', namely 'physical privacy' – containing chosen solitude and seclusion, 'informational privacy' – concerning control, access, processing and retention of personal information, and 'proprietary privacy' – as the 'control over names, likenesses, and repositories of personal identity'.[184]

Each of those distinct 'privacies' therefore has rather individualistic underpinnings and at its centre is the individual with her desires for seclusion and capacities to make

[181] Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421, 428.

[182] See Solove DJ, *Understanding Privacy* (Harvard University Press 2008), 21.

[183] Allen AL, 'Coercing Privacy' (1999) 40 William & Mary Law Review 723, 724

[184] Ibid, 723,724, for 'proprietary privacy', see also Allen AL, 'Genetic Privacy: Emerging Concepts and Values' in Rothstein MA (ed), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (Yale University Press 1997), 31-59.

rational decisions. 'Access to the self' can therefore be seen as an understanding of privacy which is based on choice on the one hand, and control on the other.

Returning to Gavison's definition of privacy as access to the self (as '…the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention'),[185] it should be noted that it contains an element beyond individual control and choice: after all, being known, physically accessed and being subject to others attention generally is determined and regulated not only by the individual, but also and maybe even foremost by the community or the society.[186] And in that sense regulating access to oneself is at least on a similar scale a matter of societal and communal regulation and therewith an essential part of the substance of societal organization.

2.2.5 Intimacy and Secrecy

A fifth approach or conceptualization of privacy discussed in this context evolves around the notions of secrecy or intimacy.[187] At first sight, 'secrecy' appears as a self-evident concept: it assumes that individuals want to keep some things secret, including personal information or some kinds of knowledge about themselves. The concept of intimacy consequently is based on the assumption that privacy related issues derive from the need and feelings for personal intimacy.

Richard Posner, a strong critic of many other understandings of privacy, contended that privacy would *de facto* be mostly about keeping secret and withholding information about oneself in order to avoid disadvantages in capitalist economies. Posner expressed this in as following:

> Much of the demand for privacy, however, concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards. And often the motive for concealment is, as suggested earlier, to mislead those with whom he transacts.[188]

---

[185] Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421, 423.

[186] This has been discussed by Etzioni and his communitarian conception of privacy. He discusses privacy as a 'societal license' which exempts groups or person from societal and communal scrutiny. See Etzioni A, *The Limits of Privacy* (Basic Books 1999), 186, 197.

[187] See Solove DJ, *Understanding Privacy* (Harvard University Press 2008), 21, 34.

[188] Posner RA, 'The Right of Privacy' (1987) 12 Georgia Law Review 393, 399.

With this, privacy is turned into a mere tool for rational individuals operating in a liberal competitive market society in which people, according to Posner, '…want to manipulate the world around them by selective disclosure of facts about themselves.'[189] In that sense, Posner's basic understanding of privacy is embedded into his theory of law and economics and appears to be rather reductionist compared to other privacy conceptions. In his 'The Economics of Justice', Posner recognized three distinct meanings of privacy: namely, privacy as secrecy, as seclusion and as autonomy, however, he strongly emphasized privacy as secrecy.[190] While Posner understood the claim for personal privacy as a tool to conceal things in order to defy others about certain facts related to a person, he recognized the importance of personal information in social economic relationships. Gathering information about another person '…enables one to form a more accurate picture of a friend or colleague, and the knowledge gained is useful in social or professional dealings with him.'[191] Furthermore, the disclosure of seemingly private information about individuals beyond one's own social realm serves, according to Posner, as a model for success or a deterrent for failure for careers and personal life choices. The rise of gossip and rumour and its media distribution which lead to Warren and Brandeis developing a right to be let alone, was, in Posner's view, not a result of the press turned rogue, but a result of market demands:

> Gossip columns provide valuable information …[on] the personal lives of wealthy and successful people whose tastes and habits offer models to the ordinary person in making consumption, career and other decisions.[192]

In fact, according to Posner, the lives of the poor were simply not that interesting and therefore there would be less demand for privacy in most poor societies.[193] Hence, the reason for the rise of privacy as a legal concept had more to do with the increase of personal income than with the increasing invasion into a sphere in need of better protection.[194]

---

[189] Ibid, 400.

[190] Posner RA, *The Economics of Justice* (Harvard University Press 1981), 231.

[191] Ibid, 232.

[192] Ibid, 238.

[193] Ibid, 238, 239.

[194] Ibid, 239.

With this Posner presented a strong and slightly polemic criticism of privacy as a right and concept. A focus purely on controlling information about oneself is, however, reducing the complexity of privacy to a large extend. Furthermore, Posner's critique is fundamentally based on assumptions and ideologies of economics and liberal market societies which are exclusively concerned with the regulation of human life through market forces and rational economic actors. Privacy as a concept and as a right has served more complex functions than regulating the dissemination of market-valuable information about individuals. What is somewhat remarkable is that while Posner seems to regard privacy as a regulatory tool hampering market societies, others have discussed understandings of privacy as property: especially a perspective on privacy as intellectual property can result in interesting discussions about the concept. [195] Nevertheless, Posner offers a strong critique of common conceptualizations of privacy.

On a more meta-critical level, it could also be argued that all attempts at synthesizing varieties of privacy concepts fail due to their legal and theoretical complexity. Indeed, the conceptualizations remain fragmented and often specialized. As a result, Daniel Solove attempted to develop an alternative approach to privacy after criticizing a variety of this pre-existing understandings.[196] With this, he developed a conclusive privacy-taxonomy in order to enable legal professionals and policy makers to understand and process privacy in a better way. [197] This taxonomy basically categorized privacy issues into four different groups: Firstly, 'information collection', secondly, 'information processing', thirdly, 'information dissemination' and fourthly, 'invasion'.[198]

Solove criticised the fact that most of the existing privacy conceptions follow a very traditional model of methodology: They undergo attempts to define privacy through

[195] For a discussion on the relationship of privacy as a right and the proprietary character of privacy see e.g. Mayer-Schönberger V, 'Beyond Privacy – Towards a "System" Theory of Information Governance.' (2010) California Law Review 1953; see also Alén-Savikko A and Pitkänen O, 'Rights and Entitlements in Information: Proprietary Perspectives and Beyond' (n 166).

[196] See Solove DJ, *Understanding privacy* (Harvard University Press 2008), 9.

[197] Ibid, 10.

[198] Ibid, 10, 11.

distinguishing it from other concepts.[199] Solove argued that many theorists were attempting to define a specific core or essence of privacy as something that delimits privacy from other concepts, but that those concepts would come with serious shortcomings.

> Ultimately, the problem emerges from the fact that theorists are attempting to conceptualize privacy with the traditional method. They are seeking to isolate its core characteristics. Privacy, however, does not lend itself very well to this form of conceptualization.[200]

Furthermore, Solove stressed that the core problems of the theoretical debates in privacy are related to the employed method of research: the search for a clearly defined and delineated scope of privacy. He contended that

> …the problem with current theories of privacy is the method of conceptualizing. The theories fail on their own terms - they never achieve the goal of finding the common denominator, and thus commentators remain unsatisfied. But perhaps the quest for a common denominator is a search for the holy grail. What if there is no essence or core dimension of privacy? Can privacy be conceptualized?[201]

Indeed, one of the problems deriving from the attempt to define privacy through the search for a clear core lies deep inside a theoretical debate on the indeterminacy of law and especially of rights as such. Solove criticised the fact that attempts to define privacy using what he calls a 'traditional method' of identifying a clear common definition of privacy are bound to fail because those definitions will either not include enough important privacy aspects, or include too many.[202] If privacy were to be defined too narrowly, many legal issues of everyday life would simply not be addressable through legal frameworks and privacy might not be able to serve well as a mechanism of protection. If, on the other hand, privacy was to be defined too broadly, it would run the dangers of rendering itself legally meaningless.

Those aspects, however, are not surprising and they are not unique to privacy. Excessive debates on rights indeterminacy have attempted to point out the dual nature of law and particularly rights.[203] Koskenniemi, for example, argued that rules -and

---

[199] Ibid, 14.

[200] Ibid.

[201] Ibid, 38.

[202] Ibid, 40.

[203] See Koskenniemi M, *From Apology to Utopia: The Structure of International Legal Argument* (Reissue with a new epilogue, Cambridge University Press 2005), 590-596.

particularly rules that come with a claimed universalism component- are always over-inclusive and under-inclusive at the same time.[204]

> The rules will include future cases we would not like to include and exclude cases that we would have wanted to include had we known of them when the rules were drafted. This fundamentally – and not just marginally – undermines their force.[205]

Koskenniemi therefore argued that indeterminacy was not only a problem of the semantic un-clarity of the legal language, but a fundamental problem due to the inherent political nature of international law and human rights and that therefore questions – also related to making decisions about privacy – could not be solved through abstract legal reasoning.[206]

While this work does not want to deeply engage in such theoretical debates on international law and human rights, it should be pointed out that Solove's critique stems therefore from a broader and deeper criticism on the nature of international law. Nevertheless, while it is indeed questionable if there can be one right and functional conceptualization of privacy, is should not be forgotten that privacy as a concept did not emerge as an attempt to ultimately regulate future legal problems, but as a legal argument *responding* to existing problems. In many ways, a right to privacy is a right with an inherent emancipatory function: it addresses severe political and societal problems or 'wrongs' as a tool of critique. Warren's and Brandeis' right to be let alone was in many ways a legal emancipatory move against certain intrusions in a similar way as the development of a right to control information can be understood as a legal response to problems emerging from the massive automated collection of personal information by states and the private sector. As a consequence, while it is important to understand the fallacies as well as the alternatives of different privacy conceptions, this study approaches privacy as a critical legal argument that functions within existing regulatory systems. Privacy and its definition as a right therefore play a very important role for approaching surveillance in public places, also because it is particularly the application of privacy in public places that may be able to break the rather limited understandings of an individualistic and proprietary focus of a legal right to privacy.

[204] Ibid, 591.

[205] Ibid, 592.

[206] Ibid, 595.

The following section therefore now turns towards the analysis of privacy as a personality right and its connection with the public-private dichotomies.

2.2.6 Privacy, Dignity, and the Right to Personality

As discussed above, privacy has been conceptualized in various forms, for example as tort, as control over information, as access to persons, or along the lines of intimacy and secrecy. Privacy, however, can also be understood in terms of individual rights, including autonomy, self-determination, and dignity, especially in in a European context.[207] It is therefore interesting to identify a further reading (or conceptualization) of privacy, namely as a personality right primarily relying on self-determination and human dignity.

Post, as a starting point, distinguished three concepts of privacy in a review essay on Rosen's *The Unwanted Gaze* by separating privacy as protecting reputation, privacy as dignity and privacy as freedom. Particularly the last two conceptions were taken up later by Whitman to separate what he calls 'two western cultures of privacy'. In Post's understanding, a privacy conception based on freedom is founded on the cores of individuality, imagining '…persons as autonomous and self-defining, rather than as socially embedded and tied together through common socialization into shared norms.'[208] In that sense, a privacy conception based on freedom is based on the very core of a classical liberal understanding of autonomous individuals. Therefore, it depends strongly on a very specific organizational model of society in which selfish autonomous individuals attempt to maximize their gains. For some, Warren and Brandeis' construction of a right to privacy as a right to be let alone exemplifies the idea of liberal privacy, '[representing] a wealthy, smug, exclusive, and self-centered upper-crust life which abhors publicity and public space.'[209]

In that sense, privacy could be understood as a concept based on individual freedoms opposing community and social relations. In many ways, the 'private' is a sphere in which the autonomous individual exists in a completely self-referential state, in a state

[207] Mayer-Schönberger V, 'Beyond Privacy – Towards a "System" Theory of Information Governance.' (2010) California Law Review 1953, 1857.

[208] Post RC, 'Three Concepts of Privacy' (2000-2001) 89 Georgetown Law Journal 2087, 2095; Rosen J, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House 2000).

[209] Gutwirth S, *Privacy and the Information Age* (Rowman & Littlefield Publishers 2002), 51.

of complete absence of community, communication and other individuals. What could be understood as 'public' would then be a sphere in which this isolated individual starts communicating and interacting with other individuals. A right to be let alone in private therefore embodies absolute freedom as no restraints whatsoever would be exercised on such autonomous individuals.

Post, then placed privacy as freedom as opposing a concept based on dignity:

> From a theoretical point of view, (…) privacy as freedom is an almost exact inversion of the concept of privacy as dignity. Privacy as freedom presupposes difference, rather than mutuality. It contemplates a space in which social norms are suspended, rather than enforced. It imagines persons as autonomous and self-defining, rather than as socially embedded and tied together through common socialization into shared norms.[210]

In many ways, privacy conceptualized as individual and liberal freedom can function as a defence mechanism against interferences of any kind against that personal freedom. The freedom to act is equalled with the freedom to act against others and to act against the community, for example the freedom to enjoy one's property, the freedom to not pay any taxes or the freedom to beat one's own children in one's own house.

Basing a conception of privacy on dignity, on the other hand, means something different. Post connected the concept of dignity with the communality and social interaction. In fact, privacy derived from dignity

> …presupposes a particular kind of social structure in which persons are joined by common norms that govern the forms of their social interactions. These norms constitute the decencies of civilization.[211]

Furthermore,

> [p]rivacy as dignity locates privacy in precisely the aspects of social life that are shared and mutual. Invading privacy causes injury because we are socialized to experience common norms as essential prerequisites of our own identity and self-respect.[212]

Apart from presenting privacy as a rather high valued normative concept, Post therewith conceptualized privacy not as an individualistic defence mechanism against

[210] Post RC, 'Three Concepts of Privacy' (n 208), 2095.

[211] Ibid, 2093.

[212] Ibid, 2094.

intrusion, interference or wrongs, but as an essential component of the self, one's own identity and personality. In many ways, such a conception can be compared to Julie Cohen's understanding of privacy as an important factor for the development of a society build by autonomous and self-determinant individuals.[213]

For Cohen, privacy presents itself as a fundamental element of autonomous individuals and civil societies: Western political philosophy and the strong emphasis of, and commitment to, human dignity requires a restrictive approach, for example banning

> …data processing practices that treat individuals as mere conglomeration of transactional data, or that rank people as prospective customers, tenant, neighbors, employees, or insured based on their financial or genetic desirability.[214]

Privacy therewith becomes an intrinsic value in societies, a prerequisite for communication, choice and freedom, the creation of identity, and the autonomy of individuals as a core of communities. Similarly, Floridi remarked that '[a]ny society in which no informational privacy is possible is one in which no personal identity can be maintained (…)'.[215]

The necessity of privacy for the autonomy of individuals leads to another argument: In fact, when privacy is an essential element of a community because it guarantees individual autonomy, it also becomes important for democracy as a whole.

Paul Schwartz argued that privacy was important for individual self-determination and the creation of identity and therewith a requirement for deliberative democracy.[216]

> The need is to insulate an individual's reflective facilities from certain forms of manipulation and coercion. Privacy rules for cyberspace must set aside areas of limited access to personal data in order to allow individuals, alone and in association with others, to deliberate about how to live their lives.[217]

---

[213] See Cohen JE, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373, 1423, 1424.

[214] Ibid, 1424.

[215] Floridi L, 'Four challenges for a theory of informational privacy' (2006) 8 Ethics and Information Technology 109, 111.

[216] See Schwartz PM, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607, 1653.

[217] Ibid, 1653.

The underlying assumption here is that privacy is more than just the control of information or an element of choice: it is essential for self-development and therewith essential in democratic communities. With this, privacy is more than just an individual value: it becomes a communal and social good that lies at the essence of a particular democratic form of society.

Cohen's and Schwartz's ideas on privacy as an essential part of autonomous individuals in democratic societies goes very much in line with a dignity-based approach on privacy deriving from a right to personality. Luciano Floridi similarly argued, that

> [l]ooking at the nature of a person as being constituted by that person's information allows one to understand the right to informational privacy as a right to personal immunity from unknown, undesired or unintentional changes in one's own identity as an informational entity, both actively and passively.[218]

In that sense, privacy is a right protecting important, if not essential societal values such as human dignity and the creation and maintenance of human identity and personality and therewith it brings essential building blocks of Western democratic societies.[219]

One of the first and highly influential legal arguments of privacy as a personality right in case law can be found in the jurisprudence of the German Federal Constitutional Court (FCC).[220] The arguments put forward by the FCC shall here serve as an example of the conceptualisation of privacy as a derivate of dignity and personality and therewith as the construction of privacy as an essential element in the political and legal design of societal communities.

Already early on, in 1969 the FCC employed concepts of free individuals and emphasized the importance of a constitutional protection of self-determination as a right. The collection of information about individuals therewith fell into the scope of protection given by human dignity. In fact, individuals' self-determination capabilities were seen as being seriously hampered merely by potential psychological pressure

[218] Floridi L, 'Four challenges for a theory of informational privacy' (n 218), 111.

[219] For a more detailed discussion on the philosophy of informational privacy, particularly with reference to privacy and identity see Richardson J, *Law and the philosophy of privacy* (Routledge 2016), esp. 137-160.

[220] See Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' (n 162), 45,46.

created through public authorities systematically collecting personal information.[221] Natural persons, so the argument went, were free to develop their personality and therewith would have a principal right to self-determination of which privacy formed an essential element. Then, in 1983, as a response to public census and governmental data collection, the FCC developed a 'right to informational self-determination' by combining the right to freely develop one's own personality (art 2(1)), and the general inviolability of human dignity in article 1(1) of the German Basic Law.[222] According to the FCC, the general personality right in the Constitution explicitly protected the dignity of persons as free members of a free society.[223] In this regard, every individual had the ability and competence to decide for herself in what way personal information was distributed and shared, but new technological means of data processing would threatened the ability to control such information, and the FCC emphasised especially the potential constraining or coercing effects of information collection, including a 'chilling-effect' for the exercise of fundamental rights.[224]

Privacy as a personality right based on inherent dignity therewith opposes an understanding of privacy as freedom. Post, and later Whitman, analysed those fundamentally different distinctions as '…privacy as and aspect of dignity and privacy as an aspect of liberty.'[225] While privacy in the latter concept works as a liberal defence mechanisms against intrusion into individual lives, it can also function as an overall critique of control in social structures. Privacy as dignity functions as an element of critique against social coercion and control and as such is a necessity for the ideal of a democratic society. The argument of the FCC essential combines a liberal conception of privacy as freedom of control with the construction of privacy as an inherent building block of community and communal interaction.

---

[221] See [Germany] FCC, BVerfG, Urteil vom 16 Juli 1969, BVerfGE 27,1, 1 BvL 19/63, (Mikrozensus), para 34.

[222] See [Germany] FCC, BVerfG, 'Volkszählungsurteil', (n 145).

[223] Ibid, II (1) A), paras 170.

[224] Ibid., paras 170-172. For a further discussion of this argument in light of public surveillance see Section 3.2.4.2.

[225] Whitman JQ, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2003-2004) 13 Yale Law Journal 1151, 1161.

Privacy as an aspect of democratic societies gained even more importance when vast scale of data processing was considered. With this, privacy theory experienced a shift from an individual problem to a collective problem as a result of modern technological data collection capabilities. Spiros Simitis argued already in 1987 that surveillance had '…lost its exceptional character…' and would manifestly impact individual behaviour: 'Information processing is developing (…) into an essential element of long-term strategies of manipulation intended to mold and adjust individual conduct.' [226] As a consequence, such information processing should be strictly regulated as participation and communication in democratic societies would depend on high levels of privacy protection.[227]

Privacy as dignity and the right to personality therefore is essentially conceptualized from two perspectives. Firstly, privacy can be derived from human dignity because massive data and information collection means treating individuals as mere objects and mere means towards an end. Such collection, retention, and dissemination of information comes with high risks of manipulation, coercion and self-alterations. The exercise of this powerful but tacit control therefore requires strict legal limitations.

Secondly, basing privacy on dignity is important because the mere volume, technological sophistication and capabilities as such come with a high risk of control which hampers democracy as the preferred model of societal organization. If democracy and therewith the ideal of autonomous and self-determinant individuals lies at the core of a society, privacy based on dignity is not only an essential right, but also a core value of a society. While societies are naturally not free from control, privacy is the language which articulates and addresses control, coercion and manipulation as a legal remedy.

This leads to the other important issue related to public space surveillance, namely the application of the legal conceptions of privacy to public space surveillance. As discussed above, there is not one single conception of privacy, but it can be conceptualized in many distinct ways. The question deriving from the discussion therefore concern the application of privacy to surveillance of public places.

[226] Simitis S, 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review 707, 710.

[227] Ibid, 746.

Intuitively, of course, it appears odd that the concept of the protection of individuals' private issues would apply to public places. The discussions above, however, showed that especially the strong connections between individual, communal or societal conceptions, and the conceptualisation of privacy as an inherent element in human dignity and personality, can form a connection between privacy and public spaces. This, of course, additionally requires reference to the classical dichotomy between the public and the private. Can privacy function as a legal argument in public places, and if so, under what conditions? Is a right to privacy therefore suitable for addressing the complexities of modern public surveillance technologies? The following section will now turn to the problem of privacy in public and its possible theoretical approaches and legal arguments.

2.2.7 Privacy in Public

Privacy can be conceptualized in a variety of ways and the concept appears to defy a universal definition. The Section above discussed several approaches to privacy, from privacy as a tort to privacy as deriving from the right to personality and dignity and therewith as right that protects central values of societies.

This section consequently turns to the core issue of this study: the conceptions of privacy in relation to public spaces. Most importantly, this section lays the grounds for a right to privacy in public spaces based on a dichotomy of privacy conceptions: privacy as individual freedom on the one hand and privacy as a derivate of dignity, on the other. When it is understood in terms of individual freedom, privacy can be conceptualized as a tool to address harm and demand freedom from it, e.g. as a right to be let alone or as a tort leading to liabilities for others. When privacy on the contrary is seen as a derivate of dignity, it becomes an essential element of societal organization and community. Privacy then functions not only as articulating demands for individual freedoms, but it addresses interferences with the mere foundations of communal and societal organization, the balances of power, and the exercise of violence.

This distinction can also be formulated through the identifications of harms. Daniel Solove described the nature of privacy problems through the concept of harms and

therefore distinguished between individual and societal harms.[228] Individual harms are injuries or damages that occur to an individual person and include 'physical injury', 'financial losses and property harms', 'reputational harms' and 'emotional and psychological harms'.[229] All such harms can be understood as harms to the individual and her abstract liberty.

Beyond this, however, Solove also articulated other harms that can be said to have a more societal or communal nature. 'Relationship harms', for example, are damages done to the relationships between people.[230] A lack of privacy protection can undermine trust in communications between people and interferes with the establishment and maintenance of trusted relationships between individuals and groups. 'Vulnerability harms', are described by Solove as the creation of risk and insecurity through a steady 'pollution' with privacy problems occurring '…through the combined activities of a multitude of institutions, each with differing motives and aims.'[231] In fact, this describes the creation of collective insecurities of a systematic nature.

Additionally, Solove described two harms which are fundamental to the discussion of privacy in public space: the interference and tampering with people's behaviours, the so called 'chilling effect' and 'power imbalances' deriving from privacy problems that affect societal and communal structures.[232] This line of argument follows a distinction between harms to the liberty of individuals and harms to communal and societal structures.

In a similar way, this section distinguishes between privacy as focused on individual freedom and privacy as a derivate of dignity forming the base of societal and communal structures, without resorting to the harm-principle. That is because fundamental rights and principles as underlying foundations for societal and legal systems go beyond the understanding of protecting individual and communities from harm: they actual establish positive foundational principles and values which lay the

[228] See Solove DJ, *Understanding Privacy* (Harvard University Press 2008), 174.

[229] Ibid, 174-175.

[230] Ibid, 176.

[231] Ibid, 177.

[232] Ibid, 177, 178.

foundation for the social systems as such. Privacy as a derivate of dignity is therefore not based on preventing harm to individuals, communities or societies, but as the mere pillar on which the functioning of a respective system relies on. An entire lack of dignity would, in a similar way as an entire lack of privacy, therefore change the very nature and structure of a society.

In the context of rights to privacy in public spaces, the distinction between individual liberty and dignity is important because it leads to two fundamentally different perceptions of a concept of privacy in public.

On the one hand, privacy in public is determined by individual liberties. This paradoxically means that individuals in public spaces are less 'free' than individuals in private spaces. That is because, if the harm principle -based argument is accepted, individuals in public, for some reason, can harm other individuals in public easier than in private simply because there is *per se* more interaction between individuals in public spaces. Individuals therefore enjoy a lesser degree of privacy than in private secluded spaces.

On the other hand, privacy in public can also be conceptualized as a dignity-based approach. If so, the public space as such forms the ultimate area of societal interaction and therewith the core of communal and societal existence. People in public spaces therefore can be subjected to insecurities, altered behaviour, self-censorship, the chilling effect, and control as the exercise of power. All those therefore touch upon the very core of the current structure and organization of social systems, namely the balance of power, rule of law and democratic governance through which privacy protection becomes an essential element in public as well as in private spaces.

Those perspectives have substantial effects on legal jurisprudence and case law on privacy in public spaces. This distinction between privacy as deriving from individual freedoms and privacy as a derivate of dignity gains additional relevance when analysing privacy problems in connection with advanced and sophisticated public surveillance systems and their legal regulations.

***

Privacy as a concept lies naturally at the crossroads between public and private space. Public and private spaces, however, are not that easy to delineate, as the discussion in

the section above showed. The final theoretical question to be discussed in this chapter is therefore a theoretical synthesis between the conceptions of privacy and the European public space. In how far do conceptions of privacy along the line of the dichotomies between privacy as freedom and privacy as a derivate of dignity and personality extend into public spaces?

A preliminary answer to this question is already evident from the discussions above and strictly depends on the theoretical conceptualizations. In that sense, privacy deriving from individual liberty is less likely to extend its protection into the public sphere than dignity based approaches. Basing privacy considerations on an individual's legitimate expectation is after all very different from understanding privacy as a tool to address chilling-effects and the exercise of control.

The distinction between a public realm and the private realm is naturally subject to broad theoretical debates.[233] In many ways, the theoretical underpinnings of the public and private dichotomy reflect the ancient question about the relationship between the individual and society and can be seen as '…a central tenet of liberalism.'[234] Particularly in liberal thought, the private sphere often describes a zone in which the community (or the state) as a bearer of power has limited influence.[235]

The abstract private and public distinction therefore plays an essential role specifically for the conceptualization of privacy, but reaches broader into discussions on social organization and the essential structure of law and even societies. In fact, the private/public distinction lies not only at the core of the philosophical thought of 19th century liberal market societies, but is at the same time foundational to law *per se*:

> Although, as we have seen, there were earlier anticipations of a distinction between public law and private law, only the nineteenth century produced a fundamental conceptual and architectural division in the way we understand the law.[236]

[233] See e.g. Horwitz MJ, 'The History of the Public/Private Distinction' (1982) 130 University of Pennsylvania Law Review 1423.

[234] Wacks R, *Personal Information: Privacy and the Law* (Clarendon Press 1989), 9.

[235] See Mnookin RH, 'Public/Private Dichotomy: Political Disagreement and Academic Repudiation' (1982) 130 University of Pennsylvania law review 1429, 1429.

[236] Horwitz MJ, 'The History of the Public/Private Distinction' (1982) 130 University of Pennsylvania Law Review 1423, 1424.

With this came the need for a clear distinction between public law as a foundational, regulatory or sanctioning mechanism and private law as the 'law of private transactions' necessary for the functioning of a market society.[237]

While this understanding appears to make sense, on closer examination the public/private distinction comes with a variety of serious problems. In fact, many argue that the public/private distinction is nothing more but a tool for simplification, a construct which is reproduced in legal thought and training, even as a pedagogical tool in order to train undergraduate students.[238] In that sense, some argue that the public private divide has vanished,[239] and some favour a theoretical understanding beyond such dogmatic differentiations.[240] Kaarlo Tuori, for example, argues that the global legal structure is in fact '…an epitome of legal hybridization'.[241] Tuori contends that

> [w]hat we call today legal hybridity is a sign of our conceptual confusion: new conceptual and systemizing grids are needed, but our legal mind-set is still in many respects attached to the state-sovereigntism of the black-box model and the distinctions of traditional systematization.[242]

While the deeper discussions on the nature of a public/private distinction and its decline are done elsewhere, it is important to keep in mind the problematic nature of such conceptualizations. Particularly because a conceptualization of individual privacy often rests on clear distinctions between public and private realms, leading to massive conceptual problems of the legal understanding of privacy. What makes

---

[237] Ibid, 1424.

[238] Hans Micklitz derived such arguments from Walter van Gerven and Felix Frankfurter. See Micklitz H, 'Rethinking the Public/Private Divide' in Maduro M, Sankari S and Tuori K (eds), *Transnational Law: Rethinking European Law and Legal Thinking* (Cambridge University Press 2014) 271-306, 271, 274.

[239] See e.g. Duncan Kennedy, 'The Stages of Decline of the Public/Private Distinction' (1982) 130 University of Pennsylvania Law Review 1349, and Hans Micklitz, who links '…the emergent state nation in the seventeenth and eighteenth centuries to the rise of the public/private divide, the nation state of the nineteenth and twentieth centuries to the early development of hybrids in all variations and the twenty-first century to the full development of the market state in which the vanishing of the divide is open-ended and the future of the divide uncertain, since it requires redefinition of the role of the state and the functions of the private.' Micklitz H, 'Rethinking the public/private divide' (n 238), 306.

[240] See e.g. Marx G, 'Murky Conceptual Waters: The Public and the Private' (2001) 3 Ethics and Information Technology 157, 160.

[241] Tuori K, 'On legal hybrids' in Micklitz H and Svetiev Y (eds), *A Self-sufficient European Private Law: A Viable Concept* (Fiesole: European University Institute Working Papers, 2012), 71.

[242] Ibid, 73.

privacy additionally complex in this regard, is the understanding of privacy as a right because it adds another layer of complexity to the alleged distinction between realms: some understandings of privacy, especially the connection between privacy and freedom led to the paradox situation that a realm of private law is protected by a public legal system from a mere intrusion through the very same public legal system. Additionally, the same right to privacy, as well as the right to data protection, are nowadays permeating into the private sphere horizontally: private individuals also have a right to be protected from violations of their rights through other private actors (such as data collecting companies) not only through the state's *Schutzpflicht* (obligation to protect) but also by direct fundamental rights obligations imposed on companies by heavy regulation of data processing and the emergence of data protection as a fundamental right. Understanding privacy in public in a more multi-dimensional way or in terms of legal hybrids is therefore more useful than relying on the clear distinctions of concepts.

Theoretically, the clear distinction between private and public realms is therefore problematic. What follows from this is that the theoretical conceptualization of privacy in public space becomes equally ambiguous. If privacy protection is extended into the public sphere, does this mean that it is in fact an expansion of the private realm into the public space? Additionally, when the clear demarcation of private from public is understood as a concept of liberal market societies, does it mean that privacy fundamentally opposes other rights, such as political participation, public speech, the freedom of assembly, let alone communal or other societal interest?

The answer to those questions depends, once again, on the respective conception of privacy and the argument made above: privacy in public can rest on the conceptualization as liberty or as dignity. While the former is focused on the liberal individual and her freedom from state or public interference, privacy as dignity in fact allows for a recognition of communal and societal interests. Here, it is not the individual and her free will which determines a rather narrow scope of privacy protection in public, but the dignity and the right to personality of the individual including the protection of communal and societal goods, if necessary even against the interests of a single individual.

Expanding a right to privacy into the public sphere means essentially to protect the capabilities of the individual to enter into a relationship with a society. It protects the right to personality and the development of such and therewith essentially the social realm: the ability of an individual to communicate, form relationships with other members in society, and participate in social and political life. Together, those three factors can be seen as an essential compound of private as well as public realms and all of those are protected by the concept of privacy relying on dignity and the right of personality. Understanding privacy as individual liberty opposes this concept because it puts individuals in a secluded space and labels them as free beings.

This is also where hybridity becomes an important tool: In a conception of privacy based on individual liberty the public/private distinction is essential to the demand of liberty. Here, the private realm is constructed as protection against interference from state and public and therewith it is conceptualized as being mutually exclusive. Privacy based on dignity and personality opposes such understandings: privacy here protects the individual in her social settings and in her abilities to participate and communicate, and at the same time the structures of a community as such. This requires an understanding of the legal realms in an alternative way, for example as a legal hybrid.

Understanding privacy in public more as a tool of community protection than the mere protection of individual freedom from public interference rests on the assumption that societies are formed through communities which require the forming of relationships between individuals, the ability to socially and politically contribute and participate, and the recognition of the importance of communication between individuals.[243] While political and social participation as well as the forming of relationship have a physical relationship with public spaces, communication has gained an essential virtual component.

This is where technological development becomes crucial for privacy in public places, simply because much of societal communication today takes place through digital

[243] Communication is often seen as the essence of political participation, communicative action or even that social systems *are* communication, see, of course, Habermas J, *Theorie des kommunikativen Handelns* (Bd.1: Handlungsrationalität und gesellschaftliche Rationalisierung, Bd. 2: Zur Kritik der funktionalistischen Vernunft, Frankfurt am Main 1981); Luhmann N, *Soziale Systeme: Grundriss einer allgemeinen Theorie* (Suhrkamp 1984).

channels in virtual spheres. In that sense, it is crucial to note that the digitization of communications has added a layer of virtual space to the public realm as much of private and public communications happen in a virtual public space. Additionally, digitization enables the collection of information in the form of data and the creation of virtual networks spanning through spheres that could be characterized as public as well as private. This leads to an ever more hybridization of the legal spaces through which those processed can be addressed. Particularly data protection, which is discussed below, can therefore be seen as connecting public and private spheres.

Privacy in public can of course also be discussed in terms of individual liberty. Particularly in the US legal theory – and probably in other common law systems, privacy in public is a matter of individual defence against state and public intrusions, as the discussion on the conceptualization of privacy above indicated. Especially in US jurisprudence, privacy in public appears to have a close connection with individual liberty and property. The doctrine of 'reasonable expectation' of privacy in public is an outcome of a liberal perspective on privacy in public. The jurisprudential understanding of privacy in the US remained very much limited to trespassing and interference with privately owned land and property up until the 1967 US Supreme Court Judgment in *Katz v US*, establishing the famous doctrine of 'reasonable expectation.'[244] The doctrine describes that persons have a subjective 'expectation' of privacy also in public areas, provided that this expectation is somehow 'reasonable'.[245] US Constitutional Jurisprudence contains an enormous body of discussion and case law on privacy in public place and more detailed discussions would exceed the limits of this study. It is however important to note that the idea of a reasonable expectation of privacy in public areas found its way into European legal jurisprudence.[246] Such expectation-centred perspectives rely on a very particular construction of the individual within the public sphere as an autonomous liberal individual in a market

[244] See Reidenberg JR, 'Privacy in Public' (2014) 69 U Miami L Rev 141, 143.

[245] See *Katz v United States*, 389 U.S. 347 (1967), 361 (Judge Harlan, concurring).

[246] For a more detailed discussion on US constitutional law on privacy in public see e.g. Rosen J, 'Privacy in Public Places' (2000) 12 Cardozo Studies in Law and Literature 167 and Reidenberg JR, 'Privacy in Public' (2014) 69 U Miami L Rev 141; for a US and Canadian constitutional analyses see Smith RE, 'Sometimes what's public is private. Legal rights to privacy in public spaces.' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge 2012) 370-379; for an overview of a European Common Law perspective see Moreham NA, 'Privacy in Public Places' (2006) 65 Cambridge Law Journal 606.

society, which leads to a very different conceptualization of privacy than if the community – or even some sort of communitarianism – would form the centre of the respective understanding of privacy.[247]

Particularly a liberal perception, however, is vulnerable to the classic critique of privacy as a right merely important for the rich and wealthy. If there was no or only a very limited privacy in public spaces, the right to privacy would become an issue of access to private spaces, and access to private spaces is reserved for those that can materially afford them. Serge Gutwirth articulated such a critique as:

> What does the inviolability of the home mean to the homeless? No one can put into question that residents in luxury apartments and fancy neighborhoods and that owners of estates guarded by security systems and pit bulls have far better opportunities to protect their privacy than people living in decrepit neighborhoods, housing projects, or in one of the endless rows of apartment blocks.[248]

On the one hand, privacy appears therefore as an essential element of possessive individualism and can therefore be criticized as a right only for the privileged, and, probably even worse, as a right cementing the relations of power in liberal market societies.[249] On the other hand, Gutwirth pointed to an antagonism in such a perspective: in fact, for totally free markets, privacy functions as a tool to shield and distort information about individuals.[250] Posner's critique[251] of privacy as a market- and trade- distorting element therefore adds to an antagonism in understanding privacy merely as a protection mechanism for enjoying wealth in a capitalist market society. The question of privacy in public appears crucial to the understandings and conceptualizations of privacy. When basing privacy on liberty, the public space lies (mostly) outside the realm of privacy protection because privacy is essentially understood as related to private space, property, seclusion and secrecy. When privacy

---

[247] Amitai Etzioni discussed a more communitarian centered privacy approach, particularly in the US context. See Etzioni A, *The limits of Privacy* (Basic Books 1999), 183-215 and Etzioni A, 'Communitarian Perspective on Privacy, A Commentary' (1999) 32 Connecticut Law Review 897.

[248] Gutwirth S, *Privacy and the Information Age* (Rowman & Littlefield Publishers 2002), 52.

[249] In a similar way, privacy can be criticized as a right shielding power relations from public scrutiny, See e.g. Allen AL, *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield Publishers 1988).

[250] See Gutwirth S, *Privacy and the Information Age (*Rowman & Littlefield Publishers 2002), 53.

[251] See the Section 2.2.5 above.

is understood in terms of a right to personality deriving from dignity, however, privacy is more than just an individualistic concept. Privacy in public then includes a variety of societal and communitarian ideals in which the individual is seen in her relations and communications with others, and as a part of a community or society. Privacy then regulates and allows emancipatory arguments against restraint, coercion and control.

In many ways, data processing has added another layer to the public/private space dichotomy. Nissenbaum, for example argued, that many of the classic privacy conceptions were problematic because merely applying privacy to intimate, private and personal spheres would fail to acknowledge threats to privacy from sophisticated (public) data processing: This is

> …problematic not because they develop normative accounts of privacy that protect the personal and intimate realms from interference, but because they neglect the relevance to privacy of realms other than the intimate and sensitive.[252]

In fact, the processing of vast amounts of information with digital means adds an additional dimension to privacy in public: Firstly, privacy as controlling one's personal information becomes an essential component of a conceptualization of privacy and secondly, virtual spaces additionally blur the boundaries between public and private spaces.

In fact, modern surveillance often does not mean that a specific person is targeted and her intimate secrets are collected, but that all members of society are somehow subject to tacit surveillance practices as information and data is collected as a by-product of daily life.[253] Once privacy derives its essential value from freedom, the conclusion is that there is a certain 'legitimate interest' of the individual also in a public sphere.[254]

---

[252] Nissenbaum HF, 'Toward an Approach to Privacy in Public: Challenges of Information Technology' (1997) 7 Ethics & Behavior 207, 210.

[253] See Schneier (n 1), who describes data as an essential by-product of computing. With computing becoming an essential element of daily life, data becomes a by-product of life which is increasingly dependent on data. For a future vision see Kaskinen T and others, 'The Future as Told Through the Garden and the Streets. Scenarios for the Hyperconnected Nordic Societies of 2015-2040' (The Naked Approach, Demos Helsinki, 2015) http://www.demoshelsinki.fi/wp-content/uploads/2015/11/Naked-approach.pdf accessed 24 April 2016, esp 24-51.

[254] See e.g. Nissenbaum HF, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559, 590-591. For further elaboration see also Nissenbaum HF,

On the other hand, when the essence of privacy is derived from dignity and personhood, the controlling of personal information as well as being in a way free from surveillance and control are essential to privacy in public spaces. Once again, the scope and application of privacy in public depends on the conceptualization of the many different 'privacies'.

***

This section discussed various theoretical aspects relating to privacy. Privacy self-evidently is a complex concept and indeed defies one single definition and conceptualization, and the perspective on privacy often determines its practical legal relevance. Privacy as a concept, however, has come a long way from its first legal expression as a right to be let alone to the complex conceptualization deriving from dignity, self-determination and personality rights. Consequently, some theories of privacy have long moved beyond their original conceptualizations, but also beyond their critique.

It is clear that a right to privacy exists and that there are many valid legal arguments which show that privacy does not only play a role for individual seclusion, solitude and expectation, but that privacy as a rights matter in most areas of daily life, also within a public context. Relying on a synthesis between privacy as freedom and privacy as self-determination and dignity shows that privacy works not only in the bathrooms in the villas of the wealthy and powerful, but also in public areas and in realms in which coercion and control are exercised on individuals and groups. Privacy in public places exists as a legal argument questioning semi-visible layers of control and manipulation, such as for example, when an overall societal chill influences individual and political life in public spheres.

It remains to be mentioned, that privacy, despite the apparent ambiguity of its theoretical underpinnings has been cemented as a global human and fundamental rights both in international as well as European contexts. Privacy was enshrined in relevant international human rights sources after the Second World War: Article 12 of the 1948 Universal Declaration of Human Rights (UDHR) prohibits arbitrary

Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford Law Books 2010), 113-126.

interferences with 'privacy, family, home or correspondence' as well as attacks on 'honour and reputation'.[255] The legally binding 1966 International Covenant on Civil and Political Rights contains a similar provision for a right to privacy[256] and there are a variety of other international sources as well as regional human rights protection regimes that come with one or another version of a legal formulation of privacy.[257] What is common to the right to privacy, though, is that it is not an absolute right, which means that privacy can be legitimately interfered with, provided that such limitations can be adequately justified.

The scope of such privacy provisions has been subject to much debate, firstly because naturally the scope of a fundamental right to privacy depends on the respective understanding of privacy as a legal concept as discussed above, and secondly, because the scope of the content of a right to privacy is articulated rather widely. Article 8 of the ECHR, for example, protects 'private life', 'family life', 'home' and 'correspondence', four concepts which each require detailed analyses in order to grasp all the possible cases falling into their realms. The ECtHR, for example, repeatedly held that the term private life was 'broad' and 'not susceptible to exhaustive definition'.[258] In that regard it may cover physical or psychological integrity, physical and social identity, gender identity, sexuality, personal development as well as a variety of cases relating to surveillance, wiretapping, identification, criminal procedure, non-discrimination and inclusion as well as freedom of communication.

The UN HRC CCPR General Comment No 16 specifies regarding the scope of ICCPR article 17 that it covers information relating to an individual's private life, the integrity and confidentiality of correspondence, various forms of surveillance, intrusions into a

[255] Art 12 Universal Declaration of Human Rights (UDHR), 10 December 1948, UNGA Res 217 A(III).

[256] Art 17 International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, entered into force 23 March 1976, 999 UNTS 171.

[257] See e.g. Art 8, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, (ECHR) Council of Europe, 4 November 1950, ETS No. 5.

[258] See e.g. *Pretty v The United Kingdom*, App no. 2346/02, Judgment, Court (Fourth Section), 29.04.2002 para 61, *Peck v The United Kingdom*, App no. 44647/98, Judgment, Court (Fourth Section), 28.01.2003 para 57.

person's home, body searches, medical examinations as well as gathering and holding personal information on computers, data banks and other devices.[259]

Of particular relevance to EU law is of course the Charter of Fundamental Rights of the European Union (EUCFR)[260], which became a binding document for EU Institutions and the Member States when implementing EU Law with the 2009 Treaty of Lisbon. The EUCFR therewith stands next to the ECHR within the realm of privacy protection in Europe and contains a separate article on the right to personal data protection (art 8) next to the 'right to respect for his or her private and family life, home and communications' in article 7. As mentioned, privacy is not an absolute right and there are a variety of mechanism in each relevant international source allowing for derogations and limitations of the enshrined rights. How public surveillance through sophisticated technologies as described in the scenario falls into the realms of protection of the existing rights will be discussed in connections with some of the specific surveillance issues below. The respective mechanisms for permissible limitations is discussed separately in Section 2.5.2 below.

For now, this discussion moves away from the legal theoretical foundations of privacy towards what appears as a separate theme next to privacy and its implications: namely personal data protection. Data protection is discussed separately because it has a special relevance in legal arguments addressing surveillance. Data protection is part of the scope of protection of a right to privacy, both within the ECHR as well as the ICCPR, as the HRC's General Comment No 16 showed.

Data protection is additionally of special relevance as it directly addresses and regulates the means and methods of information collection. Information processing, however, appears to be essential for our modern digital world and therewith comes with an enormous rise in the possibilities for surveillance. Furthermore, the regulation of data collection and processing has been subject to regulation through countless documents, ever since States and private entities started to process information with the help of computer and digital technologies. The following section discusses some

[259] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, paras 8-10.

[260] Charter of Fundamental Rights of the European Union (EUCFR), 18.12.2000, OJ 2000/C 364/1.

of those issues in relation to privacy and outlines the importance of the concept of data protection for surveillance.

2.3 Data Protection and Information Law

Both the right to privacy as well as the concept of security[261] play important roles in the debates on the surveillance of public places in Europe. Recently, however, another field of law has come to the fore, particularly on the stages of EU fundamental rights jurisprudence: the right to data protection and certain other, more particular rights and principles deriving from it. Data protection is essentially connected to surveillance as it regulates the collection and processing of all sorts of information about individuals. With the gathering of information about groups and individuals in public places, data protection, its principles, and legal systematics are crucial for legal analyses of public surveillance practices. This section therefore outlines data protection and its key elements.

2.3.1 The Emergence of Data Protection in Europe

Data protection and its legal regulation is not anything particularly new. It has started to play a role in modern regulation and legislation since the first processing systems and electronic databases began to emerge. In many ways, data protection is about the law regulating information including its collection, retention and processing. In the early advents of information and law, the legal literature in the field focused on the regulation of new technological aspects of processing information.[262] In fact, also Warren's and Brandeis' famous article on privacy partly derived from the emergence of small and portable handheld photographic cameras and resulting advancements in print media.[263]

The first data protection legislation in Europe emerged through regional and national laws starting with the 1970 Data Protection Law of the German state of Hesse as the first of such laws worldwide.[264] Sweden followed in 1973 with the first national data

[261] Security will be discussed separately in Section 2.4 below.

[262] See Reed C, *Computer Law* (Oxford University Press 2012), xi. See also Cannataci JA, *Privacy and Data Protection Law: International Development and Maltese Perspectives* (Norwegian University Press 1986), Rowland D, Kohl U and Charlesworth A, *Information Technology Law* (4th edn, Routledge 2012), Lloyd IJ, *Information Technology Law* (6th edn, Oxford University Press 2011), which focus extensively on the various aspects and relationships relating to new technology information and law.

[263] See Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 194.

[264] Hessisches Datenschutzgesetz, GVBl. II 300-10, p 625, see also González-Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2015), 56.

protection law (Swedish: Datalag)[265] which has been described as a result of debates around the means and methods of a public census in Sweden in 1969.[266] Soon after, many other European States, including Germany in 1977[267], France[268], Denmark, and Norway in 1978,[269] Luxembourg in 1979, as well as later the United Kingdom in 1984 and Switzerland in 1992[270] There are also some examples of early constitutional recognition of data protection such as in Portugal, Austria and Spain.[271] While some national data protection instruments were drafted and implemented smoothly in some countries such as in Sweden[272], in some others they were subject to intense debate. In Finland, for example, the committee which attempted to draft data protection legislation was dissolved in 1974 due to fundamentally opposing political views on data regulation and did not resume its work until the 1980s, leading to the parliamentary approval of the Finnish Personal Data Files Act only in 1986.[273]

Data protection hence became a core issue in law making and jurisprudence in the 60s and 70s, as a result of increased technological capabilities by states to collect, store and process citizens' data through technological means. Computers gained influence in public and social administrations and personal data processing and population registration entered into the picture just at a moment where many states were

[265] Datalag (1973:289), Svensk författningssamling 1973:289, t.o.m. SFS 1998:377.

[266] For a detailed discussion see González-Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2015), 58.

[267] See Bygrave LA, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 5-6.

[268] Law on Computers, Files and Freedoms, Loi no 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 6 January 1978.

[269] In Denmark, two data protection acts separately regulated private and public databases, and Norway passed the Data Registers Act. For a more detailed discussion see González-Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2015), 65-66.

[270] See Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Agre P and Rotenberg M (eds), *Data Protection in Europe* (MIT Press 1997), 219 fn 3.

[271] González-Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2015), 66-70.

[272] See Seipel, P 'Sweden' in: Blume P (ed), *Nordic Data Protection Law* (Kauppakaari, DJØF 2001) 115-151, 116; see also Bygrave LA, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 5.

[273] See Saarenpää A, 'Data protection: In pursuit of information some background to, and implementations of, data protection in Finland' (1997) 11 International Review of Law, Computers & Technology 47, 48; Saarenpää, A 'Finland' in Blume P (ed), *Nordic Data Protection Law* (Kauppakaari; DJØF 2001) 39-78, 42.

conducting significant social reforms, requiring the retention and processing of large amounts of population data, without which the governance and administration of modern welfare states would have become very difficult.[274] In fact, the discussions about privacy in the 60s and 70s were significantly determined by the emergence of new data protection capabilities through computers as well as the willingness and necessity for states, public administration and security authorities to employ them.[275] Large data banks and population registries were often seen as threats to people's rights,[276] especially when those means were used – often in secrecy - by security authorities.[277]

Victor Mayer-Schönberger divided early stage legal data protection instruments into first-, second-, and third generation data protection norms. The first generation data protection laws derived from the need to respond to large data processing in databases by states and large entities and while focusing on the functionalities of large data collection and processing, they were also seen as a tool to 'tame' the use of new technologies and data processing in government activities.[278] The second generation data protection included drafts and regulations, such as the Austrian, Spanish and Portuguese constitutional inclusion of informational privacy rights or the French, Norwegian and Danish data protection laws, which were characterized by a strong focus on individuals and their rights.[279] With this, data protection expanded from a purely functional approach to regulating big data processors to the inclusion of micro level personal data processing. In that sense, those changes can be seen as a reflection of expanding technologies, the emergence of networks and the 'World Wide Web' and the fact that the processing of personal information became a general practice.

[274] See Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Agre P and Rotenberg M (eds), *Data Protection in Europe* (MIT Press 1997), 222, Siemen B, *Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006), 36.

[275] See Bygrave LA, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 93.

[276] See Siemen B, *Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006), 36

[277] See Cameron I, *National Security and the European Convention on Human Rights* (Iustus 2000), 177, 178.

[278] See Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Agre P and Rotenberg M (eds), *Data Protection in Europe* (MIT Press 1997), 221-225.

[279] Ibid, 227.

Understanding informational privacy as a classic privacy right came with certain problems: Mayer-Schönberger pointed out that

> [c]itizens and society are so intensely and subliminally intertwined that a deliberate attempt by an individual to resist such information requests, if possible at all, carries with it an extraordinary social cost. Similarly, from bank and money matters to travel and voting, disclosure of personal information more often than not is a precondition to individual participation.[280]

This raised the question, if data protection as a defence against information processing *per se* can be a functional and efficient mechanism in societies increasingly dependent on data.

As a response to those new challenges, Mayer-Schönberger regarded a Court decision of particularly important for a European understanding of data protection: the early construction of an explicit 'right to informational self-determination' by the German FCC. He saw the German Constitutional Court's decision as a prime example for the emergence of the third generation of data protection regulation; one that grants more options for participation in decisions about the processing of an individual's personal data and one that quickly gained influence in the debates around data protection as a right throughout Europe.

On the 15th of December 1983, the German Federal Constitutional Court delivered its landmark judgement in the Census-Decision (*Volkszählungsurteil*) already briefly discussed above.[281] In this decision, the Federal Constitutional Court developed the individual right to informational self-determination, deriving from a person's inviolable dignity in art 1 (1) in connection with a general personality right in art 2 (1) of the German Constitution.[282] The Court argued that because modern data processing enables the infinite collection, retention and processing of data about individuals as well as the creation of profiles, individuals would lose the ability to determine what information is collected, retained and shared about themselves which could lead to a behavioural chilling effect.[283] In the words of the FCC:

---

[280] Ibid, 228.

[281] [Germany] FCC, BVerfG, 15. Dezember 1983 (Volkszählungsurteil), (n 145).

[282] See Art 1 (1) in connection with Art 2 (1) German Basic Law, Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Artikel 1 des Gesetzes vom 23.12.2014 (BGBl. I S. 2438).

[283] [Germany] FCC, BVerfG, 15. Dezember 1983 (Volkszählungsurteil), (n 145), C II 1 a, para 171,172.

> A right to informational self-determination is not combinable with a social order, and a legal order enabling it, in which citizens cannot know who knows what, when and in which occasion about them. A person who is insecure if deferring behaviour is noted, shared and indefinitely retained will try to avoid raising attention through behaviour.[284]

Hence, essentially, a right to informational self-determination meant that individuals have to be enabled to have some kind of control over their personal data. Control over one's personal data would liberate the individual from constraints and fear, and therewith countering a 'chilling effect' of personal behaviour, through which personal autonomy to act and communicate would be impaired and consequently can have a severe impact on democratic societies.[285]

On further examination, it can be seen that this encompasses several data protection aspects, such as control, access or rectification of information as well as the limitation of disclosure, minimalistic collection or the specification of a processing purpose.[286] Mayer-Schönberger is right in his analyses that this argument can lead to a more participatory understanding of data protection:

> Individual liberty, the right to ward off invasions into personal data, was transformed into a much more participatory right to informational self-determination. The individual now was to be able to determine how he or she would participate in society. The question was not whether one wanted to participate in societal processes, but how.[287]

With the articulation of the right to informational self-determination, Mayer-Schönberger identified a third generation of data protection regulation and he regards the German census judgment as a development towards a more participatory approach for individuals in data protection.[288] On the other hand, he argued that the concept of informational self-determination also gave an individual a wide element of choice as to what data about her can be collected and processed by whom and when. In that sense, informational self-determination could be seen as giving a wide contractual

---

[284] Ibid, para 172, own translation.

[285] See also Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' (n 162), 47.

[286] Bygrave developed 'core principles of data protection laws' in Bygrave LA, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 57-69.

[287] Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Agre P and Rotenberg M (eds), *Data Protection in Europe* (MIT Press 1997), 229.

[288] Ibid, 229.

freedom to individuals to tolerate and consent on issues concerning waiving their data protection standards.[289]

As a consequence, to this allegedly unlimited freedom to individual consent the next (fourth) generation data protection standards attempted to '…equalize bargaining positions by strengthening the individual's position vis-à-vis the generally more powerful information-gathering institutions' and, at the same time, '…take away parts of the participatory freedom given to the individual in second- and third-generation data-protection norms and subject it to mandatory legal protection.'[290] Mayer-Schönberger sees for example the general ban on data processing of sensitive data in the 1995 EU Data Protection Directive as a sign for such legal protection.[291]

The understanding of data protection therefore has changed since it first emerged. It is not a coincidence that the collection of information faces similar problems in specification and definition than the more general concept of privacy. Data protection, however logically has its roots in an understanding of privacy which advocates control and power over personal information. This understanding, however, produces similar antagonisms as the distinction between individual centred privacy protection and privacy as a societal value. Interestingly, though, particularly the argument that individuals need complete control over the sharing of information (and therewith the right to informational self-determination) derives from a legal argument based on dignity and personality. Complete realization of informational self-determination for individuals, however, embodies the core idea of free individuals and therewith comes with its own problems. While privacy as a derivate of dignity includes a societal component, data protection appears as a more choice-and consent- centred issue, and therefore takes a more liberal approach. An individually centred right to informational self-determination, without a societal or communitarian component therefore appears to contradict a dignity- and right to personality-based approach to data protection as a communal value *per se*. In that sense, data protection based on control and choice has

[289] Ibid, 232.

[290] Ibid, 232-233.

[291] Ibid, 233.

a different conceptual basis than privacy as a derivate of human dignity with its importance as a societal value.

2.3.1.1 Data Protection in the International Sphere.

Apart from the developments in national jurisdictions, data protection has also developed as an issue on the international sphere. Data protection is not enshrined as a separate right in classical international human rights instruments, [292] and consequently, the protection of personal data is considered to be part of a general right to privacy. Privacy has been a fundamental right in Europe ever since the first human rights treaties were drafted after the Second World War. Privacy is enshrined in the first non-binding international document on human rights: article 12 of the Universal Declaration of Human Rights (UDHR) states that

> [n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the legally binding 1966 International Covenant on Civil and Political Rights states the same, with the exception that it adds the word 'or unlawful' before 'interference' in the first sentence. In its 1988 ICCPR General Comment No 16 on the right to privacy, the UN Human Rights Committee stated that all collection and retention of personal information must be regulated by law and therewith included data protection into the scope of the right to privacy of art 17 ICCPR.[293] It furthermore requires state parties to the ICCPR to respect fundamental standards such as fair and lawful processing and use, data accessibility, and control as well as rectification or deletion.[294]

Data protection has also played a significant role in the international plane mostly due to the fact that data and data-exchanging networks became increasingly important to the cross-border operations of states and businesses.[295] Consequently, international organizations such as the UN, the OECD and the Council of Europe drew up early

---

[292] See Siemen B*, Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006), 39.

[293] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, para 10.

[294] Ibid, para 10.

[295] See Siemen B, *Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006), 39-41

documents addressing data issues. For example, in autumn 1990, when the UN General Assembly adopted a document titled 'Guidelines Concerning Computerized Personal Data Files' in which it laid out several minimum data protection principles such as for example purpose-specification, lawfulness, accuracy or data security.[296]

2.3.1.2 The Sources of Data Protection in Europe

Also, the Council of Europe European Convention of Human Rights (ECHR), of which the drafting history began in 1950, enshrines privacy as a 'right to respect for (…) private and family life, (…) home and (…) correspondence'. Consequently, privacy including data protection is far from being a new right in Europe and its substance and scope have been developed in many different directions within the European legal order.

There have, of course, been extensive debates on the many different aspects of privacy and data protection and there is an extensive body of case law developed by the European Court of Human Rights (ECtHR). What is relatively new within the European framework of fundamental rights protection is another fundamental rights document which derives from the European Union: The Charter of Fundamental Rights of the European Union (EUCFR) entered into force with the Treaty of Lisbon on 1st of December 2009 and is meant to close a gap between Community Law and existing fundamental rights protection in Europe. The EUCFR particularly aims to tackle fundamental right issues that are related to technological development in societies, and it wants to '…strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter.'[297] As a matter of fact, the EUCFR enshrines not only privacy as a right in article 7, but also establishes a fundamental right to personal data protection in article 8. Previously, data protection has been recognized as being part of the scope of privacy, for example when the ECtHR recognized the mere retention of personal information as interference with private life in article 8, which will be discussed in more detailed below.

---

[296] See UN GA Guidelines for the regulation of computerized personal data files, Adopted by General Assembly resolution 45/95 of 14 December 1990, A/RES/45/95.

[297] Charter of Fundamental Rights of the European Union (EUCFR), 18.12.2000, OJ 2000/C 364/1, Preamble.

International regulation of data protection consequentially has played an important role already at the dawn of the information society, when computers and information processing became a necessary part in society and in all kinds of state administrations. The Council of Europe ever since has played an important role in laying out core principles for data protection and its shift towards a fundamental right. In 1973 and 1974 the CoE Committee of Ministers adopted Resolutions on individual privacy and data collection in the private and public sector, both outlining core principles of collection and storage of information in databanks, including for example fair means of collection, purpose specification, right to access and rectify personal information as well as the requirement of legal bases for public area data collection and retention.[298] Then, in 1981, the Council of Europe adopted the first legally binding international data protection instrument, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[299] This Convention is essentially an international treaty signed and ratified by the Member States of the Council of Europe and Uruguay as the only non-CoE member[300] and applies to the automatic processing of personal data in both the public and private sectors.[301] It enshrines several basic principles of data protection including protection against abuse, fair and lawful collection and processing as well as purpose specification and proportionality. Additionally, article 12 addresses trans-border data flows, in combinations with a 2001 additional protocol to the Convention containing also provisions on third-country data flows and supervisory authorities in the member

[298] See Council of Europe, Committee of Ministers, Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies); and Resolution (74) 29 on the protection of individuals vis-à-vis electronic data banks in the public sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

[299] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (CoE Data Protection Convention), Council of Europe, 28 January 1981, entry into force 1 October 1985 ETS No. 108.

[300] The CoE Data Protection Convention is signed by all 47 member states, however, not ratified by Turkey.

[301] See Art 3 CoE Data Protection Convention.

states.[302] With this, the Council of Europe data protection framework is the most encompassing system predating the complex EU data protection regulations.

2.3.1.3 Data Protection in the EU

Data Protection in the EU consists of a variety of complex regulatory instruments and recent developments both in jurisprudence and legislative procedure. The current EU data protection reforms established the directly applicable General Data Protection Regulation (GDPR) and the Directive on the protection of personal data processed for law enforcement purposes[303] and the resulting upcoming changes in public and private data protection regulation make this field one of the most interesting in current EU law discussions.[304]

In order to give a brief overview of the relevant data protection instruments available in the EU at this point, the most important is currently still the Data Protection Directive 95/46/EC adopted in 1995.[305] The essential purpose of the Directive is to harmonize certain data protection standards and therewith make easy common market activities in an area which became extremely important for public and private sector in the EU and EEA area. Its scope includes therefore the to '…processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'[306] Excluded, however, are activities which fall outside

[302] See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Council of Europe, 8 November 2001, ETS No.181.

[303] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L 119, 4.5.2016, 1–88 and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, 89–131.

[304] It should be stressed that the European Union has a special mandate for ensuring data protection throughout its territory in Art 16 TFEU. For an extensive discussion on this article see Hijmans H, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer Berlin, Heidelberg 2016).

[305] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281, 31.

[306] Art 3 (1) Directive 95/46/EC (Data Protection Directive) (n 305).

of the scope of Community law such as public security or defence as well as processing by natural persons '...in the course of a purely personal or household activity', the so called household exemption. The harmonization of national laws through the Directive has the purpose of ensuring a certain level of protection within the Community as well as codify and expand certain data protection principles already enshrined in the Council of Europe Framework. In that regard, with coherence in Member States of Council of Europe and EU, divergent data protection standards would not have been feasible. Other Directives that are part of the EU data protection framework include the ePrivacy Directive that shall ensure equal protection levels of privacy rights in the area of electronic communications[307] and which lays out more specific provisions on information security, confidentiality of communications, traffic data as well as certain categories of data such as location data. Directive 2002/58/EC has since then been amended by several other EU legislations, including the repealed Directive 2006/24/EC (data retention) and Directive 2009/136/EC (cookies).[308]

With the adoption of the General Data Protection Regulation in April 2016, the EU 1995 Data Protection Directive will be replaced and the new data protection standards will come directly applicable within all member states on the 25th of May 2018. While the scope of the GDPR applies to public, as well as private data processing activities falling within the scope of EU law, the data protection reform process also resulted in the adoption of a new so-called 'Police'-Directive, which applies to personal data processing for purposes of public security, prevention, investigation, detection or prosecution of criminal offences.[309]

---

[307] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002, 37-47.

[308] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, (Data Retention Directive), Invalidated 8.4.2014, OJ L 105, 13.4.2006, 54-63; and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, 11–36.

[309] Directive (EU) 2016/680 (n 303).

An additional step in the modernization of European data protection rules will be the upcoming reform of the so called 'ePrivacy' Directive, which is going to be replaced by a new Regulation on Privacy and Electronic Communications.[310] Foreseeably, this Regulation will set new standards for all sorts of electronic communications, including for example messenger- and social media services.

2.3.2 Data Protection as a Fundamental Right?

An essential part of EU data protection today is the Charter of Fundamental Rights of the European Union (EUCFR). The EUCFR entered into force with the Treaty of Lisbon on 1st of December 2009 and is meant to close the gap between Community Law and existing fundamental rights protection in Europe. The Charter also specifically aims to tackle fundamental right issues that relate to technological development in societies; it wants to '…strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter.' The EUCFR enshrines, as the first international document, not only privacy as a right in article 7, but also a fundamental right to personal data protection in article 8. Article 8 ensures a right to personal data protection for everyone and at the same time lists several core principles of data protection, namely fair and lawful processing, purpose specification, consent of the data subject, access and rectification as well as the control of those principles by an independent authority.[311] With the coming into force of the Charter, data protection was explicitly mentioned as a fundamental right within the EU legal framework. Consequently, data protection in Europe is a standard that is more and more articulated as a rights-issue, affecting the public and private sectors in similar ways. Evidence of this can also be found in the recent case law of the CJEU, employing rights based arguments in order to address data protection problems arising from the public and private sectors.

[310] See Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10. January 2017, COM(2017) 10 final, 2017/0003 (COD).

[311] EUCFR, Art 8.

On the 8th of April 2014, the CJEU issued a judgment on the compatibility of the European Data Retention Directive (2006/25/EC) with fundamental rights in the European Union. The 2006 Directive was a result of widespread and longstanding discussions on the necessity of Europe-wide retention of communication meta-data for purposed of criminal investigations.[312] The Directive required member states of the EU to implement national law obliging Telecommunication Service Providers (TSP) to store meta-data of citizens' communication from 6-24 months and allow law enforcement access to these data. Meta-data in this context meant all data related to a person's communications including internet usage hence '…traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user'[313] but not the actual content of communications. From the beginning, the Directive has been subject to heavy criticism and several national constitutional Courts have issued judgments partly halting the implementation process.[314]

In April 2014, the CJEU annulled the Directive. In *Digital Rights Ireland*, the Court was specifically asked to examine the Data Retention Directive in light of the fundamental rights to private and family life, data protection and freedom of expression and information (arts 7,8, and 11) of the EUCFR.[315] The Court established a rights interference on the bases that such meta- data would allow for

> …very precise conclusions to be drawn concerning the private lives of the persons (…), such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[316]

[312] See Boehm, F and Cole DM: Data Retention after the Judgement of the Court of Justice of the European Union, Study funded by the Greens/EFA Group in the European Parliament, Münster/Luxembourg, 30.06.2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf accesses 5 October 2015, 11-12.

[313] Art 1(2) Directive 2006/24/EC (n 308).

[314] For a detailed analysis see Boehm, F and Cole DM, 'Data Retention after the Judgement of the Court of Justice of the European Union', (n 312).

[315] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, OJ C 165, 9 July 2012, ECLI:EU:C:2014:317, paras 17-22.

[316] Ibid, para 27.

The Court regarded this as a severe interference with the right to private life and data protection (it did not further examine article 11) and due to the comprehensiveness of the data, lack of safeguards against the risk of abuse, un-proportionality of the interference and controllability of the data ruled the Directive invalid.[317] With this, the court employed a very strong fundamental rights argument and at the same time set standards determining the employment of fundamental rights arguments in the field of data protection.[318] It is clear that the CJEU understands state surveillance as a fundamental rights issue, requiring strong mechanisms and safeguards on the European level. Surveillance, privacy and data protection were seen as an issue of constitutional relevance to the European Union.

The second CJEU case employing a particularly strong fundamental rights argument is *Google Spain*. In this case, the Court ruled that the internet search engine Google has to remove links to sites containing personal information of individuals from their search results if this data outlives the necessity to be processed for the specific purpose at times of collection.[319] This sparked widespread discussions on a right to be forgotten and the general effects on search engine providers that shall not be discussed here,[320] however what is interesting in that context is the fundamental rights rhetoric the Court used. Citing the preamble of the Data Protection Directive (Directive 95/46/EC), the Court stressed that it '…seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.'[321]

With this, the Court clearly laid out a partly hierarchical fundamental right based system as it reads the regulatory regime of data protection in the EU strictly in

[317] Ibid, para 73

[318] For further analyses see Ojanen T, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others' (2014) 10 European Constitutional Law Review 528, and Vainio N and Miettinen S, 'Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States' (2015) 23 International Journal of Law and Information Technology 290.

[319] Case C-131/12 *Google Spain* (n 315), para 93.

[320] For further discussions on the case see Frantziou E, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761.

[321] Case C-131/12 *Google Spain* (n 315), para 66.

connection with the EU Charter of Fundamental Rights and especially articles 7 and 8 therein. The Court explicitly stated that when provisions within the data protection regime touched upon fundamental rights issues such as the right to privacy, they '…must necessarily be interpreted in the light of fundamental rights, which, (…), form an integral part of the general principles of law whose observance the Court ensures…'.[322] Due to those fundamental rights, the status of data protection, the principles of fair and lawful processing, access to information as well a right to rectification need to be implemented by a search engine provider, whose task it would be to assess carefully upon request if the referral to personal information stored somewhere on the internet are still in compliance with those principles after a certain time span. Furthermore, the Court interestingly employed the Data Protection Directive in the Case as a source for laying out mechanisms for permissible limitations into the rights enshrined in art 7 and 8 of the EUCFR.[323]

Without going too much into the detail of the case here, the Court's fundamental rights rhetoric was similar to *Digital Rights Ireland*, where the violation of article 7 and 8 was essentially based on a failed proportionality test. Here now, the Court basically imposed the standard of a fundamental rights balancing test onto a private corporate entity and established the possibility of appealing to a public procedure if that test is not solved to the satisfaction of the complainant.[324]

The third landmark judgment which employed a fundamental rights based argument in assessing privacy issues was the *Schrems* case.[325] The case originated in a request for preliminary ruling on the adequacy of the fundamental rights protection of the so called safe harbour privacy principles deriving from a Commission Decision (2000/520/EC) of 26.07.2000.[326] Essentially, the underlying problematic arose from

[322] Ibid, para 68.

[323] Ibid, para 69.

[324] See Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland*, Judgment of the Court (Grand Chamber), 8 April 2014, ECLI:EU:C:2014:238.

[325] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, Judgment of the Court (Grand Chamber), 6 October 2015, OJ C 35, ECLI:EU:C:2015:650.

[326] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441, OJ L 215, 25.8.2000, 7–47.

NSA data collection and surveillance practices leaked by Edward Snowden during summer 2013, and the social media corporation Facebook transferring data of European citizens to the US which was then legally based on the Commission's safe harbour agreement. The question which arose from Facebook's US data transfers, was how far there really existed an 'adequate level of protection' of personal data in the US and which authority had the competence to evaluate the protection level.

Already in 2013, Maximilian Schrems filed a complaint against Facebook Ireland for those practices with the Irish Data Protection Authority on the bases that the

> …law and practice in force in [the US], did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities.[327]

The DPA rejected the compliant and stated that the Commission's Decision 2000/520 already determined the existence of adequate data protection practices in the US. The Court rejected this opinion.

Again, the CJEU emphasized that

> …the provisions of Directive 95/46, inasmuch as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to respect for private life, must necessarily be interpreted in the light of the fundamental rights guaranteed by the Charter.[328]

Furthermore, 'adequate level of protection' can only mean, in the words of the Court, the requirement for the US as a third country

> …to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.[329]

US legislation, permitting state authorities vast access to personal data and electronic communications, consequently '…must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter' as well with the right to effective judicial protection enshrined in article 47 of the Charter due to the lack of a legal recourse.[330] Such fundamental rights

[327] Case C-362/14 *Schrems*, (n 325), para 28.

[328] Ibid, para 38.

[329] Ibid, para 73.

[330] Ibid, paras 94,95.

interferences need to be strictly necessary in order to be justified and the Court did not see the strict necessity in this case and consequently declared the Commission's safe harbour Decision 2000/520 invalid.[331]

In all three cases, the CJEU has employed strong fundamental rights arguments and it has established specific mechanisms of privacy and data protection norms that apply within the European context.

Firstly, it emphasized the important of the Charter of Fundamental Rights of the European Union as a document with constitutional relevance. Especially when an issue regulated by EU law has the potential of interfering with fundamental rights enshrined in the Charter, all regulatory regimes related to that issue will need to, in one or another way, be interpreted in light of relevant fundamental rights. This is especially the case when the issue concerns the right to private life and the right to data protection.[332] Furthermore, the Court has also applied this argument to other regulatory regimes of the European Union, especially the data protection regime consisting of Directive 95/46/EC and its related Directives, Decisions and Opinions. This indicates the existence of a fundamental rights regime within the European Union which is particularly relevant for surveillance, data protection and privacy. It is also a system of protection which exists parallel to the human rights instrument of the European Convention of Human Rights. What is remarkable, though, is that particularly the *Google Spain* case showed that EU fundamental rights have a strong impact on the private sectors and therewith on private individuals as well as private companies. This means that in cases where EU regulatory instruments regulate conduct in the private sector, the actors in the private sector are bound by EU fundamental rights in the EUCFR, especially in cases concerning privacy and data protection. This shows that EU fundamental rights are directly applicability in the private sector, and therewith appear to unfold a certain '*Drittwirkung*'; especially

[331] Ibid, para 107.

[332] The CJEU has ruled similarly in two other cases which will not be discussed in this context: see Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others*, Judgment, 20 May 2003, ECLI:EU:C:2003:294, para 68; and Case C-212/13 *Ryneš*, (n 107), para 29.

private entities such as companies may be bound by the rights enshrined in the EUCFR.[333]

2.3.3 Conclusion

Privacy and Data Protection are important concepts in Europe and have an important regulatory consequences and constitutional importance. Both are constructed by employing a fundamental rights language and European Courts, as discussed above, have given them further jurisprudential relevance.

Consequently, while Data Protection is often understood as a new legal field, it has had significant practical relevance all over the world since computer technologies came to play a significant role in everyday life. In that sense, the relation of privacy and data protection can be seen as reciprocal: on the one hand the legal concept of privacy, especially when understood as a fundamental right, gained significant importance in the 60s and 70s due to states' data collection (census) and retention activities (data banks). On the other hand, data protection regulation derived their legal arguments from the early discourses and debates about privacy as a right. In other words, it seems that privacy and data protection are concepts that mutually benefitted from each other in many ways and in that sense a strict separation between privacy and data protection appears somehow artificial. Yet, data protection appears to play a particularly separated role in the framework of the European Union.

Today, technological developments and data processing capabilities have reached a new level. On the one hand, data protection is perceived as a right supposedly countering the enormous collection of information on individuals. On the other hand, data has become a tradeable good, even a currency, that is essential for economic growth and development. Even further, the protection of data today is a regulatory instrument that seems to oppose corporate developments and is often seen as an obstacle to all kinds of economic activities, from start-up founding to global trade.

In fact, the question has to be asked how much data protection has transformed into something more than the protection of specific information about individuals. Data today also functions as a currency, as code, as a decision-making tool, as exercising

[333] For an extensive and detailed discussion on 'Drittwirkung' in EU Law see Stein, SK, *Drittwirkung im Unionsrecht. Die Begründung einer Horizontalwirkung allein durch Vorrang und unmittelbare Anwendbarkeit.* (Nomos 2016).

control and even as a predictor of the future. In fact, the functionality of our world is built around data and data protection plays an integral element in that world. Data protection as a fundamental right has to be seen as an integral element in such a world even more than ever before.

Data protection, as well as privacy, therefore are essential for an analysis of public surveillance in an urban setting. In many ways, both privacy arguments, as well as data processing questions are the most important issues when addressing the question of surveillance. This is particularly the case when it comes to surveillance of actual physical public places. The analyses below will address some of the questions around the relationship between privacy and data protection as joint or separate legal arguments addressing public surveillance. Before, however, another topic demands a brief discussion, and that is the concept of security.

2.4 Security

'Security' is the primary and most predominant reason for building surveillance in public places.[334] In fact,

> …in an age when security is as much about monitoring and interdicting flows of capital, people and information as it is about defending borders with conventional military forces, cities are increasingly seen as key sites for security policies and interventions, giving rise to new policing technologies of risk, surveillance and profiling.[335]

Security, however, as a concept is as complex as it is ambivalent. In fact, it can be understood in many ways by different disciplines. On the meta-level, security is a term that has been grasped in different ways in many fields of science. Most prominently, security has appeared as the subject of studies in political sciences, international relations and even forms its own distinct discipline in the social sciences: international security studies.[336] In this context, security can be understood in different ways: for example as traditional and military security, focusing on national security, states and war.[337] Security, however, can also include less state-centric perspectives and the expansions of reference objects: the economy, the environment or international crime and terrorism are a threat to security in a similar way as warmongering states, especially since the end of the Cold War and the shift of perspective from purely external threats to global threats.[338] Further, more thorough and complex approaches to security include amongst others the concept of human security as deriving from the

[334] Security in urban contexts is in fact a very complex issue as urban spaces are complex and problematic. From criminal policy over city planning to countering terrorism, surveillance in its various forms is seen as an important operational tool. For a further and more nuanced discussions on the relationship between security and surveillance in urban contexts see Brennan-Galvin E, 'Crime and violence in an urbanizing world' (2002) 56 Journal of International Affairs 123, and Svenonius O, *Sensitising Urban Transport Security: Surveillance and Policing in Berlin, Stockholm, and Warsaw* (Stockholm University 2011), 1-27.

[335] Abrahamsen R, Hubert D and Williams MC, 'Guest Editors' Introduction' (2009) 40 Security Dialogue 363, 364.

[336] See especially Buzan B and Hansen L, *The Evolution of International Security Studies* (Cambridge University Press 2009) for the formation of security studies as distinct discipline and CASE Collective, 'Critical Approaches to Security in Europe: A Networked Manifesto' (2006) 37 Security Dialogue 443 for some critical approaches.

[337] See e.g. Walt SM, 'The Renaissance of Security Studies' (1991) 35 International Studies Quarterly 211, 212.

[338] See Buzan B and Hansen L, *The Evolution of International Security Studies* (Cambridge University Press 2009), 161-162.

1994 UN Human Development Report which criticized state-centric security conceptions and demanded a focus on individuals, their needs, rights and dignity.[339]

Another, extremely complex but interesting conception is the concept of 'securitization' developed by the so-called Copenhagen School, which constructed security as the subjective speech act of securitization, by which an issue becomes a subject of security when actors articulate it as a security problem, with the intention to claim and justify exceptional measures that would counter the existential threat.[340] Therewith, security problems are not naturally given objective threats, but subjective constructions which ultimately should be handled with care, in other words, should be 'de-securitized'.[341] Such a conception allows for a more distant, in fact, a more critical perspective on security arguments. In that sense, the Copenhagen school presented a critique on traditional realist as well as liberal conceptions of security, in which security is always perceived as something positive and something that needs to be built and achieved.

The Copenhagen School, however, has been debated and criticized extensively. Burgess, for example, recognized the originality of the Copenhagen School approach in its systematization of security as a system of reference and therewith as '…pragmatic *function*, as the transitive *act*, of "securitization".'[342] This, however, would fall short of reflexivity in that it took for granted the securitizing actor as the creator of the securitizing speech act: 'Securitization theory thus identifies the *locus* of the ethical subject of security in the logic of the speech act. And yet this approach is ultimately too narrow, precisely because "organizational logic", like the subject itself, is not neutral, not objectively given.'[343] There is, however, nothing self-evident and nothing neutral in the construction of a securitizing actor and therewith '[b]y

[339] See the United Nations Development Programme (UNDP), *Human Development Report 1994* (Oxford University Press 1994), 24, 25.

[340] See Buzan B, Weaver O and de Wilde J, *Security: A New Framework for Analysis* (Rienner 1998); Weaver, O, 'Securitization and Desecuritization' in Lipschutz RD (ed), *On Security* (Columbia University Press 1995).

[341] Ibid, 57-58.

[342] See Burgess JP, *The Ethical Subject of Security: Geopolitical Reason and the Threat against Europe* (Routledge 2011), 13.

[343] Ibid, 13.

taking the individual embedded in an organizational logic as a given, we miss the ethical nature of the subject.'[344]

Another issue that the Copenhagen School falls short on is a clarification of their understanding of the role of law in the securitization process. For some Copenhagen scholars, '[s]ecurity is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics.'[345] From a legal perspective, emergency measures enacted with the purpose to combat existential threats suggests that there are elements in the thinking of the Copenhagen school which are close to a Schmittian understanding of state of emergency and exception.[346] The state of exception stands therewith beyond the law and beyond all institutionalized forms of political governance and therewith draws a clear line between 'normal' and exceptional times[347] and it is questionable whether such clear demarcations can retain validity in times of permanent emergency measures and the *de facto* permanence of legal and constitutional changes.[348] Despite justified criticisms, however, the Copenhagen School retains theoretical viability, especially when employed as a methodological concepts in order to criticize security arguments as trumps. Constructivist argumentation, of course, is not the only critical approach to traditional perceptions. Security has also been discussed in forms with more critical perspectives: Galtung and the idea of negative and positive peace, and its relations to the concept of structural violence which prevents the liberation of individuals, is one example.[349] Security as a concept of emancipation and therewith ultimately not only the freedom from fear and want, but also the absence of structural violence enable

[344] Ibid.

[345] Buzan B, Weaver O and de Wilde J, *Security: A New Framework for Analysis* (Rienner 1998), 23.

[346] See Carl Schmitt and his famous quote: 'Souverän ist wer über den Ausnahmezustand entscheidet.' Schmitt C, *Politische Theologie* (4 Aufl., unveränderter Nachdruck der 1934 erschienene 2. Auflage, Duncker & Humblot 1985), 11. For further discussion see also Tuori K, 'A European Security Constitution' in Fichera M and Kremer J (eds), *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia 2013),

62, 63 and Kremer J 'Exception, Protection and Securitization: Security Mindsets in Law' in ibid, 19-21.

[347] See Tuori K, 'A European Security Constitution' in ibid, 63.

[348] See e.g. Scheppele KL, 'Global Security Law and the Challenge to Constitutionalism after 9/11' (2011) Public Law 352.

[349] Galtung J, 'Violence, Peace, and Peace Research' (1969) 6 Journal of Peace Research 167

individual to strive for liberation and overcome existing constraining and determining power relations.[350]

2.4.1 Security and the Law

The relationship between security and the law adds another layer of complexity. For law, security is more than just a certain theoretical conception or an approach. In fact, security is often interwoven with concrete legal arguments.

On the one side, in law, security is often used as 'certainty', e.g. as legal certainty, stability and the rule of law as cementing and underlying complex social systems. In that sense, legal certainty is in fact bringing order to chaos, and without legal certainty no constitution or system of fundamental rights protection could thrive. Security, from this perspective, can bring and demand order and can even be conceptualized as a right.

On the other side, 'security' is used in a legal argument as a justification mechanism for certain limitations and exceptions. Here, security can meet law in different ways: Firstly, as limitation and justification within the law, secondly, as amendment to the law, and thirdly, as the ultimate reason for suspension of the law as such. In that sense, security can be understood as functioning *within* the law and *above* the law.[351] Within the law, security arguments can work in order to limit certain rights or as a mechanism of justification. This is because most fundamental rights are not absolute in nature and can be interfered with. The right to privacy in article 8 ECHR, for example, grants everyone '…the right to respect for his private and family life, his home and his correspondence.'[352] Interferences with rights enshrined in article 8, however, can be permitted provided they are '…in accordance with the law', 'necessary in a democratic society' and serve a legitimate interest such as 'public safety' or 'national security', as is explicitly listed in art 8 (2) ECHR. While this appears banal, it illustrates the first

[350] See e.g. Booth K, 'Security and Emancipation' (1991) 17 Review of International Studies 313, and Booth K, *Theory of World Security* (Cambridge University Press 2007).

[351] For a more detailed discussion see Kremer J 'Exception, Protection and Securitization: Security Mindsets in Law' in Fichera M and Kremer J (eds), *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia 2013), 24-35.

[352] Art 8 (1) ECHR.

relation between law and security: safety and security can be reasons for limiting certain fundamental rights.

The second possible use of security within the law would be an in-build mechanism for possible derogations in case of threats or emergencies. The ECHR, again, as an example, contains a specific mechanism for derogations in times of emergency in article 15. Member states can derogate from certain Convention right '[i]n time of war or other public emergency threatening the life of the nation…' provided this follows a specific procedure.[353] In a similar way, many legal sources, especially of an international or constitutional nature, contain or have established mechanisms for limitations and derogations, and the justification for the activation of such mechanisms often uses functional security arguments. Understanding that such arguments are not innocent, de-politicized or objective acts is important when critically engaging with security and law. This is where the methodological framework of the Copenhagen School comes in handy.

The other frequent appearance of security in the context of law happens in areas that could be called 'beyond' the law. Security is used beyond the law when its effect leads to the amendment of law in general, or to permanent changes of legal sources, *because of* an alleged security problem. In that sense, urgent security problems can modify existing legal systems and mechanisms in many ways, one of them can be seen in the expansion of investigatory powers and repressive security actions after large-scale terror attacks. The global change of counter-terrorism laws after 9/11[354] can be regarded as one example of 'global security law' in which existing legal systems of rights protection have been systematically weakened.[355] While a state of emergency *within* the law is by definition of a temporary and exceptional nature,[356] an emergency

[353] Art 15 ECHR, see also Hartman JF, 'Derogation from Human Rights Treaties in Public Emergencies-A Critique of Implementation by the European Commission and Court of Human Rights and the Human Rights Committee of the United Nations' (1981) 22 Harvard International Law Journal 1.

[354] See e.g. Roach K, 'Sources and Trends in Post-9/11 Anti-Terrorism Laws' in Goold BJ and Lazarus L (eds), *Security and Human Rights* (Hart 2007), 230-256

[355] See Scheppele KL, 'Global Security Law and the Challenge to Constitutionalism after 9/11' (2011) Public Law 352, 356.

[356] Lawful states of emergency must be limited in time and space. There is extensive case law and legal opinions on states of exception in Europe, particularly by the Council of Europe and the ECHR as well as the European Commission for Democracy through Law (Venice Commission). See e.g. Venice Commission, Opinion on the Protection of Human Rights in Emergency Situations adopted by the

beyond the law leads to the amendment of existing laws, drafting of new laws or to the dismissal of laws entirely, for example in times of war, crises or revolutions. A more detailed discussion on states of emergencies and security however, has to be made elsewhere. The following section focuses on the implications of security on public surveillance.

2.4.2 Public Surveillance and Security

While the terminology of security in law can function as a tool for certainty as well as a mechanism for the justification of limitations, exceptions and even suspensions of laws, the relationship between security and the public space are more concrete. What is remarkable, though, is that wide varieties of discourses on public spaces address security issues. Essentially, security and public spaces revolve around three terms: public order, public safety and public security. While public safety and order are essentially terms addressing the functionality of public places, the more general and more abstract public security addresses aspect of threats and the survival of the public space as such.

What makes security a fascinating theoretical concept is that within a public place, it is essentially a mind-game. Making a public place safe requires the capabilities to control the space to some degree. In this context, 'controlling' means to be able to alter and steer events and activities in a particular frame. The degree of necessary and adequate control, however, is determined by the security mindset of the actors, institutions and logics which perceive it as their task to control that particular space.

2.4.3 The Right to Security

The discussions on the concept of security above focus on the relationship between security and the law above looks at security as a political issue and as a tool that works as a justification for certain limitations or even exceptions. In this sense, security presents one side of a balancing argument: in order to legitimately interfere with rights and freedoms. Security and its perceived necessities need to be balanced and weighted

---

Venice Commission at its 66th Plenary Session, 17-18 March 2006, CDL-AD (2006)015, No. 10; and a recent Opinion on the French emergency measures after the 2015 Paris attacks: Venice Commission, Opinion on the Draft Constitutional Law on 'Protection of the Nation' of France, Adopted at its 106th Plenary Session, 11-12 March 2016, CDL-AD(2016)006 No. 838.

against losses, values, rights and general freedoms as such.[357] Therewith, security is discussed in terms of oppositions such as security v liberty[358] or liberty v control.[359]

Law, however, can address security in another way: security in fact can be perceived as a 'right'. This way of approaching the topic somehow represents a turn in perspective: while the starting point in the discussion of the relationship between security and law above is 'security', another perspective is to prima facie start from 'the law'. Law, includes security also in a way that goes beyond a mere reason for legitimating certain interferences; and that is in the conceptualization of security as an individual right. But is there really a unique and distinguishable right to security, as there is a right to privacy? Can the right to security therefore be balanced against the right to privacy? And is there a right to security in certain circumstances, such as in a public space and are there certain obligations for states and their security authorities to secure a public area, for example with surveillance means?

2.4.3.1 The ECHR and a Right to Security

Looking at legal sources, the right to security is indeed included in the European Convention on Human Rights. Article 5 (1) reads: 'Everyone has the right to liberty and security of person.' While this as such is rather indeterminate, article 5 continues with a list of reasons justifying the deprivation of liberty making clear that article 5 in fact is about detention, imprisonment and arrests and therewith addressing fundamental principles regarding the deprivation of liberty rather than granting individuals an overarching right to security. It might still be argued, however, that a general right to security would be valid in areas, where special rights do not apply. A general human right to security would hence be related to the change of the security

[357] For a general discussion on such balancing, see Petman J, 'Egoism or altruism? The politics of the great balancing act' (2008) 5 No Foundations Journal of Extreme Legal Positivism 113. See also Lazarus, L 'Mapping the Right to Security' in Goold BJ and Lazarus L (eds), *Security and Human Rights* (Hart 2007) 325-346.

[358] See e.g. Waldron J, 'Security and Liberty: The Image of Balance' (2003) 11 Journal of Political Philosophy 191.

[359] Bruce Schneier argues that the dichotomy of a trade-off between security and privacy is a false one: in fact the debate is about liberty vs control. See Schneier B, What our top spy doesn't get: Security and Privacy aren't opposites *Wired.com*. (24.01.2008) http://www.wired.com/2008/01/securitymatters-0124/ accessed 23 March 2016.

object from states and entities to individuals, such as in the UN human security conceptualization. There is, however, reason for caution.

That is because it is important to distinguish between the argument that security *per se* would be a pre-condition for the enjoyments of rights, for example, when a certain amount of security in a public space would be required in order to guarantee freedom of expression, and actually basing fundamental rights on an overarching right of security. Lazarus, in this context, warned that there was a principle '…difference between securing rights and "securitizing" rights'.[360] Indeed,

> [t]here is a danger when the right to security slips into becoming the meta-principle grounding other rights, it can also displace the non-instrumental values upon which it properly ought to rest. In this way the right to security can inadvertently legitimise security measures that encroach upon those values it has now displaced.[361]

A right to security has to be therefore regarded as highly problematic. Apart from such criticism, a right to security is de-facto conceptualized in legal sources beyond the above mentioned article 6 ECHR: In the South-African constitutional bill of rights, for example, a 'right to freedom and security of person' is defined beyond the deprivation of liberty in Section 12. It also includes a right 'to be free from all forms of violence from either public or private sources', as well as all aspects of torture and cruel, inhuman or degrading punishments.[362] Section 12 also includes the right to 'bodily and psychological integrity' which enshrines aspects of reproduction and self-determination. This is interesting, as many of the aspects in Section 12 could, from a European perspective, be subsumed under the right to 'private life' in article 8 ECHR. In Europe, a certain 'right to security of the person' could therefore also be derived from personal integrity and self-determination rights surrounding a right to privacy.

More generally, however, the right to security has more and more been distinguished from the right to liberty and, as a more general trend, has been established as a lone-standing right in different contexts.

---

[360] Lazarus, L 'Mapping the Right to Security' in Goold BJ and Lazarus L (eds), *Security and Human Rights* (Hart 2007) 325-346, 328.

[361] Ibid, 328.

[362] Bill of Rights (Chapter 2 of the Constitution of the Republic of South Africa), No. 108 of 1996, Section 12.

From a constitutional law perspective, this trend appears to follow three steps: Firstly, the right to security is detached from liberty and articulated as a separate right, secondly the applicability and scope of security is expanded from a purely vertical public-private relationship to multi-dimensional application including public and private actors (as the horizontal effect or so called '*Drittwirkung*'), and thirdly, it is emphasized that states have positive obligations to actively protect individuals from rights violations, even in horizontal relations, meaning through other individuals.[363] This, paired with the general ambiguity and political sensitivity of the concept of security can lead to the absurd situation in which security aspects which heavily interfere with a fundamental right are masked as a fundamental right in order to be balanced against other rights. The true nature of security arguments, for example the securitization of a political interest, can easily be hidden inside an alleged fundamental rights discourse, which masks the real effect of a security measure, namely the justification of permanent changes to legal systems and power balancing mechanisms of protection.

Within the framework of the ECHR, the right to liberty and security has foremost been interpreted as the right to liberty, including safeguards against unjustified interferences.[364] The term 'security' in this context has traditionally been interpreted as relating to the strict condemnation of 'arbitrary detention'.[365] In the *Kurt* judgment, the ECtHR stated:

> What is at stake is both the protection of the physical liberty of individuals as well as their personal security in a context which, in the absence of safeguards, could result in a subversion of the rule of law and place detainees beyond the reach of the most rudimentary forms of legal protection.[366]

While article 5 is regarded primarily as addressing the deprivation of liberty, the ECtHR has been employing the security of persons in cases of disappearances, e.g. in

[363] See Tuori K, 'A European Security Constitution?' in Fichera M and Kremer J (eds), *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia 2013), 69

[364] See White R, Ovey C and Jacobs FG, *Jacobs, White and Ovey: The European Convention on Human Rights* (5th edn, Oxford University Press 2010), 209; Cameron I, *An introduction to the European Convention on Human Rights* (5th edn, Iustus 2006), 82, 83.

[365] See Macovei M, *The right to liberty and security of the person. A guide to the implementation of Article 5 of the European Convention on Human Rights* (Human rights handbooks, No. 5, Council of Europe 2002), 6.

[366] *Kurt v Turkey*, App no. 24276/94, Judgment (Court), 25.05.1998, para 123.

the *Kurt*-case cited above. Naturally so, as it is then unclear if a person's liberty or their life is at stake.[367]

It can be concluded that security in the jurisprudence of the ECHR works in fact as articulation of a protective mechanism, and as a concept that functions jointly with the right to liberty. Other scholars have confirmed the reading that security and liberty are one joint right and not distinct:

> …[T]he European Court of Human Rights has developed the concept of security in an auxiliary way, that is, the right to security of person is about *securing* liberty and has no independent content of its own. In doing so, in the context of Article 5 it has limited the context in which the security of person applies to physical liberty. It is suggested that the concept of security of person which the European Court of Human Rights develops is not a *substantive* concept with independent meaning but rather an *auxiliary* concept which attaches to *other* values or interests in order to protect or ensure them.[368]

It would therefore not be without difficulties to interpret a distinct individual 'right to security' into the ECHR. There is, however, another reason for this: Article 5 and the 'right to liberty and security of person' is not the only way in which the concept of security is used in the ECHR. Far more prominently and more widely discussed is the use of 'national security' in the Convention, namely as a legitimate aim for states to interfere with certain rights. 'National security' is listed as such a specific legitimate aim in the common limitation clauses in arts 8-11.

It is because of this reason that the construction of security as a distinct right in the Convention would be problematic: when assessing the legitimacy of interferences the ECtHR examines national security as specific aim, as a general interest, not as an individual right balanced against other individual rights.[369] Security as a distinct individual right could therefore radically change the legal reasoning of the ECtHR – and embed the obligation to protect individuals through the state (*Schutzpflicht*) directly in the test of permissible limitations on other rights. While 'national security' certainly needs to be distinguished from a right to security, such general and all-

[367] This argument is made by White R, Ovey C and Jacobs FG (n 364), 210.

[368] Powell, RL, 'The Right to Security of Person in European Court of Human Rights Jurisprudence.' (2007) 6 European Human Rights Law Review 649, 649-650.

[369] The use and meaning of 'national security' in the ECHR deserves a more thorough analysis, however, that would extend beyond the limits of this work. For a detailed discussion see: Cameron I, *National Security and the European Convention on Human Rights* (Iustus 2000).

encompassing interpretations of security run the risk of turning the concept into a carte blanche for legitimating wide-reaching interferences with fundamental rights in the ECHR.

2.4.3.2 The EU and a Right to Security

Within the EU fundamental rights framework, the EUCFR contains a right to liberty and security, in article 6, without mentioning a focus on deprivation of liberty as such.[370] Once again, taking into account common interpretations on the general right to not be deprived of one's liberty, the mentioning of 'security' in this context could have been seen merely as an addition to the primary purpose of article 6, namely to establish the 'right to freedom'. Security in a narrow sense here had to be interpreted as 'legal certainty'; and as an indication that the right to freedom shall not be arbitrarily and without proper procedure and safeguards be interfered with.

Surprisingly, however, in *Digital Rights Ireland*, the Court added an interesting, and somehow awkward side-note: After confirming that both combatting serious crime as well as international terrorism are objectives of general interest, it added: 'Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.'[371] This means that the Court read article 6 EUCFR in a new way: it seems that it now includes a right to security next to a right to liberty, although the Court did neither explicitly specify this nor clarified the relation of such a right to security with other rights in the Charter, particularly not with articles 7 and 8, the right to private life and data protection.[372]

In a more recent case, the CJEU referred to Digital Rights Ireland, when it stressed for a second time that there exists a right to security next to a right to liberty: in *J. N. v Staatssecretaris voor Veiligheid en Justitie*, the detention of the applicant, ordered for reasons of national security and public order were seen as objectives of general

[370] See Art 6 EUCFR.

[371] Cases C‑293/12 and C‑594/12 *Digital Rights Ireland*, (n 324), para 42.

[372] For a more extensive discussion of this argument, see Leuschner S, 'EuGH und Vorratsdatenspeicherung: Erfindet Europa ein neues Unionsgrundrecht auf Sicherheit?' in Schneider F, Wahl T (eds.), *Herausforderungen für das Recht der zivilen Sicherheit in Europa* (Nomos 2016), 17-46.

interest.[373] In this case, the Court repeated that '…everyone has the right not only to liberty but also to security of person (…),'[374] after which it moved on assessing the proportionality of the detention of asylum seekers. Following a more detailed analysis, it appears that there are two distinguishable concepts of security involved in the judgment. The first 'security' is the concept of protecting 'national security or public order' as a ground for the detention of asylum applicants pursuant to the Directive 2013/33/EU.[375] The second type of 'security' is an explicitly distinguished and generally construed 'right to security of person'. The pressing question in the context of the case is therefore how the general objective of protecting national security and an alleged right to security derived from article 6 of the EUCFR are related?

Unfortunately, the reasoning of the judgment does not give clear answers to this question. The Court discussed the concepts of 'public order' as entailing,

> …the existence — in addition to the disturbance of the social order which any infringement of the law involves — of a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society (...)[376]

and 'public security' as covering

> …both the internal security of a Member State and its external security and that, consequently, a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to peaceful coexistence of nations, or a risk to military interests, may affect public security (…).[377]

However, it did not return to specify the details of a special individual right to security of persons. Consequently, it can only be assumed that the CJEU here did not mitigate a right to liberty against a 'right to security of person' but that it in fact attempted to

---

[373] Case C‑601/15, *J. N. v Staatssecretaris voor Veiligheid en Justitie*, Judgment of the Court (Grand Chamber), 15 February 2016, ECLI:EU:C:2016:84, para 53.

[374] Ibid, para 53.

[375] See Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection (recast), OJ L 180/96, 29.6.2013.

[376] Case C‑601/15, *J. N. v Staatssecretaris voor Veiligheid en Justitie*, (n 373), para 65, referring to Case C‑554/13, *Zh. and Others*, Judgment of the Court (Third Chamber) of 11 June 2015, ECLI:EU:C:2015:377, para 60.

[377] Ibid, para 66, referring to Case C‑145/09, *Tsakouridis*, Judgment of the Court (Grand Chamber) of 23 November 2010, ECLI:EU:C:2010:708, paras 43, 44.

balance the individual right to liberty of the applicant against a general societal interest.

Read differently, and assuming the CJEU did indeed develop a right to security in article 6 of the Charter, this right would essentially entail two rather weird elements: Firstly, the individual right not to be disturbed by threats in one's own social order, and secondly, the individual right of the absence of threats to the functioning of institutions, essential public services and survival of the population. This obviously does not work and it is unlikely that the CJEU had the intention to develop such a right.

This shows that developing and specifying a right to security is not only problematic, but also highly dysfunctional. The right to security therefore has to be regarded as a political or theoretical argument and it comes with the similar problems of ambiguity and indeterminacy as the concept of security *per se*.

2.4.4 Conclusion

Deriving the obligation for states to protect individuals from a general right to security is highly problematic. While interferences with fundamental and human rights can very well be justified by using a security argument, turning this argument into an individual right does not make much sense, especially when considering the ambiguity of security as a concept as such. Guaranteeing security in public places by reference to an individual right to security is fundamentally flawed, simply because the exact content of such a right is of very abstract and indeterminate nature. It highly depends on the employed concept of security and there is a high risk that the core of security is determined by very specific political interests.

The Copenhagen School and critical security scholars have shown that security is not only an ambiguous but also a very problematic concept as it is prone to favour state interests over individual interests. Furthermore, it has been shown that also more human-centric conceptualizations of security run the risk of employing repressive tools for reasons of existential threats and therefore justify the use of repressive means

and methods.[378] It can be expected that legal arguments around a general right to security would have similar effects.

Both, the ECHR as well as EU case law have employed a right to security more or less carefully. Furthermore, it can be asserted that an individual 'right to security' simply does not exist within Europe. While a certain type of 'security' can, and probably should, limit certain rights in freedoms in specific ways, those limitations need to be carefully assessed.

Balancing security and freedom in public spaces is a difficult task. In order to balance those alleged two poles, however, the content and concept of security needs to be outlined. In a public context, security often actually contains a strong element of 'control' – in order to guarantee the security of public spaces, they need to be surveilled and controlled. In public places, it is therefore often not the dichotomy of security v liberty, but that of liberty v control which is at stake.[379] Only the total control of public spaces, however, guarantees total security. Taking this argument further, the only way to completely secure public places is when they lose their public character: everything happening in a public place needs to be regulated and controlled, including access and behaviour. Strong surveillance therefore tends to have a repressive character: by enabling control, in its extreme form, over the past (investigation), present (analytics), and future (prediction), surveillance has the potential to swap total control for liberty. History, however, as well as the logics of fundamental rights show that the complete elimination of liberty for the sake of security achieved by control is not only societally undesirable but also in breach of basic fundamental rights.

Before turning towards more detailed fundamental rights analyses of specific surveillance issues, the following section discusses another essential element for grasping the relation between security, surveillance and fundamental rights, and that is the importance of limitations to fundamental rights.

---

[378] See e.g. Chandler D, 'Review Essay: Human Security: The Dog That Didn't Bark' (2008) 39 Security Dialogue 427.

[379] See Schneier B, 'What our top spy doesn't get: Security and Privacy aren't opposites.' *Wired.com*, 24 January 2008 http://www.wired.com/2008/01/securitymatters-0124/ accessed 23 March 2016.

2.5 Limiting Mechanisms to Fundamental Rights

The fundamental right to privacy, as well as a possible right to the protection of one's own data, are not absolute rights. It goes without saying that such rights can be subject to limitations, provided that these limitations remain within the boundaries of the legal protection mechanisms. This applies to many fundamental rights, including privacy and data protection in the context of public area surveillance.

There are three mechanisms with particular relevance to this study: Limiting mechanisms derived from international human rights law, the permissible limitations test in the ECHR and a similar test enshrined in the EUCFR. This section describes and compares these three distinct mechanisms establishing permissible interferences with privacy and data protection in Europe.

It should be noted that there are of course mechanisms that may allow the restriction or abandonment of some human and fundamental rights, such as reservations or emergency derogations both on the European, as well as on the international level. Furthermore, legal amendments, legal change or withdrawal of Member States from human rights regimes can significantly impact fundamental rights protection. As this study primarily focuses on the fundamental rights issues of surveillance technologies in everyday-stations, those will not be discussed here.

2.5.1 Limitations of the International Human Right to Privacy and Data Protection

The right to privacy and data protection is widely recognized as an international human right. It is included either explicitly or implicitly in international, regional as well as constitutional legal sources such as article 12 of the Universal Declaration of Human Rights (UDHR), article 17 of the International Covenant on Civil and Political Rights (ICCPR), or in article 16 of the 1989 UN Convention on the Rights of the Child.[380] It might be worth mentioning in this context that universal international human rights instruments appear to express privacy as a negative right, prohibiting bearers of human rights obligations from intruding into the realm of protection without adequate justification. Particularly the wording in the UDHR and ICCPR prohibit

[380] Universal Declaration of Human Rights (UDHR) (n 255); International Covenant on Civil and Political Rights (ICCPR), (n 256); Art 16, UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, UNTS vol. 1577, 3.

'arbitrary or unlawful interference with [a person's] privacy, family, home or correspondence (…).'[381]

On the other hand, privacy appears to be articulated more as a positive right in some other regional or national constitutional human rights sources: The ECHR, for example, emphasizes a *right to respect* for private and family life, home and correspondence.[382]

The negative and positive rights distinction is an essential element for the perception of privacy protection in public places. From a US constitutional law perspective, for example, freedoms of individuals might not necessarily entail the positive obligation to protect individuals from privacy intrusions, while a European approach emphasizes positive obligations for states.[383]

Regardless of privacy being established as a more positive or more negative right, privacy is not an absolute right and can therefore be interfered with, provided interferences can be justified by following specific requirements. On the international level, the wording of article 17 of the ICCPR indicates that interferences with privacy, family, home or correspondence shall not be 'arbitrary' or 'unlawful', implying that limitations to art 17 require a legal basis or legal safeguards. It does not, however, contain expressed limitation but implies that permissible limitations need to be lawful and proportional: '[M]ost ICCPR rights may be limited by proportionate laws designed to protect a countervailing community benefit, such as public order, or to protect the conflicting right of another person.'[384] The Human Rights Committee (HRC) has made clear that authorized interferences require to be provided by national law and cannot be of an arbitrary nature:

> The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the

[381] ICCPR, Art 17. A right to privacy is articulated as a negative right also in Art 16 of the Convention of the right of the Child (n 380), Art 14 of the International Convention on the Protection of All Migrant Workers and Members of Their Families. See UN General Assembly, *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, 18 December 1990, A/RES/45/158.

[382] Art 8 ECHR.

[383] See Currie DP, 'Positive and Negative Constitutional Rights' (1986) 53 University of Chicago Law Review 864 for an early discussion on the negative focus of US constitutional rights.

[384] Joseph S and Castan M, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, (3rd edn, Oxford University Press 2013), 31.

> provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[385]

In the view of some, despite the lack of an expressed permissible limitation test in art 17 ICCPR, forbidding arbitrary interference implies an even further reaching justification mechanism. In 2009, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, published his report on the right to privacy.[386] According to the Special Rapporteur, a general interpretation of the ICCPR and the HRC General Comment No 27, which establishes an expressed limitations test for interferences with the ICCPR art 12 freedom of movement,[387] implies that a similar test applies as well to article 17.[388] In that sense, Scheinin argued that it '…codifies the position of the Human Rights Committee in the matter of permissible limitations to the rights provided under the Covenant.'[389] Consequently, a similar test could also be required in order to justify interferences with article 17 ICCPR, a test which is constructed from a common reading of limitations to several rights in the ICCPR[390] and elements contained in the HRC Comment No 27. Most of ICCPR articles containing expressed limitations include common elements: generally, restrictions require lawfulness, must be necessary in a democratic society and serve a legitimate aim. Scheinin, however, distils a more sophisticated permissible limitations test from the Comment:

> The permissible limitations test, as expressed in the general comment, includes, inter alia, the following elements:

---

[385] Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988 paras 3-4.

[386] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin (n 15).

[387] See UN Human Rights Committee (HRC), *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, 2 November 1999, CCPR/C/21/Rev.1/Add.9.

[388] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin (n 386), paras 16, 17.

[389] Ibid, para 17.

[390] Several rights enshrined in the ICCPR come with more or less expressed limitations, e.g. Article 12 (3), 18 (3), 19 (3), 21 and 22 (2) ICCPR. Art 22(2) ICCPR for example, reads: 'No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on members of the armed forces and of the police in their exercise of this right.'

(a) Any restrictions must be provided by the law (paras. 11–12);

(b) The essence of a human right is not subject to restrictions (para. 13);

(c) Restrictions must be necessary in a democratic society (para. 11);

(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);

(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);

(g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).[391]

Such a permissible limitations test, according to the Special Rapporteur's argument, would also apply to article 17, as implied by the prohibition of arbitrary and unlawful interference with the right to privacy.[392]

What follows from this is that privacy can be seen as constituting a fundamental right on the international level which is not only enshrined in binding human rights treaties, but which also comes with strict requirements in order to establish permissible limitations.

One could, of course, argue that Scheinin's construction of a detailed limitations test is not in line with a literal interpretation of the ICCPR: if the notions 'arbitrary' and 'unlawful' in the Covenant really implied all the above-mentioned elements, why did the drafters not include at least specific legitimate aims into the human rights treaty? Does not the fact that more detailed permissible limitations were included in other articles of the ICCPR indicate that a right to privacy as protected by the Covenant should explicitly not contain a strict limitation clause?

Looking at the drafting procedures in fact reveals that there had been discussions and concrete suggestions to amend article 17 with a more concrete limitation clause,

[391] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin (n 386), para 17.

[392] Ibid, para 18.

including a list of possible legitimate aims.[393] Those proposals were rejected for two reasons: some drafters felt that an explicit limitation clause would limit the scope of the article to public interferences while it was supposed to protect both against intrusions by public authorities and private actors, including organizations; and others regarded detailed limitation clauses as a collision with Member States' domestic jurisdictions and their freedom to decide on the practical application of the principles promulgated in article 17.[394] In that sense, article 17 was not drafted to establish concrete human rights with detailed limitations, but rather as a principle, leaving Member States some freedom in how they implemented it within their jurisdictions.

On the other side, of course, it is well established that a purely literal interpretation with references to the *travaux préparatoires* particularly of human rights treaties is highly problematic. Human rights treaties have to be interpreted, in line with the customary principles of treaty interpretation codified in the 1969 Vienna Convention on the Law of Treaties (VCLT),[395] considering the elements of 'good faith', 'ordinary meaning' and in light of the 'object and purpose' of the treaty.[396] Furthermore, interpretation can take into account preparatory documents as 'supplementary means of interpretation' for clarifications.[397]

Particularly, a teleological interpretation of a fundamental rights treaty in light of its object and purpose raises the question about the distinct nature of the protection of human rights through international treaties and the special nature of human rights treaty interpretation has been recognized in international law as early as in the 1950s.[398] Human rights treaties therefore require interpretations not only in light of its

[393] See Bossuyt, MJ, *Guide to the 'Travaux Préparatoires' of the International Covenant on Civil and Political Rights* (Marinus Nijhoff Publishers 1987), 339-348.

[394] Ibid, 346-347.

[395] United Nations, Vienna Convention on the Law of Treaties (VCLT), 23 May 1969, UNTS vol. 1155, 331, Arts 31-33.

[396] Art 31 (1) VCLT.

[397] Art 32 VCLT.

[398] In its 1951 Advisory Opinion on the Genocide Convention, the ICJ stated: 'In such a convention the contracting States do not have any interests of their own; they merely have, one and all, a common interest, namely, the accomplishment of those high purposes which are the *raison d'être* of the convention. Consequently, in a convention of this type one cannot speak of individual advantages or disadvantages to States, or of the maintenance of a perfect contractual balance between rights and duties. The high ideals which inspired the Convention provide, by virtue of the common will of the parties, the foundation and measure of all its provisions.' *Advisory Opinion Concerning Reservations*

original meaning, and the interests of Member States, but also in light of their nature as instruments for protecting individuals.

Regarding the interpretation of privacy and its limitations in article 17, this does allow for a more systematic and teleological interpretation. Particularly societal and technological changes, led by digitization and networking of information and communication technologies, appear to require new interpretations of article 17 ICCPR. It is also for that reason that civil rights groups as well as the former UN Special Rapporteur on human rights and counter-terrorism have argued for the urgent need of a new HRC General Comment to article 17 ICCPR, including new guidelines on permissible limitations to the right to privacy in international human rights law.[399]

In light of both technological development and the increased importance of information flows and data processing, it appears to make sense to adopt a strict permissible limitation test as described. With regards to a public surveillance scenario, limitations to a right to privacy, including personal data protection, require adequate justification already from the perspective of international human right law. This goes in line with principles and guidelines for limiting rights enshrined in the ICCPR deriving from a variety of sources and authorities[400] allowing for a conclusion that '…overarching principles of legality, necessity and proportionality…' apply when determining the legality of limitations.[401]

This means that there exists a globally (ICCPR member states) valid test establishing the permissibility of surveillance in public places containing the seven cumulative

---

to the Convention on the Prevention and Punishment of the Crime of Genocide, International Court of Justice (ICJ), 28 May 1951, ICJ Reports 1951, 15, 23.

[399] See American Civil Liberties Union (ACLU), Privacy Rights in the Digital Age. A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union, (ACLU Foundation 2014) https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf accessed 5 Mai 2016; and UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin (n 386), paras 19, 74.

[400] See UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, A/HRC/23/40, paras 28, 29; and UN Human Rights Council, The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, 30 July 2014, A/HRC/27/37, paras 21, 22; see also UN, Economic and Social Council, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, E/CN.4/1985/4, Annex (1985).

[401] UN Human Rights Council, The Right to Privacy in the Digital Age, (n 400), para 23.

elements, namely 'provided by law', 'essence', 'necessary in a democratic society' 'limited discretion', 'legitimate aims', 'proportionality' and 'consistent with other rights'.[402]

It is rather clear that restrictions to a right to privacy in public places must be based on national laws of sufficient accessibility, clarity and precision. A sophisticated camera surveillance system processing vast amounts of citizens' data, for example, can only be operated once there is adequate regulation in place. Furthermore, the surveillance system needs to be proportional regarding its functioning, the least intrusive instrument and necessary for reaching a specific legitimate aim. Additionally, the surveillance in question must be regarded as necessary in a democratic society and any discretion in applying restrictions on citizen's rights cannot be unfettered, requiring the presence of oversight and adequate remedies.

The exact meaning of what constitutes an interference 'necessary in a democratic society' in an international setting remains vague, however, guidance can be found in ECtHR case law, where the term has been interpreted excessively.[403] Generally, in order to establish a necessity in democratic societies, there needs to be a 'pressing social need' for public space surveillance as well as a discussion of how far a possible margin of appreciation –doctrine could be applied in international human rights law.[404] After all, particularly the Human Rights Committee appears to have rejected the application of the margin of appreciation doctrine on the international level.[405] Nevertheless, despite the lack of a clear application of a margin of appreciation doctrine, what is necessary in a democratic society can very well be determined with references to proportionality assessments and specific, albeit flexible, interpretations of democratic necessities in the respective countries. Both proportionality as well as that limitations must not be unfettered are, however, separate elements in the special

[402] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin (n 386), para 17.

[403] This will be discussed in the following section.

[404] See e.g. Shany Y, 'Toward a General Margin of Appreciation Doctrine in International Law?' (2005) 16 European Journal of International Law 5, 907 and Bjorge E, 'Been There, Done That: The Margin of Appreciation and International Law' (2015) 4 Cambridge Journal of International and Comparative Law 181.

[405] See McGoldrick D, 'A defence of the margin of appreciation and an argument for its application by the Human Rights Committee' (2016) 65 International & Comparative Law Quarterly 21, 23, 42-43.

rapporteur's proposed permissible limitations tests.[406] Large scale surveillance capabilities would therefore require an assessment of whether they are limited enough, proportional and correspond to a democratic necessity.

Additionally, in order for the human rights interferences to be permissible, they need to serve a specific legitimate aim or interest to which they need to be suitable and proportionate for. Restrictions through surveillance, naturally, require to be consistent with other rights in the Covenant as well.

Finally, and perhaps the most challenging element in the proposed permissible limitation test on privacy enshrined in the ICCPR is the reference to an inviolable core or an 'essence' of the fundamental right to privacy. Guidelines of an interpretation of a fundamental rights essence can be found in General Comment No. 27 stating that '…States should always be guided by the principle that the restrictions must not impair the essence of the right (…)'[407] while referring to Article 5 ICCPR, which limits limitations fundamentally contradicting the very substance of the Covenant.[408] The core of the essence formulation in international human rights law henceforth limits limitation to rights, how exactly however this could apply to an international human right to privacy remains to be interpreted.

It can be concluded that states have the obligation to respect a right to privacy in international human rights law. Interferences with the right to privacy through surveillance, data collection, and processing require compliance with the limitation principles outlined above. This requires taking into account especially legal authorization of sufficient clarity, precision and accessibility for particular

---

[406] See UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin (n 15), para 17 d) and f).

[407] UN HRC, *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, (n 387) para 13.

[408] Art 5 ICCPR states:

'1. Nothing in the present Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein or at their limitation to a greater extent than is provided for in the present Covenant.

2. There shall be no restriction upon or derogation from any of the fundamental human rights recognized or existing in any State Party to the present Covenant pursuant to law, conventions, regulations or custom on the pretext that the present Covenant does not recognize such rights or that it recognizes them to a lesser extent.'

surveillance practices, clearly defined specific legitimate aims, as well as proportionality and necessity of the operation. Furthermore, the operation cannot be unlimited in scope and time and needs adequate safeguards to counter abuse and enable remedy.[409] Additionally, legitimate surveillance operations require to take into account possible negative effects on other rights and also they cannot contradict the essential core of fundamental rights protected by the ICCPR.

While the details of an overall framework of limiting an international human right to privacy may be debatable, it appears clear that there are certain core requirements which will need to be taken seriously when surveillance and control interfere with individuals' right to privacy and data protection.

The international human rights framework protecting privacy is of course not the only one protecting –and limiting the limitations of– privacy. Both the ECHR, as well as the EU frameworks come with more detailed norms and a body of jurisprudence on permissible limitations to privacy. Both will be briefly examined in the following two sections.

2.5.2 Permissible Limitations in the ECHR

The European Convention on Human Rights and its article 8 have been protecting individual rights against state interferences ever since it entered into force in 1953 and come with an immense body of case law. Article 8 protects individual from unjustified interferences and give states a positive obligation to respect their citizens' 'private and family life', 'home' and 'correspondence'.[410]

Unlike the ICCPR, the ECHR contains a distinct limitation clause in article 8 (2), which provides for detailed guidance as to when interferences with the rights enshrined in article 8 are permissible:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-

[409] See e.g. UN Human Rights Committee (HRC), Concluding observations on the fourth periodic report of the United States of America, 23 April 2014, CCPR/C/USA/CO/4, para 22.

[410] Art 8 (1) ECHR.

being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[411]

Consequently, after determining if an issue in question falls into the scope of article 8 and constitutes an interference with a protected interest, the European Court of Human Rights (ECtHR) applies a standardized test deriving from the limitation clause as well as its case law.

In the context of this study, this means that once targeted surveillance of a person in public places falls into the scope of article 8 (1) ECHR and constitutes an interference, there are three special requirements that need to be fulfilled in order to be permissible: the surveillance action of a citizen in Helberg explicitly requires legality, a legitimate aim and a democratic necessity.

In order to perform the limitation test, the ECtHR has developed a standardized approach in its case law and it usually builds the permissible limitation test in the subsequent manner: any limitation requires legality, a legitimate aim and the previously mentioned necessity in democratic societies. This means that when the legality criterion of a measure fails, the ECtHR will find a violation without considering remaining criteria.

To comply with the first requirement, the measure needs to be in accordance with the law. This usually means that the measures have to be based on national law and that this law must be of a certain quality, and fulfil the criteria of accessibility, foreseeability, and clarity.[412]

In the *Sunday Times* judgement, the ECtHR specified accessibility and preciseness as key criteria for determining lawfulness of norms allowing for interferences: '…the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case…' and the norm needs to be '…formulated with sufficient precision to enable the citizen to regulate his conduct...'.[413] In its interpretation, however, the ECtHR also stressed that sufficient precision comes with

[411] Art 8 (2) ECHR

[412] See *Kopp v Switzerland*, App no. 23224/94, Judgment (Court), 25 March 1998, Reports 1998‑II, para 55.

[413] See *Sunday Times v The United Kingdom* (no. 1), App no. 6538/74, Judgment (Court), 26.04.1979, para 49.

an element of reasonability: A person affected by the law '…must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.'[414]

Any targeted visual surveillance in a public place – provided that this surveillance amounts to an interference - hence needs a legal basis in domestic law which must be accessible to the subject of surveillance who should be able to foresee the legal consequences of the law.[415] In addition, the domestic law should be 'compatible with the rule of law', implying

> …*inter alia*, that domestic law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention.[416]

Furthermore, the ECtHR has stressed the importance of the rule of law and independence of judicial review enshrined in legally provided review mechanisms: Especially

> …the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.[417]

Furthermore, domestic law regulating targeted surveillance in a public place needs to ensure certain safeguards against abuse and against uncontrolled powers in the hands of the authorities.[418]

This has been stressed in cases where the ECtHR examined laws authorizing secret surveillance measures: particularly because it is against the nature of secret surveillance measures to be subject to immediate scrutiny by affected individuals and

---

[414] Ibid, para 49.

[415] See *Kopp v Switzerland*, (n 412), para 55.

[416] *Fernández Martínez v Spain*, App no. 56030/07, Judgment (Grand Chamber), 12.06.2014, para 117.

[417] *Roman Zakharov v Russia*, App no. 47143/06, Judgment (Grand Chamber), 04.12.2015, para 233.

[418] See e.g. *Malone v The United Kingdom*, App no. 8691/79, Judgment (Court) 02.08.1984, paras 66‑68 and *C.G. and Others v Bulgaria*, App no. 1365/07, Judgment (Court) 24.04.2008, para 39, and *Rotaru v Romania*, App no. 28341/95, Judgment (Grand Chamber), 04.05.2000, para 59.

it would not be compatible with the rule of law to grant unfettered powers to the authorities.[419] Therefore, specific minimum safeguards that need to be laid down in the national laws include *inter alia* the nature of offences that warrant surveillance, specification of categories of people or groups potentially subject to surveillance, duration limitation, data processing procedures, data transfer precautions, and deletion of surveillance data.[420] While many of those requirements derive from wiretapping cases, laws authorizing targeted sophisticated surveillance in the public space require similar criteria. The main question arising from this is in how those requirements could work with the complex surveillance systems described in the scenario; after all such surveillance systems can be operated as very effective targeted surveillance systems for tracking and surveilling suspects in a vast area, depending on the design and prevalence of video cameras and other location sensors. This is problematic, because on the one hand the system is a public mass surveillance system, which on the other hand has the capability to be employed as a targeted surveillance system if necessary. While the ECtHR has explicitly found that simple camera surveillance systems installed in public spaces do not require a legal basis since they do not constitute an interference with rights protected in the ECHR,[421] it has on the other hand developed very detailed requirements for the lawfulness of targeted secret surveillance measures, including wiretapping. In order to be used as a targeted surveillance system, there needs to be a law specifically authorizing the employment of sophisticated public surveillance systems with both mass- and targeted surveillance capabilities.

The second criteria for determining the permissibility of an interference into the rights enshrined in article 8 ECHR is that the measures in question require specific legitimate aims.

Art 8(2) ECHR provides an exhaustive list of such aims:

[419] See *Weber and Saravia v Germany*, App no. 54934/00, Decision (Court), 29.06.2006, para 94.

[420] Ibid, para 95; See also *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, App. No 62540/00, Judgment (Court), 28.06.2007, para 76; *Roman Zakharov v Russia*, (n 417) para 231.

[421] *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, App no. 32200/96, Inadmissibility Decision (Commission), 14.01.1998, 97.

> …interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[422]

It is important to note that those interests will not justify an interference *per se*, but need to be suitable and proportionate in order to reach the particular aim.

Sophisticated surveillance of urban public spaces serves certain aims of security. Naturally, targeted surveillance of individuals in a public context most likely will have either a security or a law enforcement context. While surveillance of public places in general could serve abstract aims of upholding a certain concept of public safety, in the context of targeted surveillance however, national security or crime prevention might be more likely to be relevant.

As discussed earlier, 'national security' is a difficult concept as such but targeted surveillance might very well serve such aim if the person under surveillance is involved in activities labelled as terrorism. In the *Klass* case, the ECtHR accepted that a law granting surveillance powers to German state authorities was serving the legitimate aims of 'national security' and the 'prevention of disorder or crime'.[423] Therewith the ECtHR confirmed the authorizing law's purpose to protect

> …against "imminent dangers" threatening "the free democratic constitutional order", "the existence or security of the Federation or of a Land", "the security of the (allied) armed forces" stationed on the territory of the Republic or the security of "the troops of one of the Three Powers stationed in the Land of Berlin"…[424]

as constituting the legitimate aims of safeguarding 'national security' and 'to prevent disorder or crime'.[425]

In the *Uzun* case, the ECtHR confirmed that both visual surveillance as well as GPS tracking of a person served the '…interests of national security and public safety, the prevention of crime and the protection of the rights of the victims'[426] because the suspect was investigated for attempted murder, the case had a terrorist background

[422] Art 8 (2) ECHR.

[423] *Klass and Others v Germany*, App no. 5029/71, Judgment (Court), 06.09.1978, para 46.

[424] Ibid, para 45.

[425] Ibid, para 46.

[426] *Uzun v Germany,* App no. 35623/05, Judgment (Court), 02.09.2010, para 77.

and because the authorities attempted to prevent future bomb attacks.[427] Hence, the acceptance of national security as a legitimate aim for systematic targeted visual surveillance of an individual's action in a public area depends on the detailed circumstances and the reasons for the surveillance of the individual.

Another likely aim for targeted public visual surveillance is 'prevention of disorder or crime'. Targeted visual surveillance is naturally very often of an investigative nature or perceived as a penal measure which is why the prevention of disorder or crime is one of the most often accepted aims by the ECtHR.[428]

Other legitimate aims, such as the economic wellbeing of the country, health or morals, or the protection of the rights and freedoms of others may play a more marginal role in targeted surveillance cases.

The third element included in the legitimacy test in art 8(2) ECHR states that apart from being in accordance with the law and serve a legitimate aim is that the interference has to be 'necessary in a democratic society' in order to be legitimate. This means that targeted visual surveillance as a restriction into individual rights needs to be 'proportionate to the legitimate aim pursued' and 'correspond to a "pressing social need"'.[429] In addition, states have a 'certain but not unlimited margin of appreciation'[430] in deciding applying restrictions, however, that process will be under the review of the ECtHR.[431] In the *Handyside* Case, the ECtHR stated that principally national judges are '…in a better position than the international judge to give an opinion on the exact content of the requirements as well as in the "necessity" of a "restriction" or "penalty" intended to meet them.'[432] There is an excessive body of case law and debates on the application of such legal arguments and the ECtHR has

[427] Ibid.

[428] See White R, Ovey C and Jacobs FG (n 364), 320.

[429] See *Silver and Others v The United Kingdom*, Apps no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Judgment (Court), 25.03.1983 para 97.

[430] Ibid.

[431] Ibid, see also *Handyside v The United Kingdom*, App no. 5493/72, Judgment (Court), 07.12.1976, para 26.

[432] Ibid, para 48.

applied the argument differently, some say indeterminately and in a manner that is difficult to predict.[433]

So, what could this concept mean in the context of targeted visual surveillance? On the one hand, the proportionality test is of a certain importance. Is the measure interfering with an individual's right proportionate to the pursued aim? If the targeted measure affects a suspected drug dealer, is limited in time, and targeted towards a criminal investigation and evidence gathering, the Court might find that the measure was proportionate or that the state possessed a wide margin of appreciation on the issue. If the police use the surveillance system in order to follow and monitor the action of e.g. the political opposition for years, the ECtHR might decide differently.

In cases involving terrorism, public threats and national security, the ECtHR seems to have favoured a wider margin of appreciation, such as for example in the *Leander* case, where the ECtHR granted a wide margin to the respondent state to collect and retain secret databases in order to assess if a person is suitable to be employed in security sensitive areas.[434] Also in the *Klass* judgment, when assessing the existence of a secret system of surveillance, the ECtHR granted a wide –although not unlimited- margin of appreciation to the authorities.[435] Taking into account both the technological improvements of surveillance capabilities and development of terrorism in Europe, the Court found that:

> Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.[436]

[433] See, White R, Ovey C and Jacobs FG (n 364), 326. For a more detailed discussion see Cameron I, *National security and the European Convention on human rights* (Iustus 2000), 27-36.

[434] See *Leander v Sweden*, App no. 9248/81, Judgment (Court) 26.03.1987, para 59.

[435] *Klass and Others v Germany*, (n 423), para 49.

[436] Ibid, para 48.

Another important factor in deciding if targeted surveillance is 'necessary in a democratic society' is the ECtHR's conception of democracy. Despite granting a wide margin in the *Klass* case, the ECtHR also explicitly noted that:

> …this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.[437]

The ECtHR hence explicitly recognizes surveillance as a threat to democratic societies that need to be carefully balanced and assessed – making it necessary to take into account the ECtHR understanding of a democratic society in the individual cases.[438]

It can be concluded that for targeted visual surveillance and monitoring of an individual to be in line with the legitimacy criteria of being 'necessary in a democratic society', the overall situation, implementation, design and authority's application of balancing exercises will need to be reviewed by the ECtHR. It appears, though, that the more targeted, limited and reviewed such a surveillance procedure is designed to be, the more likely it will be deemed legitimate.

2.5.3 Permissible Limitations in the EUCFR

After discussing possible systems of permissible limitations both in international as well as European (Council of Europe) human rights mechanisms, what remains is to take a brief look at limitations enshrined in EU fundamental rights and therewith in article 52 of the EU Charter of Fundamental Rights. The EU Charter lays down two distinct articles on the protection of privacy and data protection (arts 7 and 8), however, unlike the ECHR with its similar limitation clauses in arts 8-11, most of the EUCFR articles do not contain explicit limiting elements. Instead, title VII of the

[437] Ibid, para 49.

[438] The ECtHR has discussed its views on democratic societies in a case concerning the dissolution of a political party in Turkey, see *Refah Partisi (the Welfare Party) and Others v Turkey*, App nos. 41340/98, 41342/98, 41343/98 and 41344/98, Judgment (Grand Chamber), 13.02.2003, paras 86-104.

Charter provides a separate article containing a general provision for the justification of interferences with the rights protected therein[439].

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[440]

The wording of this provision is explicitly based on established CJEU case law on limiting EU fundamental rights which in turn references the ECHR and its limiting mechanisms.[441]

Additionally, article 52 (3) provides that the EUCFR requires at least an equal level of protection when it comes to scope an interpretation of rights enshrined in the ECHR. With this, limiting elements in the ECHR become part of a EUCFR assessment, if not a distinct requirement in the EUCFR permissible limitations test.[442]

The content of the article 52(1) permissible limitation test is therefore similar to the mechanism in the ECHR. Any limitation to the rights protected requires to be 'provided by law', and it must have a legitimate aim that corresponds to genuine Union interests and/or rights and freedoms of others. Furthermore, limitations must be necessary for reaching that aim and they must generally be proportionate. In addition, article 52(1) EUCFR contains a requirement that a limitation must '…respect the essence of (…) rights and freedoms', an element which is not as such contained in the wording of the ECHR limitation clauses.

The applicability of the permissible limitation need to be, of course, approached with care, especially with regards to the problem of their scope. Foremost, the Charter

---

[439] Absolute rights, of course, cannot be subject to limitations provided by Art 52 (1) EUCFR. See Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375, 388.

[440] Art 52 (1) EUCFR.

[441] See Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, 17–35. See also Case C-5/88 *Wachauf,* Judgment (Third Chamber), 13 July 1989, ECLI:EU:C:1989:321, para 18*;* Case C-292/97, *Kjell Karlsson and Others***,** Judgment (Sixth Chamber), 13 April 2000, ECLI:EU:C:2000:202, para 45.

[442] See e.g. Ojanen T, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' (2016) 12 European Constitutional Law Review 318, 324-325.

applies primarily to the area of Union law, and therewith to issues with direct EU law relevance. Article 6(1) TEU in particular, while lifting the Charter of Fundamental Rights onto the level of the EU Treaties, at the same time states that '…the Charter shall not extend in any way the competences of the Union as defined in the Treaties.'[443] In accordance with the principles of conferral and subsidiarity, article 51 (1) and (1) EUCFR only apply when the EU Member States implement EU law and should not establish new powers of tasks.[444] This means that a permissible limitations test on an interference with a right guaranteed in the Charter is only required in case the issues at stake falls into the scope of the application and implementation of Union law and therewith imposes obligations on Member States.[445] In addition to the problem of applicability and scope, it is remarkable that the CJEU does not consistently refer to the permissible limitation test in article 52(1) EUCFR when assessing permissible limitation to Charter Rights.[446]

In case the issue at stake falls under the scope of Union law and constitutes an interference into rights protected by the Charter, the potential interference must be provided for by law. There is extensive jurisprudence on the interpretation and details of this requirement in ECHR case law, and it is clear that similar criteria apply also in the case of the EUCFR. It is important to note, though, that legal provisions qualifying for the legality criteria in an EU-context self-evidently include EU legislative acts.[447] Once, however, an issue falls within the scope of Union law, it is most likely that there exists an EU legislative act which requires compliance with the legality criteria.

---

[443] See Art 6(1) Consolidated version of the Treaty on the Functioning of the European Union (TFEU), OJ C 326, 26.10.2012, 47–390.

[444] See Article 51(1+2) EUCFR, see also Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375, 377-378.

[445] For a more detailed discussion see ibid, 376-382.

[446] Some scholars therefore call for more consistent application of a permissible limitation test in CJEU jurisprudence. See e.g. Peers S and Prechal S, 'Article 52 – Scope and Interpretation of Rights and Principles' in Peers S and others (eds), *The EU Charter of fundamental rights: A Commentary* (Hart 2014) 1455-1522, 1485.

[447] Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375, 390, 391. For a more details and references to the general discussion on limiting EC and EU rights and freedoms, see Peers S, 'Taking Rights Away? Derogations and Limitations.' in Peers S and Ward A (eds), *The European Union Charter of Fundamental Rights* (Hart 2004), 149-152; and more recently, Peers S and Prechal S, Article 52 – Scope and Interpretation of Rights and Principles, in Peers S and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart 2014), 1468 – 1521.

The next step in the EUCFR's permissible limitation test is the provision for the existence of a legitimate aim and the proportionality of the measure to reach that aim. While the ECHR and the common limitation clauses in arts 8-11 provide for an exhaustive list of specific aims, the Charter remains silent. Article 52(2) EUCFR merely names two distinct categories: firstly, 'objectives of general interest recognised by the Union' and secondly, 'the need to protect the rights and freedoms of others'. In fact, the objectives of general interest appear to be interpreted rather widely in CJEU case law: Lenaerts, for example, distils a list of aims such as for example 'establishment of a common organisation of the market', 'protection of public health', 'public security', 'international security' and 'transparency'.[448] This indicates that legitimate aims for restricting Charter rights go further than the enumerated list of legitimate aims in the ECHR.

Secondly, article 52(1) EUCFR additionally mentions the protection of 'rights and freedoms of others' as an aim for permissible limitations, which in its application, requires a balancing test between the rights limited and the rights and freedoms of others affected by the possible non-limitation. It goes without saying, that all legitimate aims are part of a necessity and a proportionality test.

The remaining criterion for the application of a permissible limitations test in light of article 52(1) of the EUCFR is that any limitation must respect 'the essence' of rights and freedoms protected in the Charter. The formulation the EUCFR's limitation clause is interesting for two reasons. Firstly, the formulation to respect the 'essence' of rights and freedoms is somehow unique in its directness in limitation clauses in international human rights law. It is not explicitly mentioned in the ICCPR, neither in the ECHR, although, as discussed above, it is mentioned in HRC General Comments No 27 as '…States should always be guided by the principle that the restrictions must not impair the essence of the right (…)'[449], and an essence argument has been put forward in some ECtHR cases.[450]

---

[448] Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375, 391-392.

[449] UN HRC, *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, (n 387), para 13.

[450] See *Christine Goodwin v the United Kingdom*, App no. 28957/95, Judgment (Grand Chamber), 11.07.2002, para 97, where the Grand Chamber stated that national regulation of the right to marry cannot amount '…to such an extent that the very essence of the right was impaired.' Or recently in *Baka v Hungary*, App no**.** 20261/12, Judgment (Grand Chamber), 23.06.2016, para 120, which stated

Secondly, it is fascinating because it points to an interpretative approach of human rights limitations which could be described as a 'categorical determination'[451] to the application and interpretation of human rights, opposing a general pull towards a balancing test.[452]

Balancing when assessing the justifiability of restriction and limitations with rights is an ever-present court practice, particularly in the context of security relevant cases and especially when employing proportionality-based tests. Indeed, the balancing of rights against rights, of rights against interests and of interest against interest has been debated extensively in legal theories.

While for some, such balancing is fundamentally based on political power decisions,[453] for others balancing is a matter of the complex quantifiably of conflicting individual and communal interests.[454] It is important to note, though, that judicial balancing, particularly when it concerns an alleged conflict between (individual) liberty and (collective) security, has another dimension, and that is one of comparability.

One of the core assumptions in favour of judicial balancing is that of the possibility of quantifiably of the two conflicting interests or social goods. At the same time, the criticism of judicial balancing is based on pointing out the arbitrariness, and the social and political dimensions of weighting those interests. What is missing from such criticism, however, is that often the alleged balancing involves comparing apples to oranges: that is because collective social goods or collective interests appear to be

---

that '…the right of access to the courts is not absolute and may be subject to limitations that do not restrict or reduce the access left to the individual in such a way or to such an extent that the very essence of the right is impaired.'

[451] See Rosenfeld, M., 'Judicial Balancing in Times of Stress: Comparing the American, British and Israeli Approaches to the War on Terror' (2006) 27 Cardozo Law Review 2079, 2094-2095.

[452] See also Scheinin M, 'Terrorism and the Pull of 'Balancing' in the Name of Security' in Scheinin M and others (eds) *Law and Security - Facing the Dilemmas*, (EUI Working Papers, LAW 2009/11, 2009) 55-63, 56.

[453] See Petman J, 'Egoism or altruism? The politics of the great balancing act' (2008) 5 No Foundations Journal of Extreme Legal Positivism 113

[454] For further discussion, see Waldron J, 'Security and Liberty: The Image of Balance' (2003)11 Journal of Political Philosophy 191.

compared and balanced against constitutionally or internationally protected human rights.[455]

In that regard, specific 'interests', when enshrined as fundamental rights may have to be taken out of the equation of balancing: because they either are inviolable, such as for example the absolute prohibition of torture or the prohibition of slavery, or because they contain a core, an inviolable substance, an 'essence' which cannot be subject to limitations and balancing. In that sense, this is what makes the EUCFR art 52(1) limitation clause so remarkable: it establishes the existence of an 'essence' of fundamental rights, which cannot be limited.

Such a reading of the Charter reminds of Robert Alexy's distinction between rules and principles.[456] Scheinin argued, that Alexy's distinction leads to the conclusion that '…most, if not all, human rights include an inviolable core with the character of a rule, surrounded by a much broader principle that is valid at the level of the legal order as a whole.'[457] In Scheinin's interpretation of Alexy, it is this strict rule which forms the core of a right, whereas the surrounding broader principle is the one that can be weighted and balanced.[458] Limitation tests therefore can only be conducted on principles, whereas the core or essence of rights form a rule that either applies categorically or does not. What matters in the application of a rule is the scope, not the balancing. But does the reference to 'essence' in the EUCFR really favour an Alexyan perspective in assessing permissible limitation to rights enshrined in the Charter?

Indeed, this argument can be made. Already in the 1970s, the European Court of Justice took the stance that rights in the Community should only be limited provided that their very substance remains untouched.[459] Today the EUCFR therefore appears

---

[455] This is certainly the case when it comes to balancing in the context of security: see Rosenfeld, M., 'Judicial Balancing in Times of Stress: Comparing the American, British and Israeli Approaches to the War on Terror', (2006) 27 Cardozo Law Review 2079, 2089-2090.

[456] See Alexy R, *Theorie der Grundrechte* (Nomos Verlagsgesellschaft 1985).

[457] Scheinin M, 'Terrorism and the Pull of 'Balancing' in the Name of Security' in Scheinin M and others (eds) *Law and Security - Facing the Dilemmas*, (EUI Working Papers, LAW 2009/11, 2009) 55-63, 56.

[458] Ibid, 55.

[459] See Case C-4/73, *Nold v Commission*, Judgment of the Court, 14 May 1974, ECLI:EU:C:1974:51 para. 14. In this connection, it is worth mentioning that for example the German Constitution contains

to contain limitation criteria based on an essence argument: fundamental rights in the Charter can therefore not be subject to limitations when the limitation touches upon the very essence and therewith the core of a right.

Interestingly, two recent cases concerning privacy and data protection, strengthen this reading: In *Digital Rights Ireland*, the CJEU discussed limitations to articles 7 and 8 of the EUCFR in light of the 2006/24/EC Data Retention Directive.[460] While applying the art 52(1) limitation test of the Charter, the Court held that because the Data Retention Directive did not allow for the collection of communication content, and because it, in the view of the Court, respected certain data protection safeguards, neither the essence of the right to privacy in article 7, nor the essence of data protection in article 8 EUCFR were impeded.[461]

In the *Schrems* judgment, however, the Court regarded general access to the content of communications as well a lack of safeguards and recourse as impeding the very essence of privacy and data protection rights guaranteed by the EUCFR.[462] The Court reasoned:

> …legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (…).[463]

Furthermore,

> …legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[464]

This means that the extend of possible content surveillance paired with a lack of recourse was reason enough for the Court to find an unjustifiable intrusion into the

---

a provision protecting the essence of right to be limited by national laws (so called 'Wesensgehaltsgarantie') in Art 19(2).

[460] Cases C‑293/12 and C‑594/12 *Digital Rights Ireland*, (n 324).

[461] Ibid, paras 39, 40.

[462] Case C-362/14 *Schrems*, (n 325).

[463] Ibid, para 94

[464] Ibid, para 95.

core of the rights (privacy and judicial remedy) protected by the Charter. The *Schrems* judgment can therefore been interpreted as a more recent turn to take privacy as a right seriously and for clarifying the understanding of the role of rights-essences in limiting fundamental rights in Europe.[465] In light of these findings, essence arguments may grow in importance, particularly in upcoming cases on the limits of privacy and data protection in Europe.[466]

One further issue deserves to be mentioned in the context of limitations to the rights enshrined in the Charter concerning the separation of privacy rights and data protection in the Charter. While there are is no specific limitation clause in the right to respect for private life, home and communications, the right to the protection of personal data comes with more specific provisions. In that sense, article 8(1) EUCFR articulates the right as: '1. Everyone has the right to the protection of personal data concerning him or her.'

Article 8(2) and (3) EUCFR then continue:

> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Following the logic of article 52 EUCFR, it should be clear that this permissible limitation test applies as well to the right to personal data protection. Article 8, however, has a somehow unique standing in the rights of the Charter.

Firstly, the EUCFR contains therewith a right to personal data protection formulated separately, next to the right to privacy enshrined in article 7. This means that when considering limitations, article 8 does not have a direct correspondence with the ECHR, which leaves a question mark behind the comparability of the meaning and scope of data protection deriving from article 8 ECHR and the protection of personal

[465] See Ojanen T, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' (2016) 12 European Constitutional Law Review 318, 327-329

[466] For further discussion see ibid, and Ojanen T, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others' 10 European Constitutional Law Review 528.

data in the EUCFR.[467] Although it is highly unlikely that a fundamental right to data protection would be narrower in scope than the protection in the ECHR, the application of article 52(3) EUCFR to limitations regarding data protection rights might be debatable.

Article 8 EUCFR, however, has to be regarded as a product of existing data protection sources such as the 1981 Council of Europe Data Protection Convention and the 95/46/EC Directive, as well as Art 8 ECHR jurisprudence.[468] Interestingly, though, here the Data Protection Directive (now replaced by the new General Data Protection Regulation (GDPR)[469], as well as the Regulation on data processing by Community Institutions (EC) No 45/2001 [470] are explicitly mentioned as setting limitation conditions for the right to data protection.[471] This means that the limiting conditions for the right to data protection are being additionally constituted through *lex specialis* provisions in the form of EU legislation.

Secondly, another reason for its separate standing is that article 8 EUCFR itself contains specific conditions in article 8 (2) and (3) EUCFR, which could be read as intrinsic limitations. Article 8(1) could therefore be read as establishing a right to data protection as a general ban on the processing of data. Paragraph 2 and 3 would then lay out the permissible limitations to the general ban of personal data processing, namely that such processing is only justified when data is processed fairly, for a specified purpose, with consent or otherwise lawfully and that a permissible limitation would include individual access rights as well as the possibility for rectification. González-Fuster and Gutwirth call this reading, which is similar to the binary structure of article 8 ECHR, a 'prohibitive' approach.[472] In that sense, para 1 of article 8 EUCFR

[467] See also Explanation on Article 52 in Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, 17–35, which does not mention Article 8 and its scope in relation to the ECHR.

[468] Ibid, Section: 'Explanation on Article 8 — Protection of personal data'.

[469] Regulation (EU) 2016/679, (GDPR), (n 303).

[470] Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, 1–22.

[471] See Section 'Explanation on Article 8' in Explanations relating to the Charter of Fundamental Rights OJ C 303, 14.12.2007, 17–35.

[472] González Fuster G and Gutwirth S, 'Opening up personal data protection: A conceptual controversy' (2013) 29 Computer Law & Security Review 531, 532.

would establish the general rule, whereas paras 2 and 3 would establish the conditions for limitations.

Another possible reading of article 8 EUCFR, according to González-Fuster and Gutwirth, could be a 'permissive' conception,[473] in which the right to the protection of personal data does not entail a general prohibition of personal data processing, but the right to have personal data processing safeguarded and conditioned upon the substantive criteria laid out in article 8 (2+3) EUCFR. Article 52 EUCFR would then further establish permissible limitations for interferences into the core conditions of data processing, rather than the justification of interference with a ban on data processing *per se*.[474]

This is an important distinction, because the reading of limitations to data protection either as a prohibitive or permissive conception can determine the standing of personal data protection as a right next to privacy. A general prohibition of personal data processing comes with the necessity to justify any processing in light of the mechanism available, while a permissive approach grants a right, not to not have one's data processed, but to have adequate safeguards and protection mechanisms in place.

As a consequence, the fundamental core (the essence) of a fundamental right to data protection would be significantly different in each case: in the former prohibitive approach, data protection has its own standing as a right next to privacy, while in the permissive approach, the core of data protection lies in the protection of individuals from harm through unsafeguarded data processing. From a permissive perspective, the individual protection needs to rely on the definition of a potential harm as such, and this definition need to derive from the concept of privacy. From a permissive perspective, data protection cannot develop an independent protective effect, without reference to the fundamental right to privacy.

Be it as it may, it becomes clear that permissible limitations of a right to personal data protection in the EUCFR consists of several layers which need to be taken into account: Firstly, EU legislative instruments e.g. nowadays the GDPR as well as the

[473] Ibid, 533.

[474] Ibid, for further discussion.

'Police'-Directive[475] may be read as setting legitimate conditions for limitations. Secondly, article 8 (2) and (3) contain conditions or principles that play a role, and thirdly, the EUCFR contains its separate mechanisms for the conditions for limitations, including a reference to the inviolability of the essence of the fundamental rights.

***

This section discussed systems for permissible limitations of privacy and data protection in international and European human rights law. Providing that certain aspects of surveillance in the scenario above fall into the scope of those rights and constitute an interference, such interferences are required to pass all applicable limitations test in order to not constitute human and fundamental rights violations. Naturally, this will have to be assessed on a case-by-case bases.

This study will now move towards a more scenario based analyses of specific issues that arise in connection with public surveillance and data collection.

[475] Directive (EU) 2016/680 (n 303).

3. European Fundamental Rights and Public Surveillance

At the core of this study lies a discussion addressing the regulation of surveillance and complex surveillance technologies in the context of urban public space surveillance. Part one of this study therefore discussed various aspects of the problem of the application of privacy in public. Part one especially focused on the foundations of fundamental rights analyses of the rights of privacy and data protection and the various problems of the concept of security. While it concludes that both the right to privacy, and a right to data protection are intertwined fundamental rights, security functions differently, namely as a limiting mechanism. Part one of this study also showed that there are a variety of limiting mechanisms to individual rights when applied in the European public space, deriving from the international human rights framework as well as both the CoE and the EU rights protection systems.

What is essential for a discussion of the function of fundamental rights in addressing surveillance in public places, however, are the theoretical underpinnings behind such rights. When privacy is conceptualized employing individual freedom, the articulation of the substance of such a right is fundamentally different then when it is deriving from dignity and personality. One of the reasons is that dignity appears to allow a broader focus on societal and communal understandings of privacy, which appears as a surprise, considering the rather liberal theoretical background of the concept of human dignity. In that sense, the first part attempted to show the importance of a differentiation between different understandings of privacy and their effects on rights application in public places.

The second part of this study will now turn towards a more concrete analysis of European case law in connection with the surveillance scenario described in the introduction. The analysis will mainly focus on the scope of application of privacy and data protection in the context of the scenario, simply because a further detailed discussion of permissible limitations would go beyond the limits of this study.

The analyses of the scenario furthermore limit themselves to four distinct issues of particular relevance and interest. Firstly, this study analyses targeted public surveillance. This is important because it is probably the most common surveillance scenario: a person in a public space is for one or the other reason a subject of surveillance targeting specifically her or him. The second issue analysed with

reference to the surveillance scenario of Helberg, is mass surveillance. This describes the indiscriminate surveillance of everybody within the reach of the respective surveillance system. Of course, one of the crucial issues of this is that both targeted and mass surveillance questions depend on the sophistication and capabilities of the surveillance technologies employed. The core in both analyses will therefore be based on understanding the function of surveillance technologies described at the outset of this study, especially when it comes to visual analytics and prediction. For this reason, a third issue analysed in this context is a brief discussion of future surveillance capabilities and their legal consequences: the issue of complex analytic and incident prediction. Before turning to the future, however, this study discusses privacy in public places in light of a further distinction of the private and public spheres: namely the relevance of private and public actors in modern urban surveillance scenarios.

3.1 Targeted Public Surveillance

As a first concrete legal assessment of the surveillance scenario, this study analyses targeted surveillance in a public space. Targeted surveillance in the context of this work means that a surveillance operation targets one or a group of suspects in order to gather information or evidence about them. This comes closest to a 'conventional' surveillance operation, where an individual is subject to surveillance for specific reasons. An array of technical means and personnel on the ground might accompany such surveillance. Targeted surveillance in the context of the urban surveillance scenario means that observers have the option to target an individual by different means, for example by tailing and observing a suspect, but also by targeting someone with surveillance technologies such as video cameras or movement trackers.

For this purpose, existing public surveillance systems can be used in aiding targeted observations. For example, video surveillance systems can monitor a single person and video content analyses (VCA) or biometric identifications systems can be used to pick out the target person from a crowd. The more sophisticated the system, the less extra means will be necessary to conduct a surveillance operation on the ground.

There are several components and capabilities of targeted surveillance that have special relevance for a legal assessment of the scenario:

A public surveillance system can be used to identify and locate a target. The moment the police in the Helberg scenario becomes aware that person A might be involved in the selling of drugs, police officers could obtain biometric data of A (image, facial profile, movement profile etc.) in order to feed them into the computer programs of the surveillance system. Once A is picked out by the system, the police know the exact whereabouts of A and can monitor her further actions and movements.

Of course, when the surveillance system is capable of VCA, behavioural analyses, or incident prediction, the software might be able to automatically single out and identify actual suspects form a group of people, leading to a further targeted surveillance operation.

Targeted surveillance of an individual hence includes the following components: Firstly, the person's location will be tracked. Location data might as well be retained and processed in order to establish connections at a later stage as well as for forensics and legal proceedings. Secondly, the individual's actions can be visually monitored. Thirdly, targeted surveillance also monitors social interactions and communications, up to the point where targeted sound sensors might record all the communications of the individual. Fourthly, in order to function, systems need to process and possibly retain significant amounts of personal data.

The following analyses will assess, whether and how a fundamental right to privacy addresses and affects targeted surveillance in the European public space.

3.1.1 The Scope of a Right to Privacy in Public

Many of the above-described components of target surveillance in public spaces might interfere with the right to private life enshrined in article 17 ICCPR, art 8 ECHR and art 7 EUCFR. Furthermore, as personal data is an essential component of the described surveillance, the right to the protection of personal data in art 8 EUCFR needs to be taken into consideration as well. As location data is used, targeted public surveillance might as well fall into the scope of the right to liberty of movement, enshrined in art 12 ICCPR, art 2 Protocol 4 to ECHR and art 45 EUCFR. Furthermore, targeted surveillance in public might also touch on certain aspects of right to freedom of opinion and expression guaranteed under art 19 ICCPR, art 10 ECHR and art 11

EUCFR as well as right to assembly of art 21 ICCPR, art 12 ECHR and art 12 EUCFR.[476]

From a fundamental rights perspective there are hence a variety of rights affected when individuals are subject to surveillance in public places. The scope of a right to privacy is one core issue when legally assessing targeted surveillance in public. The following sections therefore examine some key aspects of targeted surveillance, particularly targeted public surveillance and personal data processing. The following analyses will also employ the dichotomy of privacy conceptions between a liberal approach and a dignity/personality- based approach in targeted surveillance cases in the ECtHR.

Foremost, modern sophisticated surveillance systems in the scenario are heavily based on video surveillance. Visual surveillance alone can be used for a variety of purposes such as object surveillance and monitoring of a person's activities, their location as well as their behaviour. With the help of analytics technologies and data processing the capabilities of surveillance can be extended dramatically: facial recognition, automated tracking or behavioural analytics, just to name a few, are capabilities that have not much in common with a closed system allowing an observer to technically extend her views. This raises the question if visual surveillance in public places in Helberg creates fundamental rights issues.

It is often stated that video cameras in public places would not fall into the scope of protection of private life in the ECHR, because of their low level of intrusion, and due to the fact that an individual in public is in principle also publicly visible and therefore enjoys a lesser expectation and degree of privacy.[477] This view will be analysed in more detail in the next sections.

The ECtHR's case law on images in public spaces started rather early. Already in 1973, the Commission addressed an application concerning the taking of photographs

[476] This study limits itself to privacy and data protection and will not discuss further other affected rights. For a discussion on the relationship between freedom of expression and opinion and surveillance see e.g. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, 17 April 2013. For a sociological analysis of surveillance and the right to assembly see Starr A and others, 'The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis' (2008) 31 Qualitative Sociology 251.

[477] *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421), 94.

during a political demonstration: The applicant took part in an anti-apartheid demonstration during which she was restrained by the police, photographed against her will and asked for her identity. The applicant also claimed that the police created a file containing her picture in order to 'deter [her] from participating in similar demonstrations again'.[478] The Commission found that this could not be viewed as an interference with her private life, because a) her home was not entered for the purpose of taking photographs, b) she voluntarily took part in a public event, and c) because the photographs '…were taken solely for the purpose of her future identification on similar public occasions and there is no suggestion that they have been made available to the general public or used for any other purpose.'[479]

Similar findings were made in another case concerning the use of photographs for identification purposes in criminal investigations against people allegedly involved in squatting. The fact that the police used photographs from the applicant's driving license application and from pictures taken during previous arrests for the investigation did not amount to an interference of art 8.[480] The Commission emphasized that the way in which the photos were taken was not intrusive and that the photographs were kept in police archives, only used for the criminal investigation, and not disseminated.[481]

In 1995 when the Commission adopted its report in the *Friedl* Case, it elaborated but upheld its previous argumentation regarding the intrusiveness of images taken in public places. The case concerned political protests organized by a working group at Vienna University as a weeklong 'sit in' in an underground pedestrian passage in order to raise awareness about problems of homeless persons.[482] Due to obstruction of pedestrian traffic and security concerns, the manifestation was dissolved by the police and the participants were ordered to leave the passage. During this sit-in, police authorities took pictures and videos of the manifestation, in order '…to record the

[478] *X. v the United Kingdom*, App no. 5877/72, Decision (Commission) 12.10.1973, applicant's submission, para 1.

[479] Ibid, Commission's examination, para 2.

[480] *Lupker and Others v the Netherlands*, App no. 18395/91, Decision (Commission), 07.12.1992, Commission's findings, para 5.

[481] Ibid.

[482] *Friedl v Austria*, App no. 15225/89, Report (Commission) 19.05.1994, para 15.

conduct of the participants in the manifestation for the purposes of ensuing investigation proceedings for offences against the Road Traffic Regulations.'[483] The applicant in the case complained about the taking of images and the recording of his personal data by the police.[484]

While the Commission was of the opinion that the recording of the applicant's data constituted and interference with art 8 ECHR, capturing and retaining images would not fall into its scope.[485] The Commission based this opinion on the facts that the police took the photographic material in a public place and not in the applicant's home, that the photos were taken in the course of a public event in which the applicant took part voluntarily, and that the recordings were

> …taken for the purposes, (…), of recording the character of the manifestation and the actual situation at the place in question, e.g. the sanitary conditions, and, (…), of recording the conduct of the participants in the manifestation in view of ensuing investigation proceedings for offences against the Road Traffic Regulations.[486]

This seems to suggest that pictures taken in public places fall outside the scope of art 8 ECHR once their nature is related to public incidents. The fact that personal data is processed, however, might change the nature of the images as such as they fall into the area of protection of art 8(1) ECHR but the mere taking and retention of photographs of the applicant in a public place without processing the imagery e.g. in order to identify the individuals in the pictures did not constitute an interference of art 8.[487]

Also, the mere existence of clearly visible surveillance technology did not amount to interference into art 8 ECHR. In 1993 in the *Hutcheon* Case, police authorities erected a surveillance tower facing the home of the applicant in Northern Ireland. While the applicant believed that her movements were watched and her conversations recorded, the Commission did not see sufficient evidence for such allegations and consequently

---

[483] Ibid, para 24.

[484] Ibid, para 43.

[485] Ibid, paras 51-53.

[486] Ibid, para 49.

[487] See *Friedl v Austria*, (n 482). The case was struck from the list and settled between the applicant and defendant, see *Friedl v Austria*, App no. 15225/89, Judgment (Court), (Struck out of the List), 31.01.1995.

regarded those claims as unsubstantiated. The Commission consequently did not find any interference of the surveillance tower with the applicant's home, communications or private life – and noted that even if there was an interference, those would be justified under art 8(2) ECHR.[488]

The view that visual surveillance technology in public spaces would not *per se* interfere with a right to privacy was reconfirmed in a decision on the absence of legal regulation of unrecorded public video surveillance in Belgium. In *Herbecq and the association "Ligue des droits de l'homme" v Belgium*, the applicants claimed that the lack of legal regulation of public video surveillance in Belgium constitutes a violation of the right to private life in art 8 ECHR, because

> …it is impossible for people subject to such surveillance to know when it is occurring what means of challenging it they have, and to whom to address themselves where they suspect that they have been subjected to such surveillance.[489]

Due to this uncertainty, individuals might change their behaviour in public places. Additionally, the applicants claimed that such surveillance might even be suitable to capture personal information or certain personal behaviour, which the individual might not have wanted to disclose to anybody.[490]

The Commission did not follow this argument and decided that there has not been any interference into the scope of article 8, since unrecorded video surveillance is not suitable for obtaining permanent information about individuals. The Commission argued that '…the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person' and that '[t]herefore all that can be observed is essentially, public behavior.'[491]

The argument that the mere presence of public visual surveillance systems which do not retain images or process personal data does not constitute an interference with art 8 (1) ECHR was again brought up in *Peck v UK*: The case concerned the applicant's attempted suicide in public, which was prevented by the police. Later, after the

---

[488] See *Hutcheon v the United Kingdom*, App no. 28122/95, Decision (Commission), 27.11.1996, 'the law' para 1.

[489] See *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421), para 94.

[490] Ibid, para 94.

[491] Ibid, para 97.

incident, the video images immediately following the suicide attempt, which were captured by a surveillance camera, were broadcast on a TV channel.[492] Although the applicant challenged the publication of the video material, but not the video surveillance as such, the Court restated its criteria developed in the findings in *Friedl* and *Herbecq*. Essentially three questions were important for the findings: Firstly, how far do visual images taken in a public space interfere with a person's privacy? Secondly, do the visual images have a public or private nature? And thirdly, was the material obtained '…envisaged for a limited use or was likely to be made available to the general public'?[493] While there was no interference in *Friedl* and *Herbecq* due to the lack of intrusion into the private sphere and the lack of personal data retention, in *Peck v UK* the publication of the visual material amounted to a serious interference into the private life of the applicant.[494]

Read the cases together, the ECtHR has developed a distinction that separates 'normal' visual surveillance from a certain form of sophisticated public surveillance which processes personal data. Furthermore, the purpose, nature and circumstances of the visual surveillance play a decisive role in determining a possible interference. In the *Peck*-case, for example, the Court explicitly noted that although the suicide attempt was conducted on a public road, the applicant could not foresee the surveillance or the publication of the material, and neither was he participating in a public event, let alone could he be considered a public figure.[495]

Consequently, interference of visual surveillance of an individual in public places into the ECHR's scope of private life was determined considering the following specific elements: Firstly, the individual's expectation of being subject to surveillance and how far the individual can foresee possible consequences of the surveillance,[496] secondly, the nature and role of the subject of surveillance: was the applicant for example a public figure? Thirdly, the nature of events under which the public surveillance takes

[492] *Peck v The United Kingdom*, (n 258).

[493] Ibid, para 61.

[494] Ibid, para 63.

[495] Ibid, para 62.

[496] Ibid.

place and if the applicant was e.g. taking part in a public event e.g. a demonstration.[497] Fourthly, the retention of personal information and processing of such data and if data was retained and used for identification of persons,[498] and fifthly, considering the design, purpose and intention of the visual surveillance, e.g. purely monitoring objects for security purposes.[499]

Additionally, the Court and the Commission have developed another element addressing the expansion of the scope of art 8 ECHR into the public sphere: the right to personal identity and to develop relationships with other human beings – also in a public context.[500] The Court held that '[t]here is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".'[501] Targeted surveillance in a public place, once this has an effect on persons developing their identities, might therefore constitute an interference. This argument boils down to the question if the intensity of surveillance has any effect on the ability of a person to form relationships or develop an identity and has therefore a direct connection with mass surveillance. The right to develop relationships with the outside world will be discussed later in this study.

The ECtHR in its case law developed a twofold opinion on visual public place surveillance. On the one hand, it distinguishes between an inner circle (home, private life and secluded spaces) and takes into account different individual expectations depending on the space in which an individual is situated. On the other hand, the Court constructs the right to form personal relationships in order to expand the right to private life into the public sphere.

This applies however, only with respect to the taking of imagery from a public place. The retention of personal data, permanent surveillance records or data processing have always been considered to fall into the scope of article 8 ECHR. In *Leander v Sweden*, which addressed a secret police register containing security relevant information about

[497] *Friedl v Austria*, (n 482), para 49.

[498] Ibid, para 50, 51.

[499] *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421), 97.

[500] See *P.G. and J.H. v the United Kingdom*, App no. 44787/98, Judgment (Court), 25.09.2001, para 56.

[501] Ibid.

individuals, both the retention and the release of such information interfered with art 8 ECHR.[502] Also, the creation of records through wiretapping and storing of phone calls from and to private homes and business premises constituted interferences.[503] Consequently, all kinds of records and personal data, even when obtained from public areas or held and processed by public authorities fall into the scope of private life in article 8.

Article 8 ECHR additionally covers location tracking and the subsequent creation of location databases. This includes GPS surveillance[504] as well as data bases retaining travel activities within a member state.[505] Subsequently, all elements including targeted visual surveillance, location tracking, monitoring of social interactions and communications, and data collection, retention and processing fall into the scope of art 8(1) ECHR.

With this, targeted surveillance of individuals in public spaces interferes with fundamental rights. However, it is interesting that the focus in finding interferences with a person's privacy in public appears to rely on information collection and therewith conceptually on informational privacy. At least in its early case law, the ECHR system seemed to support a perspective in which the amount of privacy granted to individuals is less in the public context, particularly when they voluntarily and actively participate in public life. This hints towards an understanding of privacy which is based on individual choice and individual freedom – and therewith on an individual's privacy expectations. The following section will address this argument in more detail.

3.1.1.1 Reasonable Expectations of Privacy in Public and the ECHR

Some concepts which grasp privacy in public rely on the idea of 'reasonable expectations of privacy'. This means that the grade of protection for individual privacy in the public sphere somehow depends on an individual's perception of privacy.

[502] See *Leander v Sweden*, (n 434), para 48.

[503] See *Kopp v Switzerland*, (n 412) para 53, *Amann v Switzerland*, App no. 27798/95 Judgment (Grand Chamber), 16.02.2000, paras 69, 80.

[504] See *Uzun v Germany,* (n 426), paras 51-53.

[505] See *Shimovolos v Russia*, App no. 30194/09, Judgment (Court), 21.06.2011, para 66.

According to that view, an individual can expect less privacy when sojourning on a public road than sitting in one's own bathtub at home. As discussed in section 2.2.7 above, this is based on very specific theoretical conceptions of privacy. But in how far do such conceptions influence the ECtHR's understandings of a fundamental right to privacy in public places?

When addressing such issues, the ECtHR frequently resorted to a formulation of a legitimate expectation of privacy test in public. In the *P.G. and J.H. v UK*, the ECtHR stated that

> [t]here are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.[506]

Some scholars argue that the first appearance of an individual expectation reasoning influencing fundamental rights protection in Europe was the *Lüdi* Case decided in 1992.[507] Mr. Lüdi, who allegedly tried to sell 2kg of cocaine to an undercover police officer, was unsuccessful in his complaint of a breach of art 8 ECHR. The applicant particularly challenged, firstly, the employment of an undercover officer who engaged in a personal relationship with him and secondly, that the undercover officer had used technical devices in order to record conversations and intrude into the applicant's home.

The Court regarded the fact that the applicant engaged in such criminal activity as reason enough to not find a violation:

> Mr Lüdi must therefore have been aware from then on that he was engaged in a criminal act punishable under Article 19 of the Drugs Law and that consequently

[506] *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

[507] Nouwt S, de Vries BR and Loermans R, 'Analyses of the Country Reports' in Nouwt S, de Vries BR, Prins C (eds*), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser 2005) 323-358, 334.

> he was running the risk of encountering an undercover police officer whose task would in fact be to expose him.[508]

This can be interpreted that the applicant enjoyed a lesser expectation of privacy because he engaged in criminal activity.

In wording, the ECtHR used the 'reasonable expectation' – formula for the first time in the *Halford*-case.[509] The background of the case were the repeatedly unsuccessful applications for a higher-ranking position by the applicant, who was the most senior female police officer in the UK at that time. Ms. Halford hence started a complaints procedure against several superiors as she suspected gender discriminatory reasons for the repeated rejections of her applications.[510] During the investigation, the applicant's workplace phone was intercepted in order to allegedly obtain information about Ms. Halford to be used against her in the discrimination proceedings.[511] The Government argued that Ms. Halford would not have had a reasonable expectation of privacy at her workplace and that employers should be able to monitor calls made on work-phones by their employees and that henceforth the interception would fall outside the scope of protection of art 8 ECHR.[512]

The Court disagreed with that view and stated that both private but also business premises as well as correspondence can fall into the scope of art 8 ECHR and that Ms. Halford very well '…had a reasonable expectation of privacy for such calls…' especially considering the fact that she was additionally told she could use her work-phone for private purposes and for purposes of working on her discrimination case.[513] The Court furthermore found a violation of art 8 ECHR because the interception of her office phone was not in line with the legality requirement of art 8 (2) ECHR.[514]

---

[508] *Lüdi v Switzerland*, App no. 12433/86, Judgment (Court), 15.06.1992, para 40.

[509] See Gomez-Arostegui HT, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2004-2005) 35 California Western International Law Journal 153, 165.

[510] *Halford v the United Kingdom*, App no. 20605/92, Judgment (Court), 25.06.1997, paras 9-15.

[511] Ibid, para 17.

[512] Ibid, para 43.

[513] Ibid, para 45.

[514] Ibid, para 46-51.

This means, however, that the court at least partly based its assessment of whether Ms. Halford had such a reasonable expectation on the possibilities she had to subjectively expect an interception of her phone. Gómez-Arostegui rightly wonders if the Court's assessment would have been different if Ms. Halford had been informed about the possibility of workplace communication interception beforehand.[515] In any case, albeit responding to the Government's argument of reasonable expectation, the case gives little detailed guidance as to how exactly a reasonable expectation test for art 8 ECHR would look like. It also should be noted that it would have not been necessary for the Court to actually engage in that argument, as it did establish the interference without actually resorting to Ms. Halford's expectations.[516]

A similar argument was brought forward in a more recent case concerning the surveillance of communication at the workplace: in *Copland v UK*, the Court found a violation of art 8 ECHR as the monitoring of the applicant's phone and e-mail communications as well as internet activity fell under the scope of article 8 and were not in accordance with domestic law.[517] While the Court, for the first time, included e-mail communications and internet usage into the scope of article 8, it also stated that the applicant had a 'reasonable expectation as to privacy' as she was not warned that her office calls, internet usage and e-mails might be monitored.[518]

The Court, however, specified its view on 'reasonable expectation' in 2001 in *P.G. and J.H. v UK*.[519] The Court stated that '…a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor' and connected the individual's expectation to the public place:

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same

[515] See Gomez-Arostegui HT, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2004-2005) 35 California Western International Law Journal 153, 167.

[516] Ibid, 166.

[517] See *Copland v the United Kingdom*, App no. 62617/00, Judgment (Court), 03.04.2007, paras 45 - 49.

[518] Ibid, para 42.

[519] *P.G. and J.H. v the United Kingdom*, (n 500).

> public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.[520]

The background of the case concerned police investigations into a planned robbery of a money transport during which the police secretly recorded the applicants' voices in a police station in order to compare them to audio recordings obtained from a listening device installed in an apartment – which was considered to be an interference into the right to private live and a violation of art 8 as it was not in accordance with the law.[521] It is remarkable that the Court summarized its jurisprudence mentioning the reasonable expectation test in this judgment – especially as it based the interference foremost not on a reasonable expectation test, but on the fact that the secret voice recordings at the police station established permanent records of personal data.[522] Gomez-Arostegui rightly asks how the two different arguments - the legitimate expectation of privacy by the applicant and the processing of the applicant's personal data – relate to each other.[523] If joint together, this would mean that the processing of personal data such as video or audio recordings in a public place becomes an interference only in relation to the individual's expectation that her data was being processed, retained and used. One could, however also argue the contrary, namely that personal data protection works independently from one's personal expectation and that legitimate expectation in public places are only a part of the Court's general assessment of interferences *per se*.

Reading between the lines of *P.G. and J.H. v UK*, it appears that the Court was rather careful with the introduction of a general legitimate expectation test for privacy cases. In fact, in the 2003 *Perry* case, the Court referred to *P.G. and J.H.* noting that '[a] person's reasonable expectations as to privacy is a significant though not necessarily conclusive factor.'[524] The Perry case, as discussed above, concerned the manipulation of a video camera in a police station in order to obtain better images from a suspect. While the Court again emphasized that the manipulation of a normal surveillance

---

[520] Ibid, (n 500), para 57.

[521] Ibid, paras 60, 63.

[522] Ibid, para 59.

[523] See Gomez-Arostegui HT, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2004-2005) 35 California Western International Law Journal 153 p 169.

[524] *Perry v the United Kingdom*, App no. 63737/00, Judgment (Court), 17.07.2003, para 37.

camera and use of records in an identification procedure could not been expected or foreseen by the applicant, it based the finding of an interference on the facts that such manipulation created permanent records and constituted the processing of personal data.[525]

Also, shortly before *Perry*, in the *Peck* judgment, the Court partly used what could be considered a reasonable expectation of privacy test. As described above, the *Peck* case concerned the publication of video recordings relating to the applicant's suicide attempt in a public space. The Court, after quoting the above mentioned core formulation in *P.G. and J.H. v UK* and therewith once again that '…a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor'[526], established that the *disclosure* of the video footage amounted to an interference with the applicant's private life.[527] The case is somehow special as the applicant did neither complain about the video surveillance *per se*, nor about the processed personal data, but merely about the disclosure of the material for media broadcasts in which he was clearly identifiable.[528] The Court assessed the facts in light of the tests established in *Lupker* and *Friedl*[529], in which the Court weighted an intrusion into the inner circle of the applicant's life, and in that sense if the material obtained related to public or private activities or events, if the person concerned was a public figure, and if the material was published or disseminated.[530] The Court concluded that '[a]s a result, the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation (…) and to a degree surpassing that which the applicant could possibly have foreseen…'.[531] This goes in line with the Court's assessment, that certain individual expectations – expressed through the criteria of foreseeability- are part of the Court's assessment of interferences into private life in public places. The Court does however not seem to

[525] Ibid, para 41.

[526] *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

[527] *Peck v The United Kingdom*, (n 258), para 63.

[528] Ibid, para 60.

[529] See the discussion above and *Lupker and Others v the Netherlands*, (n 480); *Friedl v Austria*, (n 482).

[530] *Peck v The United Kingdom*, (n 258), para 61.

[531] Ibid, para 62.

give too much weight on individual's expectations or personal choice arguments as it regards them as a part of, but not as a fully-fledged argument in the ECtHR's case law.[532]

Recent judgments of the ECHR confirm such a reading: in *Uzun v Germany*, a case concerning GPS tracking, the Court, although citing the formulation that a person's reasonable expectation of privacy might be somehow significant, but not necessarily conclusive from *Perry v UK*,[533] quickly moved on and established the interference merely on the fact that GPS data was collected, processed and retained.[534] The Court hence did not engage in an argument about the applicant's reasonable expectation of being tracked by a GPS transmitter in public places, but concluded that '…the applicant's observation via GPS, (…) , and the processing and use of the data obtained thereby (…) amounted to an interference with his private life…'.[535]

Another significant contribution of the reasonable-expectation argument to the Court's case law, concerns the very classic issues of alleged intrusion into the privacy of persons of public interest through the media. In the 2012 *von Hannover 2* case, a case adressing the publication of images of celebrities in tabloid newspapers, the ECtHR recognized the importance of a right to personality. [536]

> …[T]he concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.[537]

Consequently, interactions with others, and the development of one's own personality fell into the protected sphere of private life. Here, also photographs fell into the protective scope, although they were taken in public places and concerned a person of

---

[532] Gomez-Arostegui, however, established an argument about how the Court could use a reasonable expectation of privacy test as a future benchmark for its case law. See Gomez-Arostegui HT, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2004-2005) 35 California Western International Law Journal 153.

[533] *Uzun v Germany,* (n 426), para 44, *Perry v the United Kingdom*, (n 524), para 37.

[534] Ibid, paras 49-53.

[535] Ibid, para 52.

[536] *Von Hannover v Germany*, App no. 59320/00, Judgment (Court) 24.06.2004; *Von Hannover v Germany* (no. 2), App nos. 40660/08, 60641/08, Judgment (Grand Chamber), 07.02.2012.

[537] *Von Hannover v Germany* (no. 2), ibid, para 95.

public interest.[538] The Court gave significant weight to the importance of images because they were

> …one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development. It mainly presupposes the individual's right to control the use of that image, including the right to refuse publication thereof.[539]

In case of questions addressing the publication of images, the ECtHR regarded it as important to emphasize that persons might have a certain legitimate expectation of privacy protection although they were persons of public interest.[540]

In cases concerning the publication of information on persons of public interest, a legitimate expectation of privacy therefore plays a role in ECHR case law when assessing whether a lack of protection from the publication of personal information constitutes a violation. Here, legitimate expectation is employed in order to balance the interest of the individual against a public interest and the freedom of expression. Nevertheless, in the *von Hannover* cases the ECtHR has also stressed individual personality rights as constituting the essence of a right to private life, and therewith appears to apply a privacy conception based on personality and dignity. At the same time, however, it employed the individual expectation of public figures, an argument that can be associated more with a liberal individual-centric conception of privacy.

This is not surprising considering the closely related natures of the *von Hannover* cases and other cases relating to the dissemination of information on public figures, and the conception of privacy as a right to be let alone by Warren and Brandeis. In fact, on a closer look, Warren and Brandeis derive the right to privacy partly also from the construction of an individual's inviolate personality.[541]

It is interesting to note that the ECtHR here uses the term 'legitimate expectation' when assessing an individual interest in public figures when challenging image publication, however, it has otherwise mostly used the term 'reasonable expectation'

---

[538] Ibid; see also *Petrina v Romania*, App no. 78060/01, Judgment (Court), 14.10.2008, para 27.

[539] *Von Hannover v Germany* (no. 2), (n 536), para 96; *Reklos and Davourlis v Greece*, App no. 1234/05, Judgment (Court), 15.01.2009, para 40.

[540] *Von Hannover v Germany* (no. 2), (n 536), para 95; *Von Hannover v Germany* (no. 3), App no. 8772/10, Judgment (Court), 19.09.2013, para 41.

[541] See Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 194.

when addressing public surveillance systems. While it is not entirely clear if and how the Court distinguishes those two formulations, one possible explanation might be that 'legitimate' expectation might have a closer judicial connection, e.g., whereas 'reasonable' might have closer societal component.

It can hence be concluded that, although the reasonable expectation of privacy can be considered a part of the Court's analyses of privacy intrusions in the public sphere, it does not appear to function as a predominant argument in the Court's case law addressing public surveillance. Particularly regarding targeted public visual surveillance, the Court has recently put more weight on the assessment of the collection, retention and processing of personal data rather than on individual's expectations when it comes to privacy in public places.

The legitimate expectation test within the ECHR framework for public place surveillance is problematic, which is reflected in the cautious approach taken by the Court. It plays a role up to a certain extend and with relevance to a certain type of cases, but it has not become a standard test, regularly applied by the ECtHR.

Hence, while one can argue that the expectation of a person in a public space matters for the assessment of whether there has been an interference or not, the expectation as such has not played such an important role and it remains unclear as to how exactly a legitimate or reasonable expectation test functions coherently in ECHR cases.

Reasonable, or legitimate expectations of privacy by individuals might however, be taken into account in concrete cases as part of a larger assessment scheme. This means that when assessing targeted visual surveillance through highly sophisticated surveillance systems as in the Helberg scenario, the Court would most likely find an interference taking into account the following factors:

Firstly, the discussion above suggests that the ECtHR would consider the design and purpose of the surveillance system in question. Why was it installed, and what is its general purpose? Is it a 'normal' security system that merely monitors places for a specific purpose? Or does it enable indiscriminate surveillance? Here, the technical sophistication of the visual targeting capabilities will play a role as well as the purpose restriction. It is however, not clear how the Court would value technical sophistication

as such. It might certainly lay weight on the system's capabilities to process personal data.

Secondly, as outlined above, the ECtHR might take into account the foreseeability and transparency of the visual surveillance system and its capabilities. This might reach from an assessment of the design of the system to questions of visibility, labelling, public warnings or even general knowledge about the system. This might also include the question of how far an individual could foresee and expect a certain kind of surveillance, including its consequences and hence take into account the reasonable expectation of individuals.

Thirdly, the Court might consider the nature of the events and the nature of surveillance in the individual case, for example, was the person under surveillance participating in a public event or alone at night in a parking lot. At least in the past, the Court has made such distinctions.

Fourthly, the nature and situation of the applicant as a person might also play a certain role, although this is does not appear too relevant concerning police surveillance.

Fifthly, as already indicated, and as will be discussed in the following section, it may play a decisive role how personal data of surveillance subjects are processed and retained.

Sixth and finally, the accessibly to surveillance data, their possible disclosure or publication may also be important factors for the Court when assessing whether an interference into art 8 (1) ECHR is established through targeted visual surveillance in a possible Helberg case.

3.1.1.2 Covert and Overt Public Surveillance

As mentioned above, targeted surveillance of individuals is often conducted directly by police authorities within criminal investigations. Public surveillance systems with a certain degree of sophistication might hence be very useful within a targeted police operation. One further question when assessing visual surveillance in public places is the question about a distinction between two design features of surveillance systems: secret and hidden systems on the one hand, and visible and open surveillance systems on the other.

Usually, covert surveillance is distinguishable from overt surveillance simply through knowledge of an individual about being subject to surveillance. Consequently, some police operations which target a specific suspect might, by their nature, be covert operations. How far does such hidden, or unforeseeable surveillance give rise to interferences with the right to privacy enshrined in the ECHR?

The ECtHR dealt with questions of targeted secret surveillance in a variety of contexts. *Perry v UK*, for example, concerned targeted secret visual surveillance of individuals. The case originated in criminal investigations into several counts of robbery against the applicant during which he was brought to a police station. While passing through the custody suite at the stations, the applicant's images were captured by a surveillance camera, which was previously manipulated to obtain better and clearer images so that those images could be shown to witnesses to identify the suspect.[542] Unlike

> …the normal use of security cameras *per se* whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose…[543]

the surveillance images in the *Perry* case constituted an interference with art 8 ECHR. The Court reasoned, firstly, that the manipulation of the camera, together with the compilation of images and the subsequent use of the material in criminal investigation and proceedings, constitutes the collection and processing of personal data and therewith an interference with art 8 ECHR.[544] Secondly, the Court emphasized that while the camera as such was visible to the applicant, he could not have known of the technical alterations and subsequent use of the material obtained.

> Whether or not he was aware of the security cameras running in the custody suite, there is no indication that the applicant had any expectation that footage was being taken of him within the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. This (…) went beyond the normal or expected use of this type of camera, as indeed is demonstrated by the fact that the police were required to obtain permission and an engineer had to adjust the camera.[545]

---

[542] See *Perry v the United Kingdom*, (n 524), paras 39-41.

[543] Ibid, para 40.

[544] Ibid, para 41.

[545] Ibid.

This can be seen as an indication of the Court's critical view towards targeted secret surveillance. It appears that a 'normal' security camera as such, with a 'legitimate and foreseeable purpose' would not raise concerns within the ECHR. However, the moment that footage is somehow altered, targeted or directed towards an individual without the individual having any expectations of being targeted, fundamental rights issues arise. The Court here used two parallel arguments: Firstly, it used the argument of legitimate expectation as discussed above. Secondly, it conditioned the question when visual surveillance becomes an interference with rights in the Convention on the processing of personal data.

Legitimate expectation hence plays a decisive role in distinguishing covert and overt surveillance in public places. Taking into account the efficiency, technical functionality and sophistication of surveillance systems today, it will be difficult for the Court to not find an interference with Convention rights. In that connection, it might be wise to view modern video surveillance systems *per se* as an interference – especially considering the fact that modern surveillance systems rarely work without certain forms of personal data processing.

Another important problem arising from the distinction between covert and overt surveillance is the question of legal safeguards and public scrutiny. The ECtHR has pointed out on several occasions, that secret surveillance comes with a high risk of a lack of control, judicial review and safeguards. Such a risk of power abuse hence required that '…domestic law provides adequate protection against arbitrary interference with Article 8 rights.' [546] Any police action conducted in secrecy consequently demands for a sufficiently clear legal base, adequate authorization and

> …must be sufficiently clear in its terms to give individuals an adequate indication of the circumstances and conditions in which public authorities are entitled to resort to such covert measures.[547]

Consequently, targeted secret surveillance in public places can be regarded as interference into art 8 ECHR and therefore requires being in line with the legitimacy

[546] See *Uzun v Germany,* (n 426), para 63, see also, *Amann v Switzerland*, (n 503), paras 76-77; *Bykov v Russia*, App no. 4378/02, Judgment (Grand Chamber), 10.03.2009, para 76; see also *Weber and Saravia v Germany*, (n 419), para 94; *Liberty and Others v the United Kingdom*, App no. 58243/00, Judgment (Court) 01.07.2008, para 62.

[547] See *Khan v the United Kingdom*, App no. 35394/97, Judgment (Court), 12.05.2000, para 26; *Taraneks v Latvia*, App no. 3082/06, Judgment (Court), 02.12.2014, para 87.

mechanisms provided in the Convention.[548] Nevertheless, it is not entirely clear how the Court would assess visual surveillance *per se* – as it has in the past relied more on either the processing of data, or monitoring of communications in order to establish interference in complex targeted surveillance cases.

If such standards were to be applied to a targeted covert police operations, it is clear that such operations would require a clear legal basis. There would therefore need to be a sufficiently clear and accessible law regulating targeted covert operations, including the use of surveillance technologies. The problem here is that there appears to be a significant difference in the requirements for techniques of targeted surveillance on the one hand, and mass surveillance technologies used for targeted surveillance on the other. While traditional targeted surveillance techniques appear limited in their effect, mass-surveillance technologies, although they are used for targeting a single person at a particular moment, have in principle unlimited surveillance capabilities. Mass-surveillance technologies therefore tend to have a greater effect on fundamental rights protection of communities, while purely targeted technologies have such effects on a more limited number of persons. This will be discussed in more detail further below.

In order to fulfil the legality requirement, the law regulating such operations needs to be '…sufficiently clear in its terms to give individuals an adequate indication of the circumstances and conditions in which public authorities are entitled to resort to such covert measures'[549]

It is difficult to see how these quality and clarity requirements can be fulfilled when, for example, the general capabilities for surveillance are kept secret, or the law does not specifically deal with the targeting capabilities of surveillance systems. While naturally covert and overt surveillance operations require some distinction regarding fundamental rights assessments, due to the technological nature of surveillance systems and surveillance techniques, it becomes increasingly difficult to legally separate targeted and mass surveillance operations. In this context, setting a lower fundamental rights threshold for visible surveillance systems than for targeted covert

[548] *Klass and Others v Germany*, (n 423), para 41.

[549] *Khan v the United Kingdom*, (n 547), para 26; *Taraneks v Latvia*, (n 547), para 87.

surveillance operations would not take into account the evolving surveillance technological capabilities of security systems.

3.1.2 Personal Information and Surveillance

Personal data plays a more and more important role in everyday life and has therewith an enormous effect on surveillance and security applications. In fact, all information about individuals in digital form qualify as personal data. Personal data has been defined as information relating to an identified or identifiable individual, essentially since the beginnings of data protection regulation.[550] It goes without saying that modern surveillance systems, especially when they are applying certain analytics software, will inevitably create and process personal data. In that regard, public surveillance as pictured in the Helberg surveillance scenario will create personal data in many forms, and modern surveillance systems have capabilities to create a holistic and real time digital information profile about a person. While the regulation of data processing is not a new phenomenon, data protection has recently gained prominence as being understood increasingly as an essential fundamental right.[551] A fundamental rights analysis of targeted surveillance systems therefore requires a closer look at data protection as a fundamental right in Europe.

There are several aspects in the scenario of particular relevance for data protection. Firstly, mostly all computer technology and all types of sensors produce data, for example the digital visual images from a video surveillance camera which are stored on a hard drive.

Secondly, data production is often an unintended by-product of computer technology.[552] Card payments, mobile phone usage, and social media activities amongst many others, produce a vast amount of information. The primary purpose of such data collection and retention is not surveillance, but to enable the technology or

---

[550] See e.g. Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation accessed 20 February 2017, 1. a); CoE Data Protection Convention, (n 299), Art 2 (a); Directive 95/46/EC (Data Protection Directive) (n 305), Art 2 (a).

[551] See Section 2.3 above.

[552] See Schneier B, *Data and Goliath: The Hidden Battles to Collect your Data and Control your World* (W.W. Norton 2015).

service to function. Similarly, a smart meter measuring the precise consumption of electricity does not only record electricity consumption for the energy company, but it allows also for extensive individual profiling and the analysis of life-patterns. Data that was created as a by-product to a certain service can be used as surveillance data.

Thirdly, data is always of different qualities and types. There is, for example a clear difference between personal data relating to an individual, a large data base or 'big data'. While big data bases are useful for large scale analytics, e.g. information on rush hour traffic flows, individual or personal data contains very specific information on single individuals.

In that regard, public surveillance would be unthinkable without the use of sophisticated data collection, data retention, and the employment of analytical tools. Modern surveillance accumulates and integrates data through a large variety of sensors and tools in order to search, sort, and filter information useful for particular surveillance purposes. Data from a large variety of sources can be employed for surveillance practices. For example, camera surveillance can be connected with mobile phone location data or information gathered from social media. German police forces have used surveillance technologies to collect mobile phone meta data around a political demonstration for the purpose of the identification of suspects - leading to debates about the possible repressive effects of such surveillance measures.[553] Data collected from mobile phones allowed the collection of location and communication data of all individuals present within a certain radio cell at a given time.

Social media data can as well play an important role in public place surveillance. During and after the so called '2011 London Riots', a series of protests leading to violent riots and looting after the police shot a Tottenham resident in August 2011, security authorities used social media sites such as Facebook and Twitter in order to identify participants in the riots, both by analysing visual data found on social media and by publishing images of perpetrators. Social media data intelligence consequently

[553] See SPIEGEL Online, Demo in Dresden: Polizei wertete Tausende Handy-Daten aus, 19.06.2011, http://www.spiegel.de/netzwelt/web/demo-in-dresden-polizei-wertete-tausende-handy-daten-aus-a-769275.html accessed 2 November 2015; Meister A, Funkzellenabfrage: Die millionenfache Handyüberwachung Unschuldiger. *Netzpolitik.org*, 21 December 2012, https://netzpolitik.org/2012/funkzellenabfrage-die-millionenfache-handyuberwachung-unschuldiger/ accessed 2 November 2015.

can play an important role in all kinds of criminal investigations as well as it can be used for political repression.[554] In both examples, data produced in non-surveillance contexts played decisive roles in public place surveillance techniques.

There are many other examples in which data from a variety of different sources could be used and integrated into complex surveillance operations and in comprehensive surveillance systems. The analyses of data streams in order to predict criminal activity and even terror attacks, for example, have been debated in 2011 after WikiLeaks released hacked e-mails from the private security company Stratfor, indicating that software called TrapWire was employed in two US cities.[555] Although the capabilities and operational methods of the system are not publicly know, the leaked sources indicated that the system employed data from video surveillance streams in order to pick out preparation operations for possible terror attacks employing video analytics.[556]

While large data collection intuitively appears better suited for mass-, and untargeted surveillance, targeted individual surveillance requires the detailed analyses of information relating to individuals. Targeted data surveillance consequently means that information about individuals is collected, retained and analysed. A video surveillance system, for example captures visual data from a public place. Once a person is clearly visible in the captured video, the video becomes personal data. Once that data is stored on a hard drive or analysed somehow, that personal data is stored and processed.

The question which will be addressed in the following sections is how data protection can function as a legal argument against mass surveillance practices. It should be noted that data protection has a somewhat strange role in surveillance operations: it bridges the gap between individual and mass surveillance and it can serve as a separate right

---

[554] See Omand D, Bartlett J and Miller C, 'Introducing Social Media Intelligence (SOCMINT)' (2012) 27 Intelligence and National Security 801; for a critical analysis and the roles of social media in public protest situations, see also Fuchs C, 'Social media, riots, and revolutions' (2012) 36 Capital & Class 383.

[555] See Eijkman Q and Weggemans D, 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?' (2012) Security and Human Rights 285, 295.

[556] See Stanley, J, 'What to Make of the TrapWire Story?' ACLU Speech, Privacy & Technology Project, ACLU, 14 August 2012, https://www.aclu.org/blog/what-make-trapwire-story?redirect=blog/technology-and-liberty-free-speech-national-security/what-make-trapwire-story accessed 3 November 2015.

in Europe in order to cover cases which are problematic to be addressed with an argument based on a right to privacy. Of particular importance is the nature of the European legal space regarding the protection of personal data as it combines two fundamental rights protection regimes that have jointly, but also independently developed data protection as a fundamental right: the ECHR and the EUCFR.

3.1.2.1 The Definition of Personal Data

Personal data protection concerns the regulation of information on individuals. The definition appears rather clear and is defined in the basic legal sources on data protection in Europe.[557] Article 2 a) of the 1981 CoE Data Protection Convention, for example defines personal data as 'any information relating to an identified or identifiable individual ("data subject")'.[558] The EU Data Protection Directive defined personal data as '…information relating to an identified or identifiable natural person,'[559] with the addition that

> …an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

In the GDPR (as well as in the new Police Directive), personal data is defined in the same way but with a slightly modified explanation of an identifiable person:

> "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;[560]

In the context of public mass surveillance, this distinction is of great relevance because not all data collect from a public environment fall into the category of 'personal' data. At first sight, non-personal data appears not relevant for the purpose of surveillance. Data on the temperature on a square, for example, will hardly be controversial from a

[557] It should be noted that the scope of application of the EU data protection sources in particular is limited to the scope of EU law, excluding especially national security and policing issues. This is discussed in more detail in Section 3.2.3.4 below.

[558] Art 2(a) CoE Data Protection Convention, (n 299).

[559] Direct Directive 95/46/EC (Data Protection Directive) (n 305), Art 2 (a).

[560] Art 4 (1), Regulation (EU) 2016/679, (GDPR), (n 303); Art 3(1) Directive (EU) 2016/680 (n 303).

fundamental rights perspective. Similarly, information about how many cars are lining up at which point in what direction, or the number of persons in a specific space at a certain time might not qualify as personal data in the respective definitions as personal data requires a connection or a relation to a natural person. Yet, such data might gain some relevance once it can either be related to a single natural persona, or if the overall data collection has an effect on individuals or groups of persons. The question in context of public surveillance is, of course, what data would qualify as personal data in the surveillance scenario and would therewith fall into the material scope of data protection in Europe.

What qualifies as 'information' in the context of data protection regulation has been extensively discussed[561] and guidance can be found in the opinions[562] of the Article 29 Data Protection Working Party', a EU advisory body on data protection issues established through article 29 of the 1995 EU Data Protection Directive. According its opinion on the concept of personal data, the nature of information relates to both objective information, such as 'person A is now walking on street X', but also subjective information on persons such as opinions or abilities, e.g. 'person B is really good at skateboarding'.[563] The Art 29 Working Party explicitly assumed that visual and audio data can contain personal information and therewith qualify as 'personal' data.[564] Also, the 1995 EU Data Protection Directive contains a direct reference to the processing of audio and visual data:

> …given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data.[565]

[561] See e.g. Lloyd IJ, *Information Technology Law* (6th edn, Oxford University Press 2011), 39-60, Bainbridge D, *Introduction to Information Technology Law* (6th edn, Longman 2008), 505, 506.

[562] Especially Article 29 Data Protection Working Party (Art 29 WP), Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN WP 136, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf accessed 10 October 2016.

[563] Ibid, 6-8.

[564] Ibid, 7-8.

[565] Recital 14, Directive 95/46/EC (Data Protection Directive) (n 305). See also Article 33 thereof.

It is therewith clear that surveillance data cannot be excluded from the scope of protection of EU data protection law simply because the processed information comes from public spaces or is available freely to anybody.

Additionally, certain types of analytics require the use of information that qualify as personal data: biometric data, for example, has a special character. A facial profile constitutes personal data as such, but also enables linking certain other types of information to an individual for example the whereabouts of person A. In a similar way to fingerprints or DNA profiles, personal information is used to create links between persons and objects.

The Art 29 WP Opinion on the concept of personal data distinguishes here between extracting information from individual tissues and the samples as such: human tissue samples as such are not considered personal data, however, the extraction of information and storage in profiles, is.[566] Therewith, the use of personal information from public individual surveillance falls into the category of personal information, both for the Council of Europe and for the EU framework.

The second question important to the definition of personal data is the meaning of the relational element in the definition. Information 'relating' to individuals evidently requires some connection between the information processed for public surveillance and a natural person. The relation between individual and information can be of a direct nature such as 'person A on camera 1 has dark hair' or of an indirect nature, e.g. 'the car causing the accident at place x had the number plate XYZ-123, and XYZ-123 belongs to person A'. In some cases, the indirect relation is not that obvious and can be problematic, as for example traffic flow data could be understood as somehow relating to each single individual participating in the respective traffic. For clarification, the Art 29 Working Party issued a document on data protection and RFID tags in 2005 in which it proposed the following definition:

[566] See Art 29 WP, Opinion 4/2007 on the concept of personal data, (n 562), 9. On tissue samples, see also Council of Europe, Recommendation No. Rec (2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin, of 15 March 2006; and Recommendation, CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, 11 May 2016.

> Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.[567]

In its further elaboration, the Art 29 WP suggested a 'three alternative elements'- test in order to determine if data relates to an individual. According to this test, the relation should be established with reference to 'content', when the information is directly about someone, with reference to 'purpose', when the information contains the purpose to somehow evaluate or influence a person, or with reference to 'result', when information is likely to have a certain impact on a person's rights and interests.[568]

Consequently, data in a public surveillance scenario generally can be considered to be related to persons when they contain information about somebody (Person A is carrying a pink bag), when the information is used to influence or evaluate a person (collection of arrival times of employees via facial recognition), or if the result of data processing has an impact on a specific person (collection of mass traffic data impacts traffic flow regulation with the result that person A at location X has to wait longer).

A third important term in the definition of personal data, both in the EU as well as the CoE frameworks, are the criteria of 'identification' and 'identifiability'. Identification can be described as distinguishing a person from another using specific criteria or characteristics unique to that person. Information about a person therefore either clearly identifies an individual (e.g. a name, birthdate etc.) or enables the identification of an individual by using further means.[569]

Discussions around the issue of identification of individuals are strongly interconnected with technological progress and the actual capabilities to identify somebody using data processing. The 1981 Explanatory Report on the CoE Data Protection Convention stated that '"[i]dentifiable persons" means a person who can be easily identified: it does not cover identification of persons by means of very

[567] Art 29 WP Working document on data protection issues related to RFID technology, 19 January 2005, 10107/05/EN WP 105, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf accessed 13 October 2016, 8.

[568] Ibid 8-11.

[569] See e.g. European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2014), 39; Bygrave LA, *Data protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 43.

sophisticated methods.'[570] This conception stems from an understanding that the more complex processing is, the harder it will be to identify a person. With increasing processing power this reading can only be seen as a misconception:[571] More recent data protection documents contain different definitions: According to the 1995 EU Data Protection Directive, '…account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person'[572] when interpreting identifiability. The GDPR states:

> …account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.[573]

This means that both direct information about an individual (name), as well as indirect information about individuals, where a unique combination of information or indicators can lead to identification, qualify as personal data. It is worth pointing out that 'reasonable likelihood' is a determining factor for identifiability in both the 1995 Directive and the 2016 Regulation and that technological capabilities play an important role in the EU data protection framework. Such definitions also consider the facts of technological progress and advancing capabilities through which today's unidentifiable data may be made identifiable tomorrow.

This is of high relevance for public surveillance practices. Data such as, for example, video stream of a public place captured from a distant perspective might fall outside the scope of data protection laws because low image quality defies individual identification. There is however no guarantee that future technologies will not make it possible to extract and process further information from such material than what can be done today.

---

[570] CoE Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981, para 28

[571] This argument is made by Bygrave LA, *Data protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 43

[572] Recital 26 Directive 95/46/EC (Data Protection Directive) (n 305).

[573] Regulation (EU) 2016/679, (GDPR), (n 303), Recital 26.

Following such a conception of identifiability, data obtained through surveillance technology is highly likely to qualify as personal data, therewith triggering the respective protective mechanisms. This includes direct information about persons but as well a variety of data that relate to persons and theoretically allow their identification. In determining identifiability, however, probability, capability and necessary efforts should be taken into consideration. Consequently, a wide variety of data which falls into that category can be taken from a public space: physical features, behaviour, personal profiles, location data, communications data and generally indicators that can be linked in order to target and distinguish individual person in public environments.

The following section will now move on towards a brief discussion of general data protection principles and their relation to urban public place surveillance.

3.1.2.2 The General Principles of Data Protection

Data protection is a complex legal field and attempts have been made to distil and distinguish several core principles of data protection which are more or less contained in legal documents regulating data protection.[574] Principles in that sense can be understood as abstract legal rules which exercise a certain form of normative force, both as 'guiding standards' as well as actual rules found in data protection regulations.[575]

The assumption behind such principles is that personal data processing in principle interferes with certain rights and freedoms of individuals. A central element in data protection is therefore the general principle of limited collection, retention and processing.[576] This follows a common understanding that information on individuals is problematic *per se* and should therefore be limited.

---

[574] See for example Bygrave LA, *Data protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 57, see also European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2014), 61-62. See also Siemen B, *Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006), 49 and for a more general discussion on the function of data protection principles for an emancipatory view on privacy see Gutwirth S, *Privacy and the Information Age* (Rowman & Littlefield Publishers 2002), 85-112.

[575] See Bygrave LA, *Data privacy law: An International Perspective* (Oxford University Press 2014), 145

[576] See Gutwirth S, *Privacy and the Information Age* (Rowman & Littlefield Publishers 2002), 85.

Bygrave established a nuanced catalogue of principles addressing the obligations of controllers and data subjects, such as 'fair and lawful processing', 'minimality', 'purpose specification', 'information quality', 'data subject participation and control', 'disclosure limitation', 'information security' and 'sensitivity'.[577] The CoE/EU handbook on data protection lists similar key principles of European Data Protection law which derive both from the Council of Europe and the EU data protection frameworks.[578] This includes the principle of lawful processing, purpose specification and limitation, data quality (relevancy and accuracy), limited retention, fair processing and accountability.

Most of those principles are also enshrined in the legal data protection documents: The CoE Data Protection Convention enshrines several principles in its second chapter, especially art 5 relating to the quality of data, art 6, which addresses special data categories and, art 7, focusing on data security.[579] Also the EU Data Protection Directive states that data should be 'processed fairly and lawfully', 'collected for specified, explicit and legitimate purposes', proportionate, accurate and timely limited.[580] The GDPR explicitly lists 'lawfulness, fairness and transparency', 'purpose limitation', 'data minimization', 'accuracy', 'storage limitation' and 'integrity and confidentiality' as core 'principles relating to personal data processing' in its art 5.[581]

Taken together, this means that the processing of personal data comes with strict limitations as it is as such an interference with personal freedom and privacy. It could be added that some of those principles reflect certain rights of individuals which have been expressed and developed in other contexts: the 'right to informational self-determination', the 'right to be forgotten' or the 'right to integrity of information technological systems' are examples of individual rights being reflected by such principles. As such, data protection rights and principles are similar in most legal documents. Additionally, a variety of them are explicitly articulated as rights: it stands

[577] Bygrave LA, *Data protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), 57.

[578] European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2014), 61-62.

[579] CoE Data Protection Convention, (n 299).

[580] Directive 95/46/EC (Data Protection Directive) (n 305), Art 6.

[581] Regulation (EU) 2016/679, (GDPR), (n 303), Art 5.

to reason that at least some may compose the very core of a right to data protection in the age of information technologies. Several principles appear to be broad and indeterminate, while others are rather specific. Within the context of targeted surveillance in public places, however, they can contain useful hints establishing the requirements for the design and character of such surveillance.

One, if not the key requirement for processing data in the context of public surveillance is lawfulness. It is one of the basic requirements for the legitimation of interferences with individual rights in Europe. Within the ECHR, lawfulness is an essential component of a permissible limitation test, in which any interference with the right to private life is required to be 'in accordance with the law'.[582] Consequently, as the processing of personal data has clearly been recognized as an interference with Convention rights, processing requires a precise, accessible and foreseeable basis in domestic law.[583]

Also, the EU Charter of Fundamental rights requires lawfulness as one of the main criteria. According to general limitation clause in art 51(1), limitations to the right to private life and data protection are only admissible if such limitations are '…provided for by law and respect the essence of those rights and freedoms.'[584] Consequently, the Council of Europe Data Protection Convention as well as the EU Data Protection Directive and the General Data Protection Regulation contain clauses on lawful processing. Both the CoE Convention as well as the EU Directive state that data must be 'processed fairly and lawfully'[585], whereas within the scope of the GDPR, personal data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject' (art 5 1) (a)). The GDPR furthermore provides a list of legal bases for processing, inter alia by individual consent, contractual necessities or legal compliance.[586]

---

[582] ECHR, Art 8 (2).

[583] See e.g. *Leander v Sweden*, (n 434), paras 49-57, *Rotaru v Romania*, (n 418), paras 47-63.

[584] Charter of Fundamental Rights of the European Union, 18.12.2000, OJ 2000/C 364/1, Art 52(1).

[585] CoE Data Protection Convention, (n 299), Art 6, 1) a); Directive 95/46/EC (Data Protection Directive) (n 305), Art 5 a).

[586] Regulation (EU) 2016/679, (GDPR), (n 303), Art 6.

This essentially means that when data is processed within the European legal space, this processing requires a legal basis. The way in which such legal basis is established and evaluated depends on the processing actor: within a security and surveillance context, an adequate legal basis is established by clear and accessible laws, foreseeable for the individual and containing adequate safeguards. For private sector data processing, lawfulness requires consent or at least certain contractual or legitimate interest.[587]

It needs to be mentioned that targeted surveillance through police authorities is covered by a different data protection framework, especially regarding the EU. While all data processing for surveillance purposes of police authorities fall within the scope of the ECHR and the CoE Convention 108, such data processing falls within the scope of the EUCFR only when EU law is regulating aspects of such actions. This means that although police surveillance may fall outside the scope of, for example, the GDPR, there may be aspects that are still covered by the EUCFR, as for example seen in *Digital Rights Ireland*, where the CJEU declared the EU Directive obliging Member States to ensure the retention of telecommunications meta-data through the TSPs between 6-24 month invalid.[588] Even more so, as the Lisbon Treaty enabled the EU to act within the ordinary legislative procedure also in the area of criminal justice. Further EU documents that may be applicable to data protection within a policing context are specialized agreements for inter- European police cooperation as well as border protection: The Council Framework Decision on the protection of personal data in the areas of police and judicial cooperation or the Prüm Convention, but also the Schengen Information System II Decision, or the Europol Decisions to name just a few.[589] Additionally, the EU data protection reforms added the 2016 Directive on data

[587] Ibid.

[588] See Cases C‑293/12 and C‑594/12 *Digital Rights Ireland*, (n 324).

[589] See Council of the European Union, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, 60–71; Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, 1–11 (Prüm); Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, 63–84; Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ L 121/37, 15.5.2009, 37–66.

processing by law enforcement authorities, which will replace the Framework Decision in 2018.[590]

In addition to the applicability of ECHR and Convention 108, the Council of Europe also adopted a Police Recommendation that applies to collection, retention and dissemination of personal data for police purpose. The preamble of the Recommendation advises the implementation of the principles in the convention in national legal frameworks.

Lawfulness therewith can be listed as one of the core principles of data protection, just as any other action or measure interfering with fundamental rights in Europe. Public surveillance and data processing for surveillance purposes requires an adequate legal basis, and surveillance conducted through security and police organizations cannot be unlimited and without control.

Very recently, the EU data protection reform adopted the new GDPR, but also a Directive applicable to police and criminal procedures data processing. From the 6th of May 2018 onwards, EU Member States will be required to have implemented a new Directive regulating data processing in the context of police and security data processing.[591] This Directive, while very similar to the wording of the GDPR, requires compliance with the data protection principles, particularly lawful and fair processing, purpose specification, adequacy, and secure amongst some others.[592] The new Directive applies to all data processing by authorities for the purposes of '…the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security,'[593] provided the processing does not fall outside of the scope of Union Law.[594]

Therefore, it can be assumed that the certain general principles of data protecting apply to public sector surveillance, if not as clear cut rules than as interpretative guidance in

[590] Directive (EU) 2016/680 (n 303).

[591] See Directive (EU) 2016/680 (n 303).

[592] Ibid, Art 4.

[593] Ibid, Art 2 (1), Art 1 (1).

[594] For a further discussion of the applicability of EU law to surveillance cases see Section 3.2.3.4 below.

fundamental rights cases. The following section takes a closer look at the ECHR and the ECtHR's use of data protection in targeted surveillance cases.

3.1.2.3 Data Protection in the Scope of the ECHR

One of the first ECHR article 8 cases on privacy already dealt with the collection and retention of personal data. *X v UK*, as already discussed above, dealt with the taking of images of a participant at a political demonstration.[595] According to the applicant's statement, pictures of her were taken against her will by the Hampshire police. Additionally, the police allegedly added the applicant's personal information to the image, including name and birthdate in order to keep a file for future reference.[596] The Commission, at that time, did not discuss the issue of data collection, but focused on the taking of an image of the applicant and found that this did not fall into the scope of art 8 because the photographs were related to a public incident.[597]

Later, in 1979, the Commission decided on the admissibility of an application regarding the continuous surveillance and supervision of an applicant by the Vienna Security Police Department. The surveillance came to light in the course of criminal trials following an anti-fascist demonstration at the University of Vienna in which the applicant was acquitted of all charges. The collected data used in the proceedings, however, listed several whereabouts and participation in youth camps and political activities in which the applicant had been involved since he was seven years of age.[598] The applicant therefore claimed that this close supervision through the Vienna Security Police department interfered with his private life, freedom of movement and freedom of thought, conscience and religion as well as right to peaceful assembly.[599]

The Government responded that the data collected was purely '…administrative data … that might admit of a conclusion as to a political motivation...' of the applicant.[600] The Commission addressed the question whether the information collection by the police and their submission to the court in the criminal proceedings could be seen as

[595] See *X. v the United Kingdom*, (n 478).

[596] Ibid, 'Applicant's statement', para 1.

[597] Ibid, 'The Law', para 2.

[598] *X v Austria*, App no. 8170/78, Commission Decision, 04.05.1979, 146-147, paras 6, 7.

[599] Ibid, 147, para 7.

[600] Ibid, 149, para 13.

an interference with private life in article 8(1) ECHR, however, left the question unanswered as it regarded it justified within article 8(2) ECHR.[601] The Commission found the interference with the applicant's private life justified as being in accordance with the law, necessary in a democratic society for the prevention of crime, although it left open the question if that particular issue of data collection really fell into the scope of article 8.

Later on, however, it became clear that data protection would become included in the scope of private life in article 8 (1) ECHR.

In *X v Germany*, the Commission found that personal data held and recorded by the police and subsequently used in criminal proceedings constituted an issue of data protection, '…which comes within the broad scope of Article 8…'.[602] The case again concerned a police report used in proceedings which consisted of files containing the applicant's name as well as copies of personal documents. Furthermore, the file was retained for several years by the police. While the Court considered the use of such files in the court proceedings to be justified, it concluded that the existence of such files was a data protection issue and that data protection as such fell within the scope of article 8.[603]

As discussed in Section 2.3 above, states started to use data more and more efficiently for administrative purposes in the early days of information technology and it didn't take long until the ECtHR had to decide on cases regarding the scope of the ECHR and the practices of collection and retention of information about citizens.

In a complaint against a public census in the UK in 1981, the Commission regarded the fact that individuals were obliged to answer questions including personal information such as gender, marital status and birthplace amounted to a *prima facie* interference with article 8(1).[604] However, the Commission considered the application as manifestly ill-founded as interferences through such censuses were considered to be necessary in a democratic society for the purpose of economic well-being, due to a

[601] Ibid, 152, para 25.

[602] *X v Federal Republic of Germany*, App no. 8334/78, Commission Decision, 07.05.1981, p 107 para 2c

[603] Ibid, 106 para 2b.

[604] See *X v The United Kingdom* App no. 9702/82, Commission Decision 6.10.1982, 240.

common practice in the Member States and due to need for such information for state administrative purposes, provided that the information is kept secured and confidential.[605]

Although censuses as well as data bases for administrative purposes therefore fall into the scope of protection of article 8(1) ECHR and have been regarded as interfering with respective rights, such limitations are often found permissible pursuant to the requirements of legal basis, legitimate aim and necessity in a democratic society.

Police registers, investigations, government registries and censuses were therewith the first issues through which data protection entered European Convention of Human Rights case law. Furthermore, the ECtHR held already very early on that what is today often referred to as communications 'meta-data' clearly falls into the scope of article 8 and constitutes an interference into the right to private life:

In the 1984 Malone case, one of the two questions relating to audio and communications surveillance by the police in the course of criminal investigations against Mr Malone, a former antique dealer suspected of handling stolen goods, was that the police obtained such data from the telecommunication provider, the Post Office at that time.[606] The so called 'metering' of a phone involved a 'meter check printer', a device which registered all dialled numbers, as well as call time and duration, on a landline phone.[607] The Government in the Malone case made the claim, that because it had not directly monitored the content of communications but only communications meta-data, the retention of such data would not be an interference with private life pursuant to article 8 ECHR.

While the Court accepted a distinction between the direct interception of communication and the collection of meta-data, it did not follow the Government's

[605] Ibid, 240-241. With regard to public censuses and government data bases, it should be noted that the Commission has also held that it could not find reasons in the ECHR that would prohibit states to use personal social identity numbers, although data bases which retain such numbers fall into the realm of data protection as protected by article 8, See *Lundvall v Sweden*, App no. 10473/83, Decision (Commission), 11.12.1985, 130. Additionally, another Commission Decision on a public census was concluded similarly to the 1982 *X v UK* Decision, See *Anderberg v Sweden*, App no. 13906/88, Decision (Commission), 29.06. 1992 and *Grafström v Sweden,* App no. 16792/90, Commission Decisions 29.06.1992.

[606] See *Malone v The United Kingdom*, (n 418), paras 17, 23.

[607] Ibid, para 56.

view.[608] Such meta-data, according to the Court, '…contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone.'[609] Therewith, meta-data collection clearly constituted an interference with article 8 and because of insufficient legal bases for that practice, the Court found that the metering constituted a violation.[610]

The Malone case is remarkable in the sense that although the Court directly dealt with the collection and retention of personal communications data, it did not yet emphasize the data protection aspects of the case. Communications interception was therefore not seen as an issue of data protection, but an issue of interference with private life and correspondence. Nevertheless, it shows that data protection goes hand in hand with other issues in the ECHR and that the ECtHR already early on interpreted the scope of private life and correspondence rather wide.

Another remarkable aspect in the case was the concurring opinion of Judge Pettiti, who took a very strong argument in favour of a different, more data-protection centred perspective on the case. He especially emphasized the threats deriving from states and governments and their temptations to analyse and process the lives of European citizens and build profiles of individuals by employing more sophisticated technologies. Especially with a reference to computer processing Judge Pettiti emphasized with remarkable foresight the need to establish and ensure strong judicial review procedures addressing issues of over intrusive data collection, retention and processing.[611]

One of the most important early cases paving the way for the inclusion of data protection as a separate issue into the scope of protection of private life in article 8 was the 1987 *Leander* judgment.[612] The case concerned a carpenter who was employed as a naval museum technician in Sweden, however, later, his employment was revoked as he had not passed a required personnel security check. The naval museum was attached to a military base and parts of the museum were located in

[608] Ibid, para 84.

[609] Ibid.

[610] Ibid, para 87.

[611] Ibid, Concurring Opinion of Judge Pettiti.

[612] *Leander v Sweden*, (n 434).

access sensitive areas. Therefore, employment at the museum required passing a security clearance procedure.[613]

For this purpose, the National Police Board's Security Department held a secret police register containing information about the private lives of individuals. The applicant in the case could not obtain any detailed information about the information retained about him and contested the fact that he was classified as a 'security risk' and therewith excluded from being employed in the museum.[614]

The Court concluded without much elaboration that a secret police register containing personal data of individuals held by a government authority falls into the scope of article 8 and had to be regarded as an interference into Leander's private live.[615] Retention and release of personal information and the refusal to allow the applicant to review such data amounted to an interference with article 8.[616] The safeguards built into the Swedish personnel control system were, however, found to be sufficient to satisfy the requirement of article 8 (2) ECHR in the case.[617] Additionally, the ECtHR also held that it did not matter how or even if the collected and retained data was used: the mere retention already qualified as an interference.[618]

A core element of targeted public surveillance through technological systems is the existence of reference data bases. Reference data bases are important, because they enable the identification of individuals out of a pool of a vast variety of other individuals in public. For example, the employment of facial recognition technology in order to identify a suspect after a crime recorded on CCTV on a public place requires the existence of a reference data base containing facial profiles together with the name of a person, her residence, birthdate etc.

Data bases are therefore crucial to targeted public surveillance, and lie at the very core of operating targeted surveillance in a public place. Consequently, state authorities

[613] Ibid, paras 23-34.

[614] Ibid, para 47.

[615] Ibid, para 48.

[616] Ibid, para 48.

[617] Ibid, para 67.

[618] See also *Amann v Switzerland*, (n 503), para 69.

often operate data bases containing information going far beyond the mere registration of citizens for administrative purposes.

One of the more recent cases addressing fundamental rights compatibility of such an extensive surveillance data base was *Shimovolos v Russia*. The case addressed the retention of personal information about travel movements of the applicant in a so-called 'surveillance database' under the category of 'human rights activists' in the context of the May 2007 EU-Russia Summit in Samara.[619] The applicant's personal data was entered into the data base and he was detained by Russian authorities in order to prevent him from participating in political activities around that event. Consequently, the applicant complained that his registration in such a database merely for alleged public and political activities, leading to the detailed monitoring of his travel movements by the police, interfered with his rights guaranteed by article 8.[620] This interference, so the applicant, had not fulfilled the requirement of legality because the creation of the database was based on unpublished ministerial orders.[621]

The Court followed this argumentation and held that there has been a violation of article 8. Firstly, the creation of a government database containing movements of the applicant clearly fell into the scope of article 8(1) and constituted an interference.[622] Secondly, particularly the fact that the legal foundations of establishing the database were secret and that there was a lack of public scrutiny and adequate safeguards led the Court to conclude that the interference was not justified and failed the requirement of legality.[623]

Similarly, the ECtHR also found a violation of article 8 in a 2014 case concerning the registration of offenders in a database.[624] From the beginning, it was not contested in that case that the French system for processing recorded offences ('système de traitement des infractions constatées', STIC)[625] constituted an interference into private

[619] *Shimovolos v Russia*, (n 505), paras 6-9.

[620] Ibid, para 60.

[621] Ibid.

[622] Ibid, paras 64-66.

[623] Ibid, paras 69-71.

[624] *Brunet v France*, App no. 21010/10, Judgment (Court), 18.09.2014.

[625] Ibid, para 7.

life.[626] Furthermore, it was considered clear that this interference served a legitimate aim and that the legal basis was sufficient for the Court to see the legality criteria fulfilled.[627] However, particularly the lack of possibilities for the applicant to get the data deleted, paired with the long retention of the data for 20 years or more, led the Court to find that the state did overstep its margin of appreciation as the measure was not proportionate.[628]

Consequently, data bases and records about persons in the hand of security authorities require clear and strict compliance with the European fundamental rights systems, and particularly the ECtHR has exercised close scrutiny over government data collection and retention practices.

The collection and retention of personal data by state authorities therefore clearly falls into the scope of private life in article 8. However, do then all the pieces of information collected and processed by state authorities trigger article 8 ECHR?

It is clear today that databases containing personal information about individuals fall into the scope of article 8, however the ECtHR has also stressed the fact that this data should be of a certain quality in order to produce effects on privacy. In its early cases, especially *Friedl* and *Pec*k addressing visual surveillance[629] the Commission and the Court took into account the specific backgrounds of the retention, its context and specific implication and especially the way that the data was obtained.

What is remarkable in that context, is the move towards data protection arguments rather than establishing the interference into private life through public surveillance *per se* in the *Peck* case. While referring to *Lupker, Friedl* and *Herbecq*[630], all cases in which the court did not find that visual public surveillance constituted an interference into the rights established in art 8, the ECtHR stressed that the fact that the applicant's image data in *Peck v UK* were recorded and disseminated constituted a serious interference with private life.[631] This finding relied heavily in the fact that personal

[626] Ibid, para 31.

[627] Ibid, paras 32.

[628] Ibid, paras 33-45.

[629] *Friedl v Austria*, (n 482), paras 49-51; *Peck v The United Kingdom*, (n 258), para 59.

[630] *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421).

[631] See *Peck v The United Kingdom*, (n 258), paras 62-63.

data was disclosed and the court also stressed that the retention of personal data, even from a public context, in that case went beyond the mere '…exposure to a passer-by or to security observation … and to a degree surpassing that which the applicant could possibly have foreseen…'[632] and therewith has to be regarded as establishing an interference.

A similar line, but even a much stronger data protection perspective was taken up by the Court in *Amann v Switzerland* and in *P.G and J.H. v UK*: in the latter recording of audio data in a police cell and subsequent processing of such data was considered an interference with article 8 because it constituted a permanent record. In the former, phone line tapping led to the creation and retention of data in a file, which was subsequently considered to be an interference.[633] Similarly, the collection and retention of data in repositories by security and intelligence services constituted interference with private life in article 8, even without employing covert data gathering.[634] In *Amann v Switzerland* the ECtHR also invoked the 1981 Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and particularly its definition of personal data as '…any information relating to an identified or identifiable individual' in article 2.

Another essential case in which the Court addressed issues resulting from surveillance and data-collection is the 2000 *Rotaru v Romania* Judgment.[635] The applicant proceeded against the Romanian state authorities in order to get certain rights fulfilled which he was seeking as a person persecuted by the former communist regime in Romania.[636] During those proceeding, the state employed (false) information about the applicant as evidence which were obtained by the Securitate, communist Romania's former Department of State Security and which were transferred into the possession of the Romanian Intelligence Service (RIS). The fact that the RIS was

[632] Ibid, para 62.

[633] *Amann v Switzerland*, (n 503), paras 66, 67; *P.G. and J.H. v the United Kingdom*, (n 500), paras 59-60.

[634] *Rotaru v Romania*, (n 418), paras 43–44.

[635] Ibid.

[636] Ibid, paras 10, 30.

holding information about the applicant which were partially false was considered a violation of article 8 ECHR as such practices did not fulfil the legality requirement.[637]

The Court referred to *Leander v Sweden* when finding that secret government registers as well as the transfer of personal information fell within the scope of article 8 ECHR and cited *Amann v Switzerland* to re-emphasize the relevance of the 1981 Council of Europe Data Protection Convention.[638] While the Government claimed that certain information about the applicant, which related to the applicant's engagement in political activities and publications, would not fall within the scope of private life of article 8 as they would relate to the applicant's public life and therefore *per se* did constitute public information,[639] the Court explicitly rejected that view. In fact, so the Court

> …public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.[640]

The ECtHR followed up on such interpretations in its *P.G. and J.H. v UK* Judgment in which it, as discussed above, stated that privacy rights can very well be applicable within a public sphere.[641] This is essential for the analyses of data collection and retention of data from public areas: once data collection, retention and processing becomes systematic, it will be difficult to exclude such data from the scope of protection of private life in article 8 ECHR.

Subsequently, data protection plays an increasingly important role as a legal argument in the Court's findings. The right to private live and subsequently a right to data protection as included in the scope of article 8(1) ECHR, however, are not absolute rights. Their interference can be justified by applying the Convention's permissible limitations tests.

Data protection within the ECHR framework also addresses several further aspects relating to the nature and way of data collection and processing, some of which are of

---

[637] Ibid, paras 62, 63.

[638] Ibid, para 43; *Leander v Sweden*, (n 434), para 48, *Amann v Switzerland*, (n 503), para 65.

[639] See *Rotaru v Romania*, (n 418), para 42.

[640] Ibid, para 43.

[641] See *P.G. and J.H. v the United Kingdom*, (n 500), para 56.

particular importance when it comes to sophisticated surveillance systems controlling public spaces.

Before discussing some of the legal issues arising from data of a certain quality and type with special relevance for public surveillance, such as for example biometrical data, this section concludes by discussing another landmark judgment on data protection within the Council of Europe framework: the 2008 *S and Marper v UK* judgment.[642]

The Grand Chamber judgment in 2008 addressed the practice of unlimited retention of fingerprints, DNA profiles and cell samples of offenders and suspects in the UK. Those records were taken from suspects and retained even if the suspects were not convicted. The applicants, which were both arrested but later acquitted, submitted that the unlimited retention of DNA profiles, fingerprints and cellular samples violated their right to private life.[643] The Grand Chamber re-emphasized the importance of data protection as an inherent element in article 8 of the ECHR:

> The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (…). The subsequent use of the stored information has no bearing on that finding (…). However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (…).[644]

Subsequently, the Grand Chamber held that both finger prints as well as DNA profiles and cellular samples raised issues under article 8 ECHR.[645] The unlimited retention of this personal data, including the retention of data from people never convicted of any crime, clearly overstepped the margin of appreciation the state enjoyed and was therefore an un-proportionate interference with the applicants' private lives and a violation of article 8 ECHR.[646] This view was reconfirmed in *M.K. v France*, where

[642] See *S and Marper v the United Kingdom*, App nos. 30562/04, 30566/04, Judgment (Grand Chamber) 04.12.2008.

[643] Ibid, paras 60, 87.

[644] Ibid, para 67.

[645] Ibid, paras 77, 86.

[646] Ibid, paras 125,126.

the retention of fingerprints of later acquitted suspects in a computerized police database was also seen as a violation.[647]

While *S and Marper* concerned personal data of a certain form, namely fingerprints, DNA profiles and cell samples, the argumentation of the case outlines a specific set of issues which are of special concern for the ECtHR regarding personal data.

Firstly, as mentioned above, the mere retention of personal data raises issues of private life, however, the Court takes into consideration how and why this information was obtained and retained, and what the information as such looks like.[648] Furthermore, the Court also emphasized the importance of the nature and way of processing such data and what consequences such processing may have on an individual. This means that the Court recognizes several core principles of data protection as a fundamental right that is triggered once any kind of personal information is stored, which the ECtHR explicitly derived from legal instruments of the Council of Europe as well as the 'law and practice of the other Contracting States.'[649] Core principles of data protection hence can be derived also from the Council of Europe Data Protection Convention, which lays out particular basic principles regarding the quality of data (article 5) special categories of data such as health or origin (article 6), data security and additional safeguards (arts 7,8).[650] In the *S and Marper* judgment, the ECtHR applied those principles in a consistent way and therewith interprets the Council of Europe data protection framework as an important source of European fundamental rights.

Following the jurisprudence of the ECtHR, fundamental right will need to be interpreted in connection with existing data protection frameworks when testing a possible fundamental rights and data protection compliance of public surveillance systems. The following section will now address a couple of specific issues in connection with data protection mechanisms in Europe, with special focus on the ECtHR. The analysis with references to the surveillance scenario particularly

[647] *M.K. v France*, App no. 19522/09, Judgment (Court), 18.04.2013.

[648] See *S and Marper v the United Kingdom*, (n 642), para 67.

[649] Ibid, paras 106, 107.

[650] CoE Data Protection Convention, (n 299).

addresses issues of the systematic collection of data, the quality of urban surveillance data as well as the retention of data.

3.1.2.4 Data Protection Issues in the Scenario

Public surveillance, as seen within the scenario, is essentially about the collection of information on individuals. Such information can take many shapes. Visual data, for example, in the form of a photograph, can be regarded as personal data, although the ECtHR addressed the use of photographs in police records long before data-protection became an issue within the ECHR. Data protection aspects are therefore difficult to distinguish from surveillance issues brought up under the Convention. Visual surveillance of a public place can both be an issue falling under the scope of protection of private life, or an issue of data protection, once, as argued in *Peck*, a 'systematic record comes into existence'.[651]

With digitization and advancement of technology, everything digital becomes data that will be processed in more or less sophisticated ways. It is therefore difficult today to draw a clear distinction between data protection and privacy as separate issues deriving from article 8 ECHR. Especially regarding government administered databanks, repositories and records, data protection is a necessary element in analysing fundamental rights issues in that area. This section addresses specific requirements for public surveillance deriving from data protection and the analyses of case law of the ECtHR above.

Targeted surveillance in a public context employing electronic surveillance mechanisms has become unthinkable without personal data collection. When police officers follow a suspect via a video surveillance system, they will watch screens on which the suspect is visible to them and as they know the location and direction of that camera, they know where the suspect is.

As discussed above, the mere watching of an individual via electronic means does not *prima facie* raise issues under the Convention, in the same way that police following a suspect by foot would not *per se* be regarded as an interference.[652] After all, the

[651] *Peck v The United Kingdom*, (n 258).

[652] See *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

collected information appears as part of the public domain and therefore in principle visible to all. Additionally, such information does not directly concern the individual's private activities and the individual has a different expectation of privacy. This view, however, relies on an understanding of privacy deriving from liberal individualism, in which the exercise and enjoyment of rights becomes connected with individual expectations and choices. Ultimately, it appears as a choice to enter into the public sphere.

Contrary to such a perspective appear two other arguments which play a crucial role in this study: on the one hand, Courts can rely on data protection to find fundamental rights problems. On the other hand, Courts can employ dignity and personality to build up an argument that understands privacy as an essential element in a free and democratic society and in that sense as a communal element of societies. Both are especially prone to address issues of systematic surveillance and systematic data collection.

In *P.G. and J.H.*, as cited several times above, the Court stated that privacy life considerations rise at the moment '…once any systematic or permanent record comes into existence of such material from the public domain.'[653] This means that if the surveilling police officers wrote the name of the abovementioned suspect on a sheet of paper, together with the time and place of the whereabouts of the person, private life considerations would arise.

The first conclusion which can be drawn form this is that data protection is a powerful argument within the ECHR, one that is more likely to establish an interference than the surveillance action as such. Data collection practices therefore can be distinguished into several important elements addressed by the ECtHR: systematic collection, quality of data and the retention of data.

3.1.2.4.1 Systematic Collection

Systematic collection as such has two distinct features in the context of the surveillance scenario. Firstly, targeted surveillance employs and relies on information which has been collected and retained previously. Secondly, the targeted surveillance operation produces information which will most likely be retained. For example,

[653] *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

employing facial recognition technology in Helberg in order to follow a suspect via video surveillance requires the existence of a facial profile database. In that sense, once an individual is targeted, the reason for targeting that particular person possibly derive already from the combination of a series of previously collected information sets stored in some database. The existence of such databases containing information of individuals has been found to fall within the scope of private life and constitute and interference regardless of the use or sensitivity of the information,[654] when collected from a public context,[655] or regardless if the gathering method is covert or overt.[656]

It is important to emphasize, that the ECtHR has particularly stated in *P.G. and J.H.* and in the *Rotaru* judgment that public information as well as information gathered from a public domain can very well constitute an interference with private life.[657]. Consequently, databases used for public surveillance purposes, or created from public surveillance, need adequate justifications in order to comply with fundamental rights set out in the ECHR.

One of the most relevant issues in relation to sophisticated targeted surveillance in public places is the practice of profiling – a consequence of systematic collection and processing. Profiled data in itself then can be re-used for more data collection. For example, a facial profile reference database can be used for locating a suspect within a wide public area employing facial recognition technology.

The slippery slopes of systematic data collection are obvious and are one of the reasons, why the ECtHR laid special emphasis on the problem of the creation of systematic data gathering and storing from public places. After all, while for example only one piece of information about a person gathered from a public place might not be considered to be heavily intrusive - for example that a person bought a can of beer at a supermarket – the same information gathered over time – the same person buying a can of beer at the same supermarket 8 times a day – will have to be considered more

[654] See *Amann v Switzerland*, (n 503), paras 65-67.

[655] See *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

[656] *Rotaru v Romania*, (n 418), paras 43-44, *Leander v Sweden*, (n 434), para 48.

[657] Including '…material from the public domain', see *P.G. and J.H. v the United Kingdom*, (n 500), para 57; as well as '…'…public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities.' See *Rotaru v Romania*, (n 418), para 43.

intrusive as the connection of information becomes data with health relevance. In fact, not only does systematic data collection play a crucial role in targeted surveillance compliance with fundamental rights, but also the nature and categories of data, elements that can be summarized as data quality.

3.1.2.4.2 Data Quality

For the data collected within a public surveillance system to fall within the scope of protection of article 8 ECHR, it needs to be personal data as defined in the CoE Data Protection Convention.[658]

The Court has however considered various types of data and the level of intrusiveness which comes with them. In *S and Marper v UK*, for example, the Court distinguished between fingerprints on the one side and DNA profiles and cell samples on the others, whereas the latter were considered more intrusive than the former, although the collection of both forms of data was considered an interference due to the fact that records were created.[659] Fingerprints had to be regarded as external features enabling individual identification and were therefore considered personal data within the context of the ECHR.[660] Earlier, though, the Commission found that the taking of fingerprints and photos of a criminal suspect after arrest did not amount to an interference with the applicant's right to private life, because the

> …information retained (…) was not of such a character that it could have adversely affected the applicant any more significantly than the publicly known fact that he had been charged with, but acquitted of, certain charges.[661]

This view was refuted in *S and Marper*, when the Court lifted fingerprints onto the same level of protection as visual data and audio recordings. The government argued that fingerprints were '…constituted neutral, objective and irrefutable material and, unlike photographs, were unintelligible to the untutored eye and without a comparator fingerprint.'[662] The Court, although principally confirming this argument, found an

[658] Art 2(a) CoE Data Protection Convention, (n 299). The ECtHR has recognized this definition in see e.g. in *Amann v Switzerland*, (n 503), para 65.

[659] *S and Marper v the United Kingdom*, (n 642), paras 70-86.

[660] Ibid, paras 78-86.

[661] *Kinnunen v Finland*, App no. 24950/94, Decision (Commission) 15.05.1996, para 2(ii).

[662] *S and Marper v the United Kingdom*, (n 642), para 84.

interference with private life because fingerprints can be used to identify individuals in many ways, and therefore essentially constitute personal data.[663]

Furthermore, data quality also had a significant influence on the ECtHR's assessment as to whether the interference can be justified. Special categories of data, as defined in article 6 of the 1981 Data Protection Convention, require strict legal protection mechanisms in order to be processed. This applies to data concerning origin, political opinion, religion, health, sexual life and criminal convictions and the ECtHR has included DNA information and profiles into such sensitive data.[664]

Consequently, apart from systematic collection mechanisms, the specific nature of data can play a role in the fundamental rights assessment, and particularly bioidentifiers such as DNA and biometric data were clear concerns for the Court in the *S and Marper* case.

Urban surveillance potentially produces a variety of different data. Most relevant in that context is location data, communication meta-data, data about an individual's appearance, and biometric data that can be used for identification purposes. Generally, the systematic collection of information from individuals in public spaces might allow the linking wide varieties of information in order to gather additional data about a person's whereabouts, behaviour or other relevant information. Data analytics can allow for individual profiling in an advanced way, and can create specifically sensitive information even without the direct collection of such information. For example, communication data analytics might reveal sensitive health information, when suspects frequently call or visit certain medical specialists, or religious beliefs when they frequently visit places of worship. Systematic profiling from data gathered from urban surveillance might therefore fall into distinct categories that enjoy special protection.

In that sense, data quality or the nature of data can also change once a temporal aspect is added: Data from the past and data gathered over a longer period of time are more likely to raise issues under the ECHR, especially when a systematic element is added. This was also emphasized by the Grand Chamber in *Rotaru v Romania*:

[663] Ibid, para 85.

[664] Ibid, paras 72, 76, 103.

> …public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.[665]

Questions of the nature, scope and especially duration of data retention are therefore another relevant element when assessing the compliance of surveillance systems.

3.1.2.4.3 Data Retention

A core purpose of targeted surveillance operations is the gathering of information about a specific individual. Police authorities keep and preserve specific information for a certain purpose, which can reach from retaining very isolated and specific information about an individual for the purpose of a criminal procedure to the retention of complete personal profiles including for example biometrical data, whereabouts, contacts with other individuals, political activities or communications to name just a view.

The ECtHR has been rather sceptical about excessive practices of data retention, especially when the information stored is of a high quality and the retention period extends beyond a certain threshold. The Court has given special weight to elements such as the possible future use and effects of such retained data on individuals. In S and Marper, for example, the Court emphasized that it

> …cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.[666]

Underlying to such an argument is the concern that temporally unlimited retention could have serious negative effects on individuals in the future, for example due to technological advancements or possible further use and analytics for exiting datasets.

This aspect is especially relevant when it comes to public surveillance practices. For example, a digital photo about a person stored in an administrative register could be used to create a digital facial profile with which that person's location could be found employing an automated facial recognition system. Retaining vast facial profile databases indefinitely would hence enable a theoretically unlimited automated

[665] *Rotaru v Romania*, (n 418), para 43

[666] *S and Marper v the United Kingdom*, (n 642), para 71.

surveillance of large areas such as whole cities, depending on the infrastructure of sensors.

While it is clear that data retention as such does interfere with the rights guaranteed by article 8 ECHR, unlimited storage is even more difficult to justify. Already the 1981 CoE Data Protection Convention clearly states in article 5 (e):

> Personal data undergoing automatic processing shall be… preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[667]

Consequently, the ECtHR recognized that '[t]he core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage (…).'[668] In *Brunet v France*, the Court stressed that while the duration of retaining information in an offender database of 20 years was limited, there was not a factual possibility to request his data to be deleted, leading to the conclusion that the state overstepped its boundaries.[669] Similarly, in a case concerning the registration of fingerprints for 25 years as a consequence of a minor offence (book theft) and no factual possibilities for the applicant to request deletion was also found to be a violation of article 8 because France overstepped its margin of appreciation.[670]

With this, the ECtHR clearly recognizes one of the core principles of data protection: namely that data retention should in principle be temporarily limited and purpose specific, especially once the data is of a certain quality. On the other hand, there are ways in which the retention period of data can be very lengthy. In other cases concerning registration of persons in a sex offender data base in France, a data retention of 30 years was not considered disproportionate to the pursued aim of preventing crime, combating repetition of sexual crimes and enabling a better identification of sexual offenders.[671] This was especially the case because there were adequate mechanisms in place to legally challenge the retention of data as well as the

[667] CoE Data Protection Convention, (n 299).

[668] *S and Marper v the United Kingdom*, (n 642), para 107.

[669] *Brunet v France*, (n 624).

[670] See *M.K. v France*, (n 647), paras 37-47.

[671] *Gardel v France*, App no. 16428/05, Judgment (Court) 17.12.2009, paras 63-71.

given opportunity to apply for earlier deletion of personal information from the sex offender database.[672]

It can be concluded that personal data, including biometric information or bioidentifiers can legitimately be stored for a very long period of time, provided that such retention passes the legitimacy test of legality, proportionality and legitimate aim. This has been repeatedly confirmed regarding DNA profiles as well as cell samples in the cases of convicts,[673] but has been found to cross the line of proportionality once of a too general nature. In case of sexual offenders, the Court confirmed even the permissibility of a preventive nature of the measures. Nevertheless, once the retention becomes too broad, too long, too unspecified and once it lacks adequate safeguard mechanisms, large-scale data retention will be difficult to justify from the fundamental rights perspective of the ECHR.

3.1.3 Conclusion

This section discussed individually focused and therewith targeted surveillance in public places. This was approached from two different perspectives: on the one hand through legal arguments deriving from a right to privacy, and on the other hand through the lenses of data protection. Both, data protection, as well as privacy, derive from fundamental rights frameworks protecting a right to private life, the inviolability of the home and the privacy of communications.

Generally, targeted individual surveillance does not appear as a new problem. In fact, the surveillance of individuals in both a private and a public context, as well as the interception of communications form a rather classic body of fundamental rights case law in the ECHR.

The right to privacy and its application in public spaces appear in two lines of arguments. Firstly, privacy in public was understood in relation to the background and setting of the individual: in a public place, or as a participant in a public event, it

[672] Ibid, paras 68, 69. See also *B.B. v France*, App no. 5335/06, Judgment (Court), 17.12.2009; and *M.B. v France*, App no. 22115/06, Judgment (Court), 17.12.2009. See also: *J.P.D. v France,* App no. 55432/10. Decision (Court), 16.09.2014.

[673] See e.g. *Peruzzo and Martens v Germany*, App nos. 7841/08, 57900/12, Decision (Court), 04.06.2013.

appears that privacy was mostly evaluated by the ECtHR in connection with an individual's expectation, at least in its early case law. Pure observation, the taking of images or police surveillance were either not placed within the scope of protection of privacy of the ECHR or the interferences were easily justifiable. In that sense, the early case law of the ECtHR addressing visual surveillance appear to have a strong connection with the legitimate expectation arguments: it was within the realm of free individuals to expect and therewith adjust their behaviour in surveilled public contexts.

The second line of argument discussed in this section, was the reasons when public surveillance was regarded as a strong interference with individual privacy, namely when it could not be expected from the individual to expect surveillance. Cases addressing secret surveillance or an unknown manipulation or sophistication of surveillance technologies appear to have a stronger interference with individual privacy than if surveillance occurs in overt, known and expectable situations. Again, a legitimate expectation argument appeared at least to some extend in the egal assessments.

With the emergence of data protection, a different approach to address surveillance issues emerges. It is not the surveillance practice as such which is seen as a clear interference with individual rights, but the collection of information about individuals. With this, the understanding of individual privacy in public places shifts from a legitimate expectation approach towards informational privacy. The collection of information in itself raises fundamental rights issues.

The second part of this section therefore discussed data protection as a legal argument addressing public surveillance in the scenario.

Taken together, it becomes clear that the sophisticated surveillance systems in Helberg have to be considered as a serious interference with individual fundamental rights. This is due to their unforeseeable capabilities on the one hand, and their massive and systematic data processing on the other. Those capabilities pose serious threats to an individual's right to privacy and data protection in Europe. Furthermore, the technology enables targeting individuals in a systematic way, placing surveillance between individually targeted surveillance and mass surveillance. This has a strong effect on the assessment of permissible limitations.

Articulating data protection as a decisive factor for establishing rights interferences, yet has another effect: the processing of personal data somehow bridges the gap between individual surveillance and systematic mass surveillance.

Privacy based on legitimate expectation is applied more easily on individual surveillance than on mass surveillance. Data protection, on the other hand, can function as an argument without focusing on a single individual's expectations and therewith might be a better legal argument for addressing mass- and systematic surveillance.

Consequently, the next section will turn from targeted individual surveillance towards an analysis of legal arguments addressing the mass surveillance of public places.

3.2 Mass Surveillance

Mass surveillance is a term that has recently gained significant importance in legal debates around the world. One of the reasons for this were a series of 'revelations' about secret US intelligence programmes, showing the existence of a variety of tools and surveillance capabilities which were previously only speculated about.[674] Those large-scale surveillance practices showed the attempt by security and intelligence agencies to gain access, retain and analyse massive amounts of communications data in order to process and filter information about individuals.

The existence of 'big data' and the availability of large 'treasure troves' of data that can be used for many purposes is nothing new in the digital age. Technical developments have led to the fact that everyday life is accompanied by vast streams of information transferred through expanding and highly integrated networks. Phenomena like this have been described as the rise of ubiquitous computing and as the 'internet of things'.[675] Networks, data and integrated sensors, have become functional elements in modern societies. Today, businesses, administrations and governments alike operate with collection, retention, and analytics of vast amounts of data.

In a similar way, modern urban environments have become important sources for such information. Traffic, pollution, or customer locations are only a few examples of data flows that can play an important role in improving business profit or operating the complexities of modern urban spaces and they play an important role in urban public mass surveillance.

Mass surveillance in urban public spaces comes with many promises but also threats. On the one hand, the surveillance of public places promises to make them safer, fight petty crime, unwanted behaviours and also serious crimes or terrorism. Prevention and protection, but also repressive action and investigation allegedly become easier once public spaces are monitored. On the other hand, fears of a total control of public

[674] See Greenwald G, *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state* (Metropolitan Books/Henry Holt 2014).

[675] See e.g. Rouvroy A, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence' (2008) 2 Studies in Ethics, Law and Technology 1, Wright D and Others (eds), *Safeguards in a World of Ambient Intelligence* (Springer 2010).

spaces, the loss of freedom, the chilling-effects and a forced change of behaviour in public can deliver valid arguments against wide scale public space surveillance.

Mass surveillance, for the purpose of this study shall mean 'the subjection of a population or significant component of a group to indiscriminate monitoring,'[676] a definition adapted from Privacy International. Consequently, '[a]ny system that generates and collects data on individuals without attempting to limit the dataset to well-defined targeted individuals is a form of mass surveillance.'[677] In that sense, this study employs a definition of 'mass surveillance' on a rather low threshold. The line between mass surveillance and targeted surveillance could very well be drawn on a higher level, for example where potentially legitimate surveillance of certain groups or populations becomes illegitimate due to the mere expansion of scale. Bigo and others, for example, rightly argue that while surveillance of categorized groups has always been part of liberal societies, it is precisely the scale and the purposes of group surveillance which distinguishes police states from democratic ones.[678] This study, however, sets the threshold for mass surveillance lower: In accordance with the definition above, surveillance can be regarded as mass surveillance once it reaches beyond the targeted surveillance of single individual or very small group for a narrowly defined purpose.

Once mass surveillance is defined in this way, it is evident that public surveillance systems and capabilities in the scenario are mass surveillance systems. Already a simple video surveillance system qualifies as a mass surveillance system for the purpose of this study because it monitors indiscriminately and without pre-defined target.

This section analyses a couple of distinct legal issues of different categories that come with wide scale and systematic public mass-surveillance. Naturally, some of those

[676] Privacy International: 'What is mass surveillance?' https://www.privacyinternational.org/node/52 accessed 16 October 2016.

[677] Ibid.

[678] Bigo D and others, 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law', CEPS Paper in Liberty and Security in Europe, No. 61/ November 2013, https://ssrn.com/abstract=2360473 accessed 10 January 2017, 6.

issues fall into the realm of data protection law and some are better grasped from a privacy perspective.

3.2.1 Distinguishing Mass Surveillance from Targeted Surveillance

This study approaches mass-surveillance and targeted surveillance as distinct issues deriving from the scenario. This distinction is chosen, because there are separate issues from the perspective of a fundamental rights analyses. Mass surveillance is, by its very nature, different than targeted individual surveillance. The distinction is clear on first sight: While targeted surveillance operates on the basis of a known individual and a specific reason for the surveillance, mass-surveillance operates on the bases of collecting and analysing vast amounts of information on many individuals. Mass surveillance naturally will have similar components as targeted surveillance, however it comes with a wider scope.

Addressing the urban public surveillance scenario as a mass-surveillance issue appears more natural than as a targeted surveillance problem. It goes without saying that public surveillance systems are usually designed as mass surveillance systems, simply because they will inevitably be directed at every person sojourning in the respective area. The more proliferated and the more capable surveillance systems become, the more they become mass-surveillance systems.

In order to legally grasp urban surveillance beyond the individual perspective, this section tackles some legal issues particularly related to mass surveillance questions, although, of course, they are directly related to individual surveillance as such. After all, one of the central abilities of sophisticated mass surveillance in urban spaces is that a system build for general public surveillance can easily be transformed into a highly efficient targeted surveillance system.

The theft of a purse on the main square of Helberg can serve as a good example of a petty crime within an urban public space surveillance context. The surveillance system in Helberg might be able to automatically identify pickpocketing by recognizing certain specific patterns on a video stream. For this, video analytical software would continuously analyse all video material and once as pattern is recognized, the system could automatically target the alleged perpetrator.

Once the security system targets the perpetrator, other mechanisms can locate the place of theft, track the location and movement of the perpetrator and identify the perpetrator through facial recognition software. Theoretically some, or even all, of those processes might happen fully automatically before a human operator of the security system is notified. Later on, after the perpetrator has been identified and arrested, the surveillance material can be used as evidence in a criminal trial.

This example shows, that mass surveillance of public places becomes a targeted surveillance issue the moment an identifiable individual is targeted at which time the borders between untargeted mass surveillance and targeted individual surveillance become blurred.

Such public surveillance, however, starts off as general surveillance rather than as targeted surveillance. This means, that in the first place, every individual in the public space is automatically and indiscriminately a subject of surveillance. A video camera captures everybody passing by in its field of direction in the same way that other surveillance sensors capture data indiscriminately.

At first sight, the relationship between mass-surveillance and fundamental rights appears rather unspectacular. In fact, it is in many ways undisputed that targeted surveillance in the same way as mass surveillance falls within the scope of a right to privacy in international fundamental rights protection. Yet, there are some issues at stake which make it important to distinguish fundamental rights protection of surveillance from similar protection from mass-surveillance.

Firstly, as discussed in the previous section, individual and targeted surveillance clearly interferes with a single person's fundamental right. A citizen in Helberg, for example, as a natural person, enjoys respective fundamental rights, including access to legal remedies. In mass-surveillance cases, however, accessibility to remedies tends to be more complex. Groups of natural persons, organizations or institutions and even societies as a whole have a more complicated standing from a fundamental rights perspective. Additionally, it might be more difficult for individuals to claim a violation of their right to privacy because of a lack of evidence or legal standing of having been concretely subject to rights interferences especially when mass-surveillance practices are secret.

Secondly, the legal claim challenging mass surveillance requires a different and more abstract legal argumentation than a claim against individual surveillance. This section shows that while individual claims can easily be based on individual freedom and liberty, mass-surveillance claims require the construction of a common good or a collective end. Judicial decisions in individual surveillance claims require balancing individual rights against collective interests, in mass surveillance cases, this balancing much more requires the choice of an important good or end for society as a whole. This is, once again, heavily dependent on the actual conceptualization of privacy. A dignity-based or communal privacy approach conceptually enables the articulation of common goods and ends, while an individual liberty centred approach comes with a stronger focus on the individual. This section, which employs European fundamental rights case law, shows some of the problems that fundamental rights arguments face when mass-surveillance is at stake.

3.2.2 Mass Surveillance and Privacy

Within recent years, the ECHR has addressed a variety of cases concerning surveillance, both targeted individual as well as systematic mass surveillance. While targeted surveillance has been analysed in Section 3.1, this part shall now look in more detail at possible responses to mass surveillance in public places from the perspective of the ECtHR.

There are a number of classificatory problems when analysing the European Convention on Human Rights in terms of targeted individual and mass surveillance.

The first is that the ECtHR has dealt with a variety of surveillance technologies, some of which can be categorized as technologies for individual surveillance, some of which as more generally mass surveillance systems. While for example a sophisticated camera surveillance system is more a mass surveillance instrument than an instrument of individual surveillance, a wiretapping system which is only directed at a specific person is more suitable to be classified as a tool for individual surveillance. The technology employed for surveillance and its specific features and capabilities consequently play a significant role in the legal assessment of surveillance. On top of the technology as such, the Court has been using data protection arguments in order

to address surveillance, posing a specific form of fundamental rights argumentation.[679] The protection of individual rights relating to the collection of personal information therewith functions as a bridging mechanism between targeted individual surveillance and mass surveillance.

The second core issues in addressing fundamental rights protection in mass-surveillance cases is the accessibility of, and legal standing before a fundamental rights Court. Admission of a mass surveillance case and establishing an interference into a right to privacy require different legal argumentation than in a case addressing targeted surveillance.

3.2.2.1 Admissibility and Victim Status in ECHR Mass Surveillance Cases

The legal issue that arises from the classification of surveillance into targeted individual and mass surveillance is related to the nature and construction of fundamental rights protection in the ECHR *per se*. After all, the ECHR requires an individual or an organization to be a direct victim of a rights violation in article 34 ECHR in order for the case to be admissible.[680] This may be less straightforward when considering complaints against mass surveillance systems, particularly where the systems as such are kept at least partly secret and where the complainant belongs to a group of person only potentially affected by a surveillance regime. The massive interception of telephone calls or the bulk collection and retention of personal data could create a situation where it might be difficult to determine if a complainant is a direct victim.

The Court, however, has interpreted this admissibility criterion rather broadly. Already in the 1978 *Klass* case, the Court accepted that individuals can claim to be the victim of a violation '…by the mere existence of secret measures or of legislation

[679] As discussed in the previous section, the simple fact that personal information is recorded in a systematic way raises issued under the ECHR. See *Leander v Sweden*, (n 434), and *S and Marper v the United Kingdom*, (n 642), para 67.

[680] Article 37 ECHR states that application can be submitted '…from any person, nongovernmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto.' This has been interpreted rather broadly and includes international organizations, churches, trade unions and NGOs amongst others. See Cameron I, *An Introduction to the European Convention on Human Rights* (5th ed, Iustus 2006), 56.

permitting secret measures, without having to allege that such measures were in fact applied to him.'[681] The Court considered that the existence of a systematic surveillance mechanism, allowing for interception of telecommunications and the mail of citizens in Germany in itself allowed for the applicants to claim to be victims without having to be directly subject to such surveillance themselves.[682]

Similarly in *Malone*, where the Commission and the Court confirmed that the mere existence of a law and practice of surveillance and the fact that the applicant belonged to a group of person potentially affected by communication interception were sufficient for the applicant to be regarded as a victim and to establish an interference.[683] With this, the Court as well as the Commission addressed potential admissibility problems for applicants in case they cannot directly prove having being individually targeted and affected by state surveillance. The admissibility of mass surveillance cases as such therefore does not necessarily require direct proof of the applicant being subject to targeted surveillance, because the mere

> …menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8.[684]

On the one hand, the Convention Organs have therewith addressed mass surveillance systems as *per se* problematic for fundamental rights and given applicants a rather easy way to be accepted as victims. On the other hand, however, the ECtHR has also sometimes held that the establishment of a status as victim requires at least a certain likelihood of being affected by surveillance measures. In this regard, the burden of proof can also be with the applicant in some cases, in order to establish what the Commission called a 'reasonable likelihood' to be subject to surveillance measures.[685] According to this interpretation, the applicant is required to show that she or he was affected by surveillance or information collection with a 'reasonable likelihood'.

---

[681] *Klass and Others v Germany*, (n 423), para 34.

[682] Ibid, paras 37, 38.

[683] Ibid, para 64.

[684] Ibid, para 37.

[685] See *Hilton v The United Kingdom*, App no. 12015/86 (Commission Decision), 06.07.1988, 'the Law' 1.2.B.

Commission and Court employed this test in a variety of cases that were distinguishable from *Klass v Germany*.

For example, in *Hilton v UK*, a case addressing security checks for employment reasons, the Commission found no interference with the applicant's rights enshrined in article 8 ECHR because the applicant failed to show that there was '…at least a reasonable likelihood that the Secret Service has compiled and continues to retain personal information about her.'[686] On closer reading, the Commission particularly interpreted the plausibility of the applicant being subject to secret surveillance and data collection due to the fact that she did not belong to a 'category of persons' of possible interest.[687] Such categories have been found to include for example persons with political and party activities.[688]

In *Esbester v UK*, a case concerning security checks for employment reasons – the applicant was refused a position in the Central Office of Information. The applicant claimed that information concerning his private life were collected, retained and disclosed by state security organs, however, neither did the Government confirm such an allegation nor did the applicant have any detailed insights into how the security assessment leading to the employment refusal was carried out and what information had been used.[689] The Commission, albeit declaring the application inadmissible, found that the fact of such a security check being conducted showed with reasonable likelihood that some security service compiled some personal information concerning the applicant's private life.[690] Similarly in the case *Christie v UK*, in which the applicant complained against alleged GCHQ interception of Telex communication with East European trade unions, the Commission confirmed there was a reasonable likelihood that such communication was intercepted.[691] It is remarkable that the Government in the case, albeit neither confirming nor denying a possible interception,

[686] Ibid.

[687] Ibid.

[688] See *Redgrave v the United Kingdom*, App no. 20271/92, Decision (Commission), 01.09.1993. For a further discussion on the case law on that matter see Cameron I, *National security and the European Convention on Human Rights* (Iustus 2000), 98-99.

[689] *Esbester v the United Kingdom*, App no. 18601/91, Decision (Commission), 02/04/1993.

[690] Ibid.

[691] *Christie v the United Kingdom*, App no. 21482/93, Decision (Commission), 27.06.1994.

did accept that it may have been reasonably likely that communications were in fact monitored.

The ECtHR has also employed the 'reasonable likelihood'-test to visual surveillance. In *Hutcheon v UK*, the applicant contested the erection of a police surveillance tower and complained that her home was subject to visual surveillance as well as that her telecommunications were intercepted because her house and garden were in the direct vicinity of the tower.[692] Here the Commission did not find that Ms. Hutcheon could produce enough evidence for it to be reasonably likely for her home and family to having been subject to surveillance through the tower.[693] Hence, while the ECtHR generally has addressed mass surveillance as a general issue, in some cases the requirement and burden of proof on the applicant to establish a reasonable likelihood can render an application inadmissible.

In several more recent cases, however, the ECtHR has taken a more critical stand regarding the admissibility of cases addressing the existence of mass surveillance mechanisms. *Weber and Saravia v Germany*, for example, addressed surveillance competences given to the German Federal Intelligence Agency (BND), the Federal Office (and '*Länder*'-Offices) for the Protection of the Constitution, and the Military Counterintelligence Service (MAD)[694] by the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications. This so called 'G10 Act' imposed restrictions on the secrecy of mail and telecommunication guaranteed by article 10 of the German Constitution.[695] The applicants, a German free-lance journalist and a Uruguayan National, both living in Uruguay, claimed that the powers given to the Federal Intelligence Agency (BND) to monitor communications violated their rights guaranteed by article 8 ECHR.[696] The applicant contested five measures relating to strategic mass monitoring: the use and transmission of data, the transfer and use of

[692] See *Hutcheon v the United Kingdom*, (n 488).

[693] Ibid, 'the Law', 1.

[694] The German names of the intelligence organisations are: 'Bundesnachrichtendienst (BND)', 'Verfassungsschutzbehörden des Bundes und der Länder', and 'Militärischer Abschirmdienst (MAD)'.

[695] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, (Artikel 10-Gesetz), 26 June 2001, BGBl. I S. 1254, 2298; 2007 I S. 154.

[696] See *Weber and Saravia v Germany*, (n 419).

personal data by other security agencies, the destruction of data as well as restriction on notification of surveillance measures.[697]

The Court took a similar stand as in *Klass* and *Malone* and stated that the

> …mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (…).[698]

Consequently, the broad authorization for surveillance through the G 10 law was considered a clear interference with article 8 of the Convention, however, it was found to be justified under article 8(2) in the case. The same formula was used by the Court in *Liberty and others v UK*, a case addressing warrants for mass surveillance of international communications from the UK. Here again, the UK government remained silent on the matter but accepted that the applicant could be regarded as a victim of an interference due to the potential effect of surveillance measures on them.[699]

In another claim challenging the compliance of a national surveillance act, the Bulgarian Special Surveillance Means Act of 1997, with the ECHR, a human rights NGO and a lawyer succeeded with their claim that under the existing laws, they may at any time become subject to surveillance measures – without claiming to have been directly or indirectly affected by surveillance measures.[700] The Court emphasized that both an individual as well as a legal person can be threatened by surveillance measures and enjoy article 8 protection. Because the applicants did not claim that they had been *de facto* directly subjected to surveillance measures, there was no need to prove a 'reasonable likelihood'.[701] The existence of legislation enabling secret surveillance *per se* therefore constitutes an interference with article 8 ECHR and the Court did not see that this interference was justified in the case.[702]

---

[697] Ibid, para 74.

[698] Ibid, 78 see also *Klass and Others v Germany*, (n 423), para 41, and *Malone v The United Kingdom*, (n 418), para 64.

[699] *Liberty and Others v the United Kingdom*, (n 546), paras 56, 57.

[700] *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, (n 420).

[701] Ibid, paras 58-63.

[702] Ibid, paras 69-94.

3.2.2.1.1 Challenging Mass Surveillance *in abstracto*

Despite of the rather broad approach of upholding potential effects of secret surveillance on applicants, the ECtHR also frequently emphasized its general principle of denying individuals the right to complain against an existing law *in abstracto*.[703] In *Kennedy v UK*, the Forth Section Court elaborated extensively on its two earlier approaches. On the one hand it had allowed for general complaints against surveillance regimes in cases where the secret nature of surveillance would bar the applicant from proving to be directly affected by surveillance. If applicants were barred from challenging secret surveillance regimes, the protected rights in article 8 (1) ECHR would *de facto* be nullified.[704]

On the other hand, it re-emphasized that in case the actual surveillance of communication is merely assumed, there should at least be a 'reasonable likelihood' of applied surveillance measures to the applicant.[705]

Generally, however, '…[t]he Court will make its assessment in light of all the circumstances of the case and will not limit its review to the existence of direct proof that surveillance has taken place given that such proof is generally difficult or impossible to obtain.'[706]

This created some tension within the Court's arguments. On the one hand, an applicant formally needs to be a victim of a concrete interference and the Court does not see its role in examining Member State's legislation *in abstracto*. On the other hand, the Court has clearly permitted and reviewed complaints in which the applicants did not claim to be directly victims of surveillance but merely potentially might have been affected.

The reason for this appears to be the special nature of secret surveillance practices. Simply because people don't know and can't prove that their rights are being violated cannot mean that they don't have access to the Convention's complaint mechanism. In the words of the Court '…where a State institutes secret surveillance the existence

[703] *Kennedy v the United Kingdom*, App no. 26839/05, Judgment (Court), 18.05.2010, para 124.

[704] See *Klass and Others v Germany*, (n 423), para 36.

[705] See *Kennedy v the United Kingdom*, (n 703), para 123. See also *Halford v the United Kingdom*, (n 510), paras 56, 57.

[706] *Kennedy v the United Kingdom*, (n 703), para 123.

of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (...) could to a large extent be reduced to a nullity.'[707]

As a consequence, the Court has recently extensively addressed that issue and attempted to create a general harmonization of its earlier approaches. In the 2015 *Roman Zakharov v Russia* case, the applicant complained that the Russian system and practices of mobile phone communication interception would not comply with the rights standard of article 8 ECHR.[708] Roman Zakharov, an editor in chief in a Russian publishing company, complained that the legislation allowing for covert interception of mobile phone communications put him at risk of being subjected to such surveillance. Hence, Zakharov challenged legislation on the bases of a possibility of being subject to the measures rather than as a result of actually being a subject to concrete surveillance actions.[709] The Court emphasized the article 34 requirement for a complainant to be directly affected and be a victim of the challenged measures, however, extensively cited the *Klass*- judgement for justifying that in some situations such general challenges of a legislative framework could be permissible.[710]

The Court acknowledged that it had developed two approaches for accepting the victim status of the applicant. While in some cases the Court found an interference because

> …the mere existence of laws and practices which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied,

in other cases, either a 'reasonably likelihood' to be affected by concrete measure was required, or that

> …the test in *Klass and Others* could not be interpreted so broadly as to encompass every person in the respondent State who feared that the security services might have compiled information about him or her.[711]

[707] *Klass and Others v Germany*, (n 423), para 36.

[708] See *Roman Zakharov v Russia*, (n 417).

[709] Ibid, para 163.

[710] Ibid, paras 164, 165.

[711] Ibid, paras 166-169.

3.2.2.1.2 The Victim-Status Test

Consequently, in the *Zakharov* Case, the Court attempted to create a synthesis between those different approaches. In fact, the Court referred to *Kennedy v UK,* where it had already partly established a certain harmonization and a general test for admissibility and victim status of an applicant in secret surveillance cases.[712] In *Zakharov*, the Court re-established a test starting with the scope of the legislation permitting surveillance measures:

Firstly, the Court generally examines the possibility for the applicant to be affected by surveillance permitted through legislation either by being a member of a targeted group or because the legislation permits indiscriminate mass surveillance.[713] The victim's status can therefore be established by plausibility and the possibility of being affected.

Secondly, the Court assesses accessibility and the structure of a possible remedy system in the Member State and adjusts '…the degree of scrutiny depending on the effectiveness of such remedies.'[714] If such a remedy system is found not to be accessible and effective, the applicant is not required to show a risk of being personally affected by surveillance.[715] This means on the other hand, that if the remedies on the national level are found to work effectively, the applicant needs to show at least a certain risk of being personally subjected to concrete surveillance measures in order to be considered a victim in the case. The reason for this is that the Court regards the unavailability of the possibility to challenge surveillance, paired with the secrecy of such measures, as suitable to have a strong impact on populations as a whole. Already in *Kennedy v UK*, the Court explicitly noted that

> [w]here there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified.[716]

[712] See *Kennedy v the United Kingdom*, (n 703).

[713] *Roman Zakharov v Russia*, (n 417) para 171.

[714] Ibid, para 171.

[715] Ibid, para 171.

[716] *Kennedy v the United Kingdom*, (n 703), para 124.

Due to establishing a test of admissibility based on the assessment of remedies, the Court in the *Zakharov* case spent much effort testing the structure, availability and effectiveness of the Russian remedy system on mobile phone communication interceptions.[717] In the end it concluded that there had not been an effective remedy available to the applicant and that there had been a violation of article 8 ECHR due to the '…existence of arbitrary and abusive surveillance practices, which appear to be due to the inadequate safeguards provided by law (…).' The Russian law authorizing mobile phone interceptions does therefore '…not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society".'[718]

***

The arguments regarding the victim status test put forward in the *Zakharov* judgment are interesting because they show how the ECtHR attempts to balance its own argumentation and forms a coherent test applicable to admissibility and interference assessment when cases concerning secret mass surveillance reach the Strasbourg Court. Although they are not particularly new, the arguments in the *Zakharov* case sum up, clarify and unite previous case law regarding secret surveillance.

Article 34 ECHR defines criteria regarding admissibility of individual complaints, one of which requires the applicant to be able to claim to be a victim of a violation of rights in the ECHR System. Yet, the victim-test set out by the Court in surveillance cases connects this victim status not only to an established interference, but also to an assessment of the justification of an interference set out in article 8(2), particularly the requirement of legality. Following the victim test, the Court needs to take into account the possibility of the applicant being subjected to surveillance and the remedies available. In line with the Convention's systematics, however, the existence of adequate safeguard and remedies are assessed as part of the legality requirement when testing a possible justification of an already established interference in article 8(2)

[717] *Roman Zakharov v Russia*, (n 417), paras 286-300.

[718] Ibid, paras 303, 304.

ECHR. This means, that admissibility, interference and justification of an interference are heavily interdependent in mass surveillance cases. Consequently, in the *Zakharov* judgment, the Court justified the applicant's claim to challenge the legislative system of surveillance authorization as it potentially affects all users of mobile communication. Additionally, however, the Court referred to its own following assessment of the legality requirement in the case when it found that there is a lack of effective remedies in the Russian system. [719] Due to this, challenging the surveillance system *in abstracto* can be justified as an exception to the general principle of requiring the applicant to be a direct victim of an interference. Whether the strict interdependencies between justification of interference, establishing an interference, and admissibility requirements will cause problems for the Court's argumentation in the future remains to be seen. With *Zakharov*, however, it becomes clear that the Court is very well willing to extensively engage with mass-surveillance cases. The most challenging ones are yet to be heard.[720] Admissibility and interference into rights enshrined in the Convention play a crucial role also in case of mass urban surveillance.

It additionally becomes clear that the Court referred to the abstract threats of mass-surveillance in order to justify admissibly. Potential fears of population, surveillance as a 'menace' for society and similar arguments in the cases show that mass-surveillance requires abstract arguments. It shows, however, that abstract challenges of mass-surveillance systems are not barred from being successful.

The discussion on admissibility and victim status tests showed a general problem with challenging mass surveillance cases before Courts: admissibility often depends on a burden of proof and a personal affectedness, and both can be challenging arguments to make, especially when the capabilities of mass surveillance systems are not transparent. The example of the ECtHR arguments in those cases, however, show that

[719] The ECtHR stated: 'Furthermore, for the reasons set out below (see paragraphs 286 to 300), Russian law does not provide for effective remedies for a person who suspects that he or she was subjected to secret surveillance.' *Roman Zakharov v Russia*, (n 417), para 176.

[720] See e.g. the pending cases: *Centrum För Rättvisa v Sweden*, App no. 35252/08, Communicated Case, 14.10.2014; *Big Brother Watch and Others v the United Kingdom*, App no. 58170/13, Communicated Case, 07.01.2014, *Bureau of Investigative Journalism and Alice Ross v the United Kingdom*, App no. 62322/14, Communicated Case, 05.01.2015; *10 Human Rights Organisations and Others v the United Kingdom*, App no. 24960/15, Communicated Case, 24.11.2015.

the Court found ways to not make admissibility become an insuperable barrier for challenging mass surveillance.

3.2.2.2 Fundamental Rights Arguments against Mass Surveillance

As has been shown in the analyses of targeted and individual surveillance in section 3.1 above, many surveillance technologies fall within the scope of the ECHR *per se*. Audio surveillance and communication interception, location data, the collection of personal information and also, as shown from the discussion on victim status and admissibility above, mass surveillance regimes as such can trigger article 8 issues. The remaining question to be discussed is how far highly integrated mass surveillance system operating in public spaces as described in the Helberg scenario can give rise to article 8 issues.

3.2.2.2.1 Mass Surveillance and the Scope of Privacy

Mass surveillance systems in public places employ a variety of different types of technologies, for example video camera surveillance, tracking technologies or analytics software. As discussed above, the ECtHR held repeatedly that, for example, camera surveillance used merely for security purposes and observations does not constitute an interference with article 8, however, with the caveat that once such a surveillance system records and retains personal data, the fact that systematic records are used, is enough to amount to an interference with private life in article 8.

In *Herbecq and the Association Ligue des Droits de L'Homme*, both a natural person and an association challenged the lack of legislation regulating the use of unrecorded public video surveillance in Belgium.[721] The applicants in the case claimed that the absence of legislation would have made it *de facto* impossible for individuals to challenge the use and spread of video surveillance.

The applicants, however, also challenged unrecorded video surveillance by pointing to a potentially negative societal impact. In fact, the applicants employed a chilling-effect argument in the case:

[721] *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421), 93.

> Since no one has this information everyone may feel obliged to censor their own behavior so as to avoid doing anything or behaving in any way which could be interpreted by potential observers using such surveillance equipment.[722]

The Commission did not follow this argumentation and held that the application was manifestly ill-founded. Firstly, it rejected the view that an association can complain against the lack of legal bases permitting public video surveillance in the case. Only the first applicant or identified specific victims, but not associations could be subject to visual surveillance. Secondly, the Commission re-emphasized earlier case law on the use of photographic equipment in finding that visual imagery from public areas as such do not amount to an interference with the scope of protection of article 8.[723] Provided that no systematic or permanent record is created, visual surveillance of public areas therefore falls outside the scope of protection, although depending on the assessment and nature of such images.

It would most likely however be difficult for the Court to come to the same conclusion regarding sophisticated surveillance systems in the scenario.

Much of the technology employed in Helberg is based on data collection, retention and especially analytics. A video surveillance system, for example, which allows personal data to be analysed, however, clearly falls within the scope of protection of the ECHR. After all, sophisticated technological surveillance capabilities such as tracking an individual's movements, the identification of behavioural patterns, or predictive analytics touch the essence of privacy as a right enshrined in its various forms.[724] Furthermore, sophisticated capabilities in Helberg include extensive monitoring and surveillance of individuals and groups and allow for the efficient control of vast spaces.

Already potential mass surveillance capabilities of such sophisticated surveillance, might lead the ECtHR to the conclusion that such surveillance *per se* constitutes

[722] Ibid, 94.

[723] See discussion on *Friedl v Austria*, (n 482), and *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421) above.

[724] For a more detailed discussion on prediction see Section 3.4 Automation and Prediction.

interference with a right to private life in article 8 ECHR even if a possible applicant could not directly prove to be subject to concrete targeted surveillance.[725]

In that case, a person walking on a public place might very well argue that the existence of such sophisticated surveillance capabilities *per se* interferes with several of her rights enshrined in the Convention. After all technology is way more advanced than what a simple security guard present at that place might be able to discern.

The Court employed the *Kennedy* and *Zakharov* cases admissibility test also in a recent judgment. In the early 2016 judgment *Szabó and Vissy v Hungary*, the Court found that Hungary's secret anti-terrorism surveillance legislation was in breach of article 8 ECHR because the measures were broad and there were no adequate safeguards in place preventing abuse of the surveillance system.[726] The applicants were staff members of a politically active NGO and due to that, claimed to be more likely affected by article 8 interferences through broad surveillance competencies given to anti-terrorism policing.[727] The Court however, stated that while it may have been important to consider certain special issues relating to politically active NGOs, the particular anti-terrorism surveillance measures potentially targeted all 'users of communication systems and all homes'.[728] Paired with the fact that there was no possibility for individuals to complain before an independent body against assumed and potential surveillance, the Court confirmed the victim status of the applicants and declared the application admissible.[729]

In *Szabó and Vissy*, the ECtHR clarified the relationship between a legal analysis of judicial safeguards and a proportionality test: In its evaluation of possible justifications of interferences in the case, the Court clarified, that when the applicant's complaint is directed against a specific system of surveillance and not against concrete or targeted surveillance, it would focus on an analysis of legislation and safeguards rather than on the proportionality of measures directed towards an individual.[730] This

[725] See *Roman Zakharov v Russia*, (n 417); and Section 3.2.2.1.1.

[726] See *Szabó and Vissy v Hungary*, App no. 37138/14, Judgment (Court), 12.01.2016.

[727] Ibid, para 37.

[728] Ibid, para 38.

[729] Ibid, para 39.

[730] Ibid, para 58.

means that once an application is admissible but challenges legislation *in abstracto*, the Court will assess the legislation and the adequacy and efficiency of inbuilt safeguards. Once, on the other hand, concrete surveillance measures against an applicant are challenged, the Court will analyse the specific surveillance measures as to their proportionality in respect to the circumstances and situation of the applicant.

This sheds some light onto the question of how an interference in cases concerning a sophisticated public surveillance system in a public area could be found. For this, a claim could either focus on the legal source establishing the possibility of installing and operating surveillance systems, or on the potential collective or individual effects of a concrete surveillance system. The result might then depend on the very nature of the system. It appears, though, that the more hidden a system is and the higher its capabilities to operate in the background are, the more it makes sense to analyse interference on the bases of legal safeguards and the collective or societal effect of the surveillance system.

Additionally, data collection as such can also play a decisive role. As already discussed above, the collection and processing of personal data as such falls into the scope of article 8 ECHR, giving rise to another factor for arguing an interference with privacy rights.

The notions of 'private life', 'home' and 'correspondence' in article 8(1) ECHR clearly cover: 'to search and keep under surveillance the applicants' homes secretly, to check their postal mail and parcels, to monitor their electronic communications and computer data transmissions and to make recordings of any data acquired through these methods.'[731] As much as individual surveillance matters for the Court, in mass surveillance cases it has often emphasized the finding that surveillance, especially when conducted without proper legal bases and safeguards, can become a 'menace' to democratic societies and therewith an interference *per se*.[732]

It is apparent from the discussion above, that the ECHR rights protection system is fundamentally targeted towards individual complaints. The requirement of a victim

[731] Ibid, para 52.

[732] *Klass and Others v Germany*, (n 423), para 37, *Halford v the United Kingdom*, (n 510), paras 53, 56; *Iordachi and Others v Moldova*, App no. 25198/02, Judgement (Court), 14.09.2009, para 34; *Roman Zakharov v Russia*, (n 417), para 171; *Szabó and Vissy v Hungary*, (n 726), para 53.

status for admissibility and the general principle of the ECtHR to not examine legal regimes *in abstracto* show that the ECHR system is originally not designed for addressing abstract and general questions regarding fundamental rights. It is indeed a control mechanisms focusing on the possibility of individuals complaining against alleged violations of their fundamental rights. Yet, as can be seen above, the ECtHR sometimes makes exceptions to that rule, and cases involving mass surveillance are treated as such an exception simply because of the nature of surveillance, especially when the extend of surveillance practices remain secret. While the section above discussed the admissibility and rights interferences of mass surveillance, the following section will now return to a discussion of mass surveillance in public places.

3.2.2.2.2 Mass Surveillance as a 'Menace to Society'

The ECtHR adapted its own argument of a reasonable expectation for individuals to be surveilled in public as analysed in Section 3.1.1.1 above. In *P.G. and J.H. v UK*, the Court has coined the formula:

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.[733]

Consequently, the ECtHR came up with an argument that suggest that individuals once placed on a public street enjoy a lesser amount of privacy than in secluded places as in public they enjoy a lesser 'expectation of privacy'. On the other hand, it is also clear from previous findings that the right to privacy protects individuals in all places and in all situations, especially when the person's social interactions, honour or dignity are affected.[734]

In that sense, the ECtHR has indicated that it distinguishes between levels of intrusiveness of surveillance in public spaces. As discussed already above, in *Herbecq* the applicant complained against a lack of legal regulation on video surveillance cameras in public places in Belgium. The applicants particularly challenged public

[733] *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

[734] See Council of Europe, Venice Commission), Opinion on Video Surveillance, (n 101), para 32 for a similar conclusion.

unrecorded video surveillance by employing a 'chilling-effect' argument. The lack of adequate regulation would make video surveillance directly unchallengeable for individuals which may have the effect that people in public places change their behaviour due to the ever-present threat of being watched with a video camera. Furthermore, for the applicants in the case, such visual surveillance could reveal '…information, consisting in certain modes of behaviour or physical attitudes, which the individual in question may not have wished to divulge.'[735] The argument, hence, was based on the general perception that people who are being surveilled or who think they are being surveilled change, restrict or adopt their behaviour and therefore restrict their freedom within a public context. This should be seen as an interference with the right to private life protected by article 8 ECHR as such. The 'chilling-effect' of a surveillance camera would then *per se* constitute an interference.

The commission did not follow this argument. It emphasized that the applicant challenged merely unrecorded video surveillance in public places by public and private actors and referred to its earlier case law on the use of photographic equipment in public spaces.[736] The video surveillance system also did not collect any personal data which could be stored analysed and disseminated.

> [T]he data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person (…). Therefore, all that can be observed is essentially, public behavior.[737]

The Commission declared the application manifestly ill-founded. Unrecorded video surveillance therefore seemed not intrusive enough to constitute an interference with private life protected by the ECHR. Nevertheless, it is highly unlikely that the ECtHR would uphold such a finding when it is confronted with a case challenging a sophisticated surveillance system as exemplified in the urban surveillance scenario. Firstly, the mere scale and systematic surveillance capabilities might already raise issues in relation to article 8 ECHR. Secondly, the collection, processing and retention of personal data would constitute an interference[738] and thirdly, seen as a holistic tool for mass surveillance, challenging wide-scale surveillance might even be permissible

[735] See *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421).

[736] As discussed above and see *Friedl v Austria*, (n 482), para 48.

[737] *Herbecq and the Association Ligue des droits de l 'homme v Belgium*, (n 421).

[738] See *Rotaru v Romania*, (n 418), paras 43-44, and *Amann v Switzerland*, (n 503), paras 65-67.

in abstracto, depending on the outcome of a successful test in line with the *Kennedy* and *Zakharov* requirements. Furthermore, the ECtHR has clearly described mass surveillance as a 'menace' to society and therewith operated on a collective, rather than an individual-centred perspective.

The ECtHR, however, has constructed another argument in earlier cases which might be suitable to be employed in surveillance cases. Not only does an individual enjoy a right to her own secluded circle, but also enjoys the 'right to form relationships'. This reasoning has particular relevance for mass-surveillance: Could mass-surveillance in public interfere with the right to form relationships?

3.2.2.2.3 The Right to Establish Relationships with the Outside World.

This aspect has been frequently reasoned by the ECtHR in article 8 and in surveillance cases. In fact, the 'right to establish and develop relationships with other human beings' was coined in the 1992 *Niemitz v Germany* judgment:

> [I]t would be too restrictive to limit the notion [of private life] to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.[739]

This formula contains two elements: Firstly, article 8 protects at least in some ways the forming of personal relationships with other individuals and secondly, the notion of private life expands to the outside world, beyond a narrow application of privacy rights in strictly secluded spaces. For this reason, the ECtHR has found that aspects of private life expand in spheres such as business life or other public contexts.[740]

Additionally, it is important to note that the Court explicitly grants a right to form relationships with other persons as part of the creation of personal identity and the development of one's own personality.[741] In *Fernández Martínez v Spain*, the Court additionally emphasized a right to 'self-fulfillment' through personal development or the '…right to establish and develop relationships with other human beings and the

[739] *Niemietz v Germany,* App no. 13710/88, Judgment (Court), 16.12.1992, para 29.

[740] Ibid, para. 29, *Burghartz v Switzerland*, App no. 16213/90, Judgment (Court), 22.02.1994, para 24.

[741] See *Bărbulescu v Romania*, App no. 61496/08, Judgment (Court), 12.01.2016, para 35. See also *Peck v The United Kingdom*, (n 258), para 57.

outside world.' The Court furthermore regarded 'personal autonomy' as a crucial principle enshrined in article 8 ECHR.[742] This reading of privacy goes beyond the limited understanding of privacy as an individual expectation. Here, privacy is connected with self-determination and a personality right.[743] In that sense, because article 8 also protects personal autonomy, it entails a level of privacy which goes beyond individual expectations: In the well-known *Pretty* case, the ECtHR stated that

> [a]lthough no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.[744]

The right to private life, article 8 ECHR and questions relating to personal autonomy and self-determination have been extensively discussed in case-law and the literature, for example in connection with sexual orientation, gender identity or the right to end one's own life.[745] It is however important to note that the ECtHR has limited the application of private life and the right to form relationships in spheres with others that go beyond a narrow interpretation of the private sphere. In the *Botta* case, the applicant, a person with disabilities, complained that the lack of accessibility features in a private bathing establishment restricted his private life and personality development because

> …he was unable to enjoy a normal social life which would enable him to participate in the life of the community and to exercise essential rights, such as his non-pecuniary personal rights (…).[746]

The Court did not follow this argument because it saw such interpersonal relations as being too broad in order to be protected by article 8. Similarly, in *Friend and Others* the Court found that hunting bans did not interfere with article 8 ECHR because personal enjoyment and personal relationships gained from such practices would fall

---

[742] *Fernández Martínez v Spain*, (n 416), para 126; *Pretty v The United Kingdom*, (n 258), para 61.

[743] See Section 2.2.7 Privacy in Public.

[744] *Pretty v The United Kingdom*, (n 258), para 61.

[745] For a detailed discussion see Koffeman NR, (The right to) personal autonomy in the case law of the European Court of Human Rights (External Research Report, Leiden: Leiden University 2010), 23-52 https://openaccess.leidenuniv.nl/bitstream/handle/1887/15890/N.R.%20Koffeman%20-%20%28The%20right%29%20to%20personal%20autonomy%20in%20the%20case%20law%20of%20the%20ECtHR%20%282010%29.pdf accessed 16 October 2016.

[746] *Botta v Italy*, App no. 21439/93, Judgment (Court), 24.02.1998, para 27.

outside the scope for similar reasons.[747] Recently the Court repeated that private life in article 8 does not protect

> (…) every activity a person might seek to engage in with other human beings in order to establish and develop such relationships. It will not, for example, protect interpersonal relations of such broad and indeterminate scope that there can be no conceivable direct link between the action or inaction of a State and a person's private life.[748]

Therefore, challenging mass-surveillance in public spaces on the basis of a right to form relationships in a public sphere would need constructing a clear connection between an individual's right to private life and a negative impact of mass-surveillance on the forming of relationships. It is in a way possible that sophisticated public surveillance and the control of space through state security authorities could in an indirect way interfere with a person's private life and their abilities to form relationships and enjoy participation in social life. For example, if a person lives in an area subject to heavy surveillance, friends might avoid visiting because they do not want to subject themselves to surveillance in the public space or on the way there. Or, in a more concrete example, when a person is visible for surveillance organs once she steps outside her own doorstep, that person might limit leaving the home to what is absolutely necessary and therefore self-restrict her participation in public social life.

While many examples could be constructed in which surveillance in one or the other way interferes with forming personal relationships and other personal freedoms in a public surveillance scenario, the most likely and most clear establishment of an interference stems from the fact that systematic surveillance collects, processes and retains personal information. The right to personal data protection therefore appears to be stronger than a right to develop interpersonal relationships deriving from article 8 ECHR.

3.2.3 Mass Surveillance and Data Protection

Data protection and mass-surveillance have a complex relationship. On the one hand, the processing of personal information is a crucial part of mass-surveillance practices

[747] *Friend and Others v the United Kingdom*, App nos. 16072/06, 27809/08 Decision (Court) 24.11.2009.

[748] *Bărbulescu v Romania*, (n 741), para 35.

today, on the other hand, the legal discussions on mass surveillance in the ECtHR jurisprudence appear to distinguish between data-protection issues and mass surveillance.

Personal data collection, retention and processing, however, clearly falls within the scope of protection of article 8 ECHR. Additionally, the EUCFR and regulatory instruments in the EU as well as CJEU jurisprudence made data protection an essential element of European fundamental rights law.

The distinction between targeted and untargeted surveillance in the analyses of the scenario above, however reaches its limits with regards to data protection. That is because the legal protection mechanisms of data protection in mass- as well as in targeted surveillance depend on the classification of data as 'personal' data.

Because personal data is defined as '…any information relating to an identified or identifiable individual ("data subject")',[749] any mass-surveillance data processing can be seen to have a very specific individual focus.

Generally, however, data protection and fundamental rights implications have played an important role in the definition of the scope and interpretation of the right to private life in the ECHR, especially relating to new technologies. Public surveillance via technologically advanced surveillance systems as described in the technological part as well as the public surveillance scenario heavily relies on the collection of massive amounts of personal data. A CCTV image of a person, the GPS coordinates of a person's mobile phone, their communications and respective meta-data all constitute personal data.

Mass-surveillance of public places, however, is not always only concerned with data relating to an individual. Often, mass surveillance also collects a bulk of data that is processed for other purposes than targeted surveillance. As discussed in the outline of this section, surveillance is not solely about individuals and their information, but also about managing, governing and controlling large amounts of people and large systems, as well as administering risk.[750] What follows from this is the question if the

[749] CoE Data Protection Convention, (n 299), Art 2 a).

[750] See e.g. Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001), 6.

mass data-collection and therewith the exercise of such administration and control could be seen as an interference with fundamental rights in the ECHR system.

This is a somewhat tricky question, as it defies the essential basics of the ECHR fundamental rights system. Human Rights in the ECHR and especially the right to private life and the interpretations on personal data protection are conceptualized as individual rights that depend on the relation to an individual. Data falling into the scope of protection of the ECHR as well as the CoE Data Protection Convention 108 is always 'personal' data, not just data. Furthermore, the object and purpose of Convention 108 is tackling data protection as '…automatic processing of personal data relating to him.'[751] Some data collected by mass surveillance systems might however, not *prima facie* qualify as personal data.

What remains to be discussed especially in connection of mass surveillance are therefore two issues. Firstly, surveillance data that falls completely outside the scope of data protection frameworks, and secondly, data that falls outside of the scope today, but due to expanding technological capabilities, could fall into the category of personal data in the future.

3.2.3.1 The Scope of Data Protection

Public surveillance, employing technology described in the scenario, naturally is primarily concerned with the identification of individuals. Advanced technologies such as facial recognition or video content analyses attempt nothing more but to single out individuals, either because they pose a threat, or because they are the subject of surveillance. One core issue relating to modern technological mass surveillance is that it blurs the border of targeted and non-targeted surveillance. Additionally, such technologies, for example facial recognition, operate in the invisible background therewith blurring the border between covert and overt surveillance. Modern surveillance, especially in the sense of the scenario, is targeted and non-targeted as well as covert and overt at the same time and hence creating an omnipresent web of data processing operating in the background behind visible sensors.

[751] CoE Data Protection Convention, (n 299), Art 1.

For classical data protection and the definition of personal data, this might mean that originally non-personal data in which individuals are not identified or identifiable, become data points leading to the identification, or at least, identifiability of persons in the future. For example, low resolution video images unsuitable for identification of persons could be processed and analysed using powerful software which can identify specific individual movement patterns leading to the identifiability of individuals. With this, data protection standards would start to apply for data which originally fell outside of such scope. This could create a prima facie loophole in fundamental rights protection from public surveillance.

3.2.3.2 Big Data

The other category with significant relevance to mass surveillance and data protection regulation is the massive collection of vast quantities of data and the subsequent analytics. The buzzword for this phenomenon is 'Big Data', describing the collection and analytics of vast amounts of information. For Mayer-Schönberger and Cukier, Big Data is about '…seeing and understanding the relations within and among pieces of information that, until very recently, we struggled to fully grasp.'[752] Boyd and Crawford define Big Data as a '…cultural, technological, and scholarly phenomenon' which is founded on the interplay of three interrelated aspects namely 'technology', 'analyses', and 'mythology'.[753] What they mean is that Big Data essentially describes a phenomenon deriving from technological progress and the vastly increasing collection and retention of data, improved capabilities for analytics and a common rhetoric around the phenomenon that it would somehow objectively improve insights into aspects of the real world. In that sense, Big Data is indeed '…less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets.'[754] Following such an understanding of Big Data, it becomes clear that it can describe different types of data analytics, from global data on climate change to the

[752] Mayer-Schönberger V and Cukier K, *Big Data: A revolution that will transform how we live, work, and think* (Houghton Mifflin Harcourt 2013), 19.

[753] Boyd D and Crawford K, 'Critical Questions for Big Data' (2012) 15 Information, Communication & Society 662, 663.

[754] Ibid, 663.

analytics of all Facebook posts. Lyon therefore rightly pointed out that possible applications of Big Data analytics vary so much that a legal analysis would have to take into account different aspects of each field – after all Big Data analytics in the field of terrorism prevention has more impact on individual rights than climate data on the melting of the polar ice caps.[755]

Beyond such rather critical views, Big Data is often understood to have enormous promise for technological process, economic growth and innovation and any regulation in this area is perceived as impeding progress and a positive future.[756] While those debates have to be held elsewhere, one important question arises in connection with mass surveillance in a public context: Does Big Data analytics interfere with fundamental rights and how is it regulated in that context?

Public data collection and analytics which are large enough come with two essential legal questions: Firstly, does Big Data interfere with a right to privacy and data protection. For this the essential question at this point seems to be how far the actual data in Big Data analytics can be categorized as personal data or not.

Secondly, as Big Data is collected, retained, and analysed by private corporations or non-governmental organizations rather than governments and security authorities, how does the private sector big data processing and subsequent law enforcement access affect the protection through fundamental rights regimes?

Regarding the latter, it has become clear since Edward Snowden leaked classified intelligence files in 2013, that while the US security authorities collect and retain larger amounts of data and communications than anticipated, there also existed a system of coercion and cooperation for government access to data held by corporations and private sector entities. Additionally, a large private security industry today collects and retains data with the specific purpose of selling data to intelligence

[755] Lyon D, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) 1 Big Data & Society 1, 2.

[756] See e.g. Tene O and Polonetsky J, 'Privacy in the Age of Big Data. A Time for Big Decisions' (2012) 64 Stanford Law Review Online 63.

services and governments.[757] This has enormous implications, both for practical protection as well as theoretical analyses of human rights.

What this section argues is that using the analyses of vast quantities of data and Big Data processing for the purpose of surveillance will constitute an interference with human rights in the European legal space.

The starting and most essential question is, if Big Data analytics falls within the scope of data protection rights. At first sight, the answer is rather simple: once Big Data qualifies as personal information, data protection standards apply because it then falls within the scope of article 8 ECHR and the Council of Europe Data Protection Convention, or, provided the processing happens within the scope of EU law, also in the EU data protection framework. Secondly, once data processing falls into those areas of law, the information processed would need to fulfil the criteria of personal data as information relating to an identified or identifiable individual. Considering the rather wide legal interpretations, it is difficult to imagine any surveillance related data that would not fall into this category, however, it is crucial to understand how far it is technically feasible to attribute information to an individual and how likely such a process would be. In the end, it would depend on the actual nature, purpose and technical analytics of such data.

What is remarkable in this regard is that the nature of data as well as the nature of surveillance has radically changed. Data is collected, retained, and analysed in a very different way today than ten years ago, naturally questioning the conceptual relationship between individual and information. Surveillance understood as targeted operation on single individuals has changed to what could be called 'dataveillance' and the sources of data gathering have changed from targeted collection to accessing the large data pools created through information and communication technologies.[758] With this, however, is the current classification into personal and non-personal data still useful?

---

[757] For an early analysis of this phenomenon see Hoofnagle CJ, 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement.' (2004) 29 North Carolina Journal of International Law and Commercial Regulation 595.

[758] See van Dijck, J 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology' (2014) 12 Surveillance & Society, 198.

Within the European context, both the Council of Europe Data Protection Convention and the definition on the European Union framework, namely in the 95/46 Data Protection Directive and the General Data Protection Regulation (GDPR), understand personal data as 'information relating to an identified or identifiable natural person.'[759] While all of the definitions are essentially similar, their interpretations vary between CoE and EU framework, especially with regards to the interpretation of what essentially determines 'identifiability'. Here, the interpretations of the two sources appear manifestly different: where the CoE Explanary Report on Convention 108 finds that identifiability requires an easy identification possibility (excluding 'sophisticated methods')[760], the GDPR interpretation focusses on the criterion of 'reasonable likelihood'. In fact, Recital 26 of the GDPR states that in interpreting identifiability in article 4 (1), '…account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the individual directly or indirectly.'[761] Such reasonable likelihood is established by taking into consideration '…all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.'[762] Consequently, all information that can be attributed to a natural person (including pseudonymization) constitute personal data and only completely anonymous information which cannot be traced back to a person is excluded from the scope of the GDPR (this also applies to research statistics).[763]

What consequences would the CoE interpretation of identifiability have for sophisticated public surveillance? Would, for example information on persons gathered by facial recognition systems in public spaces fall outside the scope of the

[759] See Regulation (EU) 2016/679, (GDPR), (n 303), Art 4 (1); See also Directive 95/46/EC (Data Protection Directive) (n 305), Art 2(a); CoE Data Protection Convention, (n 299), Art 2(a).

[760] See Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (n 570), para 28: '"Identifiable persons" means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods.'

[761] Regulation (EU) 2016/679, (GDPR), (n 303), Recital 26.

[762] Ibid.

[763] Ibid.

CoE Data Protection Convention because it does not include the '…identification of persons by means of very sophisticated methods'?[764]

In order to answer this question, it needs to be discussed what could be considered a 'sophisticated method' in the sense of the commentary. Taking into account that the Convention as well as the commentary date back to 1981, it becomes clear that a crucial factor is technological progress. While the identification of a person on a video tape on a public place 35 years ago would have required watching hours of recorded video, it could be possible to achieve identification today within seconds. It seems obvious that the sophistication of method relates to the actual effort which needs to be expended to connect a piece of information with a real person. With advancing technologies, and the sophistication of methods in that sense, connecting such dots becomes easier. Taking into consideration the object and purpose of the Data Protection Convention, namely the protection and strengthening of fundamental rights,[765] it is unlikely that the sophisticated processing and analytics of information would result in the personal information falling outside the scope of the treaty.

In that sense, technological sophistication should not be confused with the 'identification of persons by means of a very sophisticated method' in the CoE Explanatory report. What remains, would be a classification of personal data along the lines of ease and effort to actually achieve identification of an individual or information attribution – the easier it is and the less effort it takes, the more likely it

[764] Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (n 570), para 28.

[765] It can be concluded from interpretations of the Data Protection Convention that new technological developments are very well taken into considerations. Of particular importance is a reference to paragraphs 1 and 25 of the CoE Explanatory Report (ibid): '1.The object of this convention is to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. There is a need for such legal rules in view of the increasing use made of computers for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed. Further growth of automatic data processing in the administrative field is expected in the coming years inter alia as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission. (…).

25. The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms. Moreover, it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit).'

is that the information will be considered personal data. With Big Data, however, most of the information that is processed, especially in a surveillance context, would fall into the category of personal data and therewith within the scope of the CoE Data Protection Convention. Therewith, much of mass surveillance Big Data should be considered as processing of personal data - unless the information is absolutely unrelated to individual human beings. Much therewith also depends on the actual detailed technological processes in the surveillance system. For example, assuming it is of importance for a public transport authority to know how many people use the transportation system at what time, to adjust transportation capacities. One way of getting such information is to install a video camera and run specific software which counts individuals on the video stream. As it is in principle easy to identify people on video camera images, this would qualify as processing of personal data in the meaning of the CoE Convention 108. The only option to design the system in a way that it might fall outside the scope of the Convention would be if the system actually did not at any moment retain any real video images; e.g. the system takes the video stream, counts the individuals and immediately and un-recoverably deletes the video stream.

Therefore, such video analytics processes non-personal data only when the data are either not retained or immediately anonymized. However, even then it could be argued that because the system actually takes and processes real images of people, it could still be classified as processing personal data.

In that sense, only the non-existence of senor data guarantees the non-personality of such information. The distinction between personal data and non-personal data in Big Data processing therewith is very difficult to grasp and to delineate.

A slightly different formulation on the interpretation of personal data and non-personal data can be found in the EU framework and the new GDPR. The GDPR requires a certain ‘reasonable likelihood’ for the data to be used for identification. The identifiability of an individual therefore requires an assessment test: identifiable information is attributable to a person, and this attribution requires to be firstly, possible, and secondly, reasonably likely. Consequently, the available means as well as the objective factors involved, e.g. effort, time, or costs, need to be part of the assessment. In that sense, an assessment of a person counting system in the example above would need to focus on the technological capabilities to extract information

attributable to a specific individual, and how likely is it that a controller or operator could extract such information with a reasonable effort.

Additionally, however, the GDPR is not intended to apply to anonymized data:

> The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable.[766]

The definition of anonymization, however, depends again on the test outlined above. Anonymized Big Data, provided that such information is not reasonably likely to be re-attributed to an individual would therefore fall outside of the EU data protection framework. Surveillance Big Data, however, is difficult to place outside of data protection frameworks, simply because surveillance data, by definition, is likely to single out individuals.

3.2.3.3 Big Data, Societal data and Data Protection Principles

Data protection in general can be understood in terms of specific principles that are more or less contained in all data protection laws and regulations. Furthermore, especially recently, data protection principles increasingly found their voices in European Courts, spearheaded by the CJEU and its recent landmark judgments on the right to privacy and the right to data protection.[767] Data protection principles furthermore have developed rapidly and became an important factor for case law and jurisprudence in Europe. In line with such interpretations, the crucial question relating to Big Data and public surveillance is in how far public surveillance systems collide with particular principles of data protection. Mass surveillance is of particular importance in this regard because the core of such types of surveillance is the bulk collection of information, as opposed to the targeted gathering of data on a specific suspect. Big Data surveillance therewith marks a shift from targeted and purpose specific data collections to the pre-emptive and causeless collection of information processed in order to identify persons, patterns or anomalies.

[766] Regulation (EU) 2016/679, (GDPR), (n 303), Recital 23.

[767] See Section 2.3.2 above

With Big Data used as surveillance information, ordinary and on first sight seemingly meaningless and unrelated information is collected and retained, leading to classification, quantification and real-time tracking and monitoring of individual and societal information. Societal information in this regard is the mix of environmental information, meta-information, operational data as well as information on groups as well as on individuals. While targeted surveillance is collected and stored for a specific purpose, mass surveillance by gathering societal data in a public context is collected pre-emptively and without a specific purpose, and often even without any current capabilities to process all this data. One of the characteristics of bulk collection, for example, is the collection, aggregation and retention of all sorts of information, with a future perspective that it might be a possibility that this data would become relevant for future processes. In that sense, data today is often collected '…before determining the full range of their actual and potential uses and mobilizing algorithms and analytics not only to understand a past sequence of events but also to predict and intervene before behaviours, events, and processes are set in train.'[768]

Within the context of Big Data and public surveillance, and therewith the gathering of societal data from a public environment, how do such practices interfere with specific data protection principles? Taking into account the data protection principles in European fundamental rights law, it becomes clear that many of such collections might contradict the prohibitions of limitless and uncontrolled collection of all sorts of personal information. Convention 108 but also both the GDPR as well as the new Police Directive[769] contain similar general principles of data processing: personal data shall only be collected for 'specified, explicit and legitimate purposes', limited to the purpose and not kept longer than necessary for that purpose.[770] Provided that Big Data qualifies as personal data, such surveillance data collection would collide with at least some of the data protection principles.

On a general level, the collection and processing of large amounts of data in public places might have an overall negative societal effect, and chilling effects-

[768] Lyon D, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) Big Data & Society 1, 4.

[769] Directive (EU) 2016/680 (n 303).

[770] See Art 4 Regulation (EU) 2016/679, (GDPR), (n 303), Art 4 Directive (EU) 2016/680 (n 303), Art 5 CoE Data Protection Convention, (n 299).

argumentation can be connected with data collection and processing. The collection and processing of societal data might as well qualify as secret surveillance practices towards which particularly the ECtHR has taken a rather critical stand against.[771]

3.2.3.4 Applicability of EU Data Protection to Mass Surveillance

As can be clearly seen from the analyses on data protection above, responses to mass surveillance within a European legal context are not limited to the framework of the European Convention on Human Rights. In recent years, the EU has strengthened its Fundamental Rights framework not at last with the Treaty of Lisbon in 2009 and the binding legal status of the Charter of Fundamental Rights of the European Union. This means that surveillance issues are not only subject to fundamental rights considerations at the ECHR/Council of Europe level, but also at the level of the European Union. There is, however, a caveat: The EU Charter's scope extends to '…the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law.'[772] Personal data protection is furthermore contained in art 16 TFEU[773] and art 39 TEU.[774] Generally, as discussed already in Section 2.3 above, there is a wide body of EU regulation on data protection.

In this context, the question arises of how far mass surveillance and surveillance of public places fall within the scope of Union Law, provided it concerns actions that can be related to EU law. Security and law enforcement have traditionally been placed outside of the scope of Community Law. How far can mass surveillance and public surveillance therewith be addressed by the EU Fundamental Rights framework? This is a somehow tricky issue, because it is often unclear how far the scope of fundamental rights extends to issues only indirectly related to EU regulation and because it can be very difficult to determine which actions fall within the scope of Union Law.

---

[771] See e.g *Roman Zakharov v Russia*, (n 417), para 169

[772] Article 51 EUCFR

[773] See Consolidated version of the Treaty on the Functioning of the European Union (TFEU), OJ C 326, 26.10.2012, 47–390.

[774] Consolidated version of the Treaty on European Union (TEU), OJ C 326, 26.10.2012, 13–390.

In that regard, fundamental rights within the EU context theoretically apply to measures that are in one or another way related to Union Law. An issue regulated by National Law will therefore not directly be subject to EU fundamental rights review unless it can be related to the scope of Union Law.[775] Once member states act within the scope or implement EU law, they should be bound by the principles of that framework, including its fundamental rights protection.[776] The obligation to comply with EU fundamental rights, however, once within the scope, cannot be limited. In *Åkerberg Fransson*, the Court clearly stated that

> …situations cannot exist which are covered in that way by European Union law without those fundamental rights being applicable. The applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter.[777]

This applies to all forms of direct, indirect and even partly regulations.[778] The essential question in that regard, is how far the actual 'implementation' of Union Law in article 51 of the Fundamental Rights Charter can be extended to affect surveillance issues.

The answer to this question depends heavily on the purpose and field of law in which certain surveillance measures take place. That is also why there is no easy answer to that question and the applicability of the EU Fundamental rights framework is subject to debate.[779]

What is important to note, though, is that article 4 (2) of the TEU establishes a clear exemption for national security issues. Certain core state functions shall be respected, including '…the territorial integrity of the State, maintaining law and order and

---

[775] See Rosas A and Armati L, *EU Constitutional Law: An Introduction* (2nd edn, Hart Publishing 2012), 167.

[776] See Spaventa, E, 'Fundamental Rights in the European Union' in Barnard C and Peers S (eds), *European Union Law* (Oxford University Press 2014), 232.

[777] Case C‑617/10 *Åklagaren v Hans Åkerberg Fransson*, (Grand Chamber), 26 February 2013 ECLI:EU:C:2013:105, para 21.

[778] For a more detailed discussion see Spaventa E, 'Fundamental Rights in the European Union' (n 776), 240-241.

[779] Ibid, 232 -234, see also Schütze R, *European Union Law* (Cambridge University Press 2015), 430-438. For general discussion on the horizontal effect of fundamental rights in the EU see Walkila S, *Horizontal effect of fundamental rights contributing to the 'primacy, unity and effectiveness of European Union law'* (Diss, University of Helsinki, 2015), 85-91.

safeguarding national security. In particular, national security remains the sole responsibility of each Member State.'[780]

There are, however, certain aspects to mass surveillance that can fall within the scope of EU law. Data protection, in particular, is an area of the law that falls within the scope and which has been heavily regulated by employing a number of instruments. ever since the beginning of the information age. The EU Data Protection Directive, for example, applies to personal data issues, unless outside its scope of application, e.g. when data processing falls within the so called 'household-exemption' and in cases of '…public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.'[781] Similarly, the 2008 EU Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[782] contains an exclusion of national security and security interest. Problematic in this regard, of course, is the principal indeterminacy of the term 'national security'.[783] Its interpretation can vary drastically in dependence to the circumstances of application.

In April 2016, the Data Protection Directive as well as the Framework Decision were replaced by the General Data Protection Regulation and a new Directive applying to data processing for law enforcement and public sector processing.[784] While the GDPR has a similar limited scope as the former Directive 95/46, the new 'law enforcement'-Directive applies to all data processing '…by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'[785] At the same time, however, article 2 3) (a) of the 2016/680 Directive excludes data processing 'in the course of an activity which falls

[780] Art 4 (2) TEU.

[781] See Art 3 (2) Directive 95/46/EC (Data Protection Directive) (n 305).

[782] EU Framework Decision 2008/977/JHA (n 589).

[783] See Article 29 Data Protection Working Party (Art 29 WP), Working Document on surveillance of electronic communications for intelligence and national security purposes, 5 December 2014, 14/EN WP 228, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf accessed 10 January 2016, 22-23.

[784] See Regulation (EU) 2016/679, (GDPR), (n 303); Directive (EU) 2016/680 (n 303).

[785] Art 2(1) and 1 (1) Directive (EU) 2016/680 (n 303).

outside the scope of Union law'. The purpose and scope of the Directive appears therefore either expansive or contradictory, as 'public security' and the prevention of threats thereto could intuitively be seen to fall outside the scope of Union Law.

Additionally, while the replaced Council Framework Decision 2008/977/JHA was limited to the transfer of personal data between member states, it appears the new Directive takes a more inclusive stand. This is interesting, because it raises the question in how far data processing in public surveillance systems would fall under the new 2016/680 Directive and therewith become subject to additional EU fundamental rights safeguards of the EUCFR.[786]

General surveillance and wide scale data collection can ntrigger the applicability of EU fundamental rights. For example, when private entities collect data such as, e.g., when the owner of a grocery store installs video surveillance in her premises. In that case, the private owner or company has to be regarded as a data controller in light of the EU data protection framework – and corresponding EU rules are applicable.

Consequently, although 'national security' in general excludes the application of EU data protection frameworks, once EU companies and private entities collect, retain and process personal data and transfer these data to security authorities including intelligence agencies, this transfer can be seen as falling within the scope of EU law.

This applicability has been emphasized by the CJEU in several cases addressing data protection as a fundamental right issue in the EU: In *Digital Rights Ireland*, the CJEU made clear that a Directive obliging States to implement laws that force telecommunication companies to retain communication meta-data has to be tested for validity in light of EU fundamental rights, especially the right to private life and data protection in arts 7 & 8 of the Charter of Fundamental Rights.[787]

A similar approach was taken by the CJEU in the *Schrems* judgment: the transfer of personal data to a third country requires the same levels of fundamental rights

[786] See De Hert P and Papakonstantinou V, 'The New Police and Criminal Justice Data Protection Directive. A First Analysis' (2016) New Journal of European Criminal Law 7, 10.

[787] See Cases C‑293/12 and C‑594/12 *Digital Rights Ireland*, (n 324) paras 23-31.

protection as in the EU, especially when such data might be transferred to law enforcement or security authorities.[788]

> In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (…).[789]

It has to be concluded in this context, that once surveillance data are collected, retained or processed by private actors and such data are accessed by security authorities, the assessments of the legality of such actions have to be based on the Charter of Fundamental Rights and the relevant EU data protection and privacy regulatory frameworks. EU data protection law then applies to all forms of corporate, private as well as private security operations in public places. This causes a controversial situation in terms of public surveillance: While a surveillance camera which is installed and operated by a police force might not fall into the scope of EU law and the Charter of Fundamental Rights, a surveillance camera installed and operated by a private actor might very well do so. This would mean that private actors are directly bound by EU fundamental rights, while public actors are, in principal excluded, at least from a direct application of the EUCFR. Systematic mass surveillance by states, however, would still be likely to fall into the scope of protection because such practices often require derogations from relevant EU directives in the respective field, provided that such derogations fall within the scope of application of the EUCFR.[790]

It is clear, however, that the CJEU has significantly strengthened the rights to private life and data protection during recent years. Government mass-surveillance has been seen especially critical when there appears to be a lack of oversight and remedy. Ironically, the CJEU has addressed here especially the US system of mass-surveillance which came into the focus after the Snowden revelations. The *Schrems* judgment, in which the CJEU declared the EU/US safe-harbour framework as essentially

---

[788] Case C-362/14 *Schrems*, (n 325).

[789] Ibid, para 94, see also Cases C‑293/12 and C‑594/12 *Digital Rights Ireland*, (n 324), para 39.

[790] In how far derogations from EU legal instruments constitute 'implementation' of EU law pursuant to Art 51 of the EUCFR is disputed. This discussion is left out from this work. For a rather straightforward approach see FRA, Surveillance by Intelligence Services, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf accessed 6 Mai 2015, 11

incompatible with EU fundamental rights norms reflects such a turn. Due to the above-mentioned restriction of the scope of EU law however, it is questionable how far the CJEU would be able to directly address government surveillance frameworks. However, *Digital Rights Ireland* and *Schrems*, as well as to a certain extent also *Google Spain* have shown that EU fundamental rights ought to be taken seriously in the EU and that governments and security authorities do not enjoy a carte blanche from a EU law perspective when operating systems of mass surveillance. In any case, even if the EU right to privacy and data protection framework were left out of the consideration, both the ECHR as well as the Council of Europe Convention 108 and its 2001 Additional Protocol guarantee data protection standards in cases of mass surveillance.

***

3.2.4 Mass Surveillance and Dignity

Mass surveillance of public places triggers a variety of fundamental rights arguments. There is enough case law to confirm that mass surveillance in public places will trigger issues in relation to private life and article 8 ECHR, especially when individuals can claim a specific personal effect. Even if that cannot be proven, mass surveillance cases can still be admissible within the ECHR framework, provided they pass the above discussed test in *Kennedy* and *Zakharov*.[791] Vast technological security systems enabling surveillance and control of public spaces therefore trigger individual rights issues which can be challenged by affected individuals employing fundamental rights frameworks. This applies both to the ECHR and the EU rights frameworks. There is however another aspect of mass surveillance which deserves deeper discussion at this point.

Throughout this study, two fundamentally different approaches towards privacy and surveillance became visible. Those became clear already in the section on the philosophical foundations of privacy in the beginning of this study. Simplified, those arguments go as follows: on the one hand, privacy in public is legally protected in a narrow way. It has to be interpreted in connection with the individual's expectation to

[791] See Section 3.2.2 above.

be visible to others. Once in a public place, an individual enjoys less privacy protection than in the secluded private sphere of the home. On the other side, privacy extends beyond the pure private sphere. Individual self-determination, the right to form relationships with others, personal autonomy, identity and freedom of decision making and choice are as well in a certain way an inherent part of the concept of privacy. The chilling effect, in which an individual alters her behaviour as a response to real or alleged surveillance is part of such an argument. Such argumentation may be derived from concepts such as a right to personality or dignity.

The question arising from this in the context of urban mass surveillance at this stage is therefore, if there is legal evidence that a sophistication of surveillance and security technology in public spaces require a reformulation of such concepts. After all, simply the massively improved capabilities and sophistication of surveillance might lead to the necessity of articulating a clear and precise fundamental rights argument challenging mass surveillance beyond individual rights and its common arguments. In that sense, there could be a need for the formulation of a collective right to be free from surveillance and control also in public unless there are adequate justifications and safeguards. How can a mass surveillance scenario be legally challenged from a more collective perspective?

3.2.4.1 Personal Autonomy and Self-Determination

This study has previously discussed the use of a legitimate expectation test in the ECHR system. The Court held in the already excessively discussed *P.G. and J.H* case that

> (…) there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.[792]

[792] *P.G. and J.H. v the United Kingdom*, (n 500), para 57.

This means basically that individuals have a lesser expectation of privacy in public spaces as compared to their secluded private spaces. Furthermore, this only applies once the system does not collect personal data – because personal data *per se* interferes with the right to private life in article 8 ECHR. Additionally, however, the ECHR system also protects '(…) a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world.'[793] Private life therefore cannot only include a clearly secluded real or virtual space, but there are areas of public life and publicity that are important if not crucial for a person's life. This seems to be also in mind of the ECtHR when not limiting its interpretations of private life to a secluded inner sphere of an individual.

In that sense, it can be argued that using legitimate expectation of individuals to determine the scope of their privacy has severe shortfalls. One problem with the expectation of privacy argument is that it bases the assessment of intrusiveness of individual surveillance on the subjective perception of the surveillance through that individual. Ultimately, this would mean that simply making people aware of surveillance (ensuring they expect to be surveilled) and therewith lowering their 'expectation' means that surveillance is more justified.[794] In this sense it would be questionable if notifying people about surveillance as such can be sufficient for its justification especially in light of the enormous sophistication and capabilities of surveillance means and methods.

Within the ECHR framework, several notions appear to counter the legitimate expectation argument: the 'right to identity', 'personal development' and the 'right to establish relationships with other human beings and the outside world' have been explicitly mentioned by the ECtHR on several occasions.[795] In connection with this, the ECtHR has also used the notion of self-determination and personal autonomy as a fundamental rights principle. 'Although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying

[793] Ibid, para 56, see also *Niemietz v Germany*, (n 739), para 29, and *Halford v the United Kingdom*, (n 510), para 44.

[794] See Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' (n 162), 48.

[795] *P.G. and J.H. v the United Kingdom*, (n 500), para 56.

the interpretation of its guarantees.'[796] Self-determination, personal autonomy and personal freedom can therefore be interpreted to lie at the core of article 8 ECHR, yet, when it comes to surveillance cases, this notion has hardly been employed by the Court. Personal autonomy and the right to self-determination, however, were frequently discussed in cases concerning identity, transgender and discussions around the 'right to die' in the *Pretty* case.[797] Yet, the relationships and nature of such notions in the ECHR are far from clear.

In this regard, Nelleke Koffeman sketches two interpretations of the relationship of human dignity, personal autonomy and freedom. The first line of interpretation understands '…personal autonomy as a general principle of law on equal footing with human dignity and personal freedom',[798] while the second interpretation sees, '…personal autonomy as a right in itself with a specific content and with human dignity as its underlying value.'[799] Personal autonomy and the right to self-determination can be interpreted either as a notion deriving from the general concept of dignity and freedom - after all, the ECtHR has found that '[t]he very essence of the Convention is respect for human dignity and human freedom'[800], or as a separate right in itself.

Whichever interpretation is favoured, it is in a way conceivable that massive surveillance of public spaces can restrict personal autonomy, freedom and self-determination and is therefore essentially an interference with human dignity. In that sense, thought even further, private life, backed up by the notions of dignity and self-determination, is an essential prerequisite for keeping up societal forms of organization. Rouvroy and Poullet advocate for the right to privacy to be understood as '…an *instrument* for fostering the specific yet changing *autonomic capabilities* of individuals that are, in a given society at a given time, necessary for sustaining a vivid

[796] *Pretty v The United Kingdom*, (n 258), para 61.

[797] Ibid.

[798] Koffeman NR, (The right to) personal autonomy in the case law of the European Court of Human Rights (n 745), 5.

[799] Ibid, 7.

[800] *Pretty v The United Kingdom*, (n 258), para. 65. For the first time this formulation was used in *C.R. v the United Kingdom*, App no. 20190/92, Judgment (Court), 27.09.1995, para 42.

democracy.' [801] Based on freedom, autonomy and dignity, privacy becomes a vanguard to counter interferences and restrictions into individual lives and freedoms through coercion and manipulation by states.

3.2.4.2 Dignity and State Surveillance

In fact, a very sophisticated and early legal argument deriving a specific privacy related right from dignity is found in the case law of the German Federal Constitutional Court already in the 80s. In 1983, the Federal Constitutional Court developed a 'right to informational self-determination' from a combination of the right to freely develop one's own personality (art 2(1) German Constitution), and the general inviolability of human dignity in article 1(1) of the German Constitution.[802] This general personality right in the Constitution explicitly protects the dignity of persons as free members of a free society.[803] In this regard, every individual has the ability and competence to decide for herself in what way her personal information is distributed and shared, but this ability is threatened through new technological means of data processing.[804] The FCC interestingly emphasized that technological means of data gathering and processing as well as the combination of information from a variety of sources and the use of integrated information technological systems inherently come with the threat that an individual loses control over personal information.[805] The core of the argument, however, lies in the threat of behavioural coercion and the possible loss of freedom that comes with uncontrolled and intransparent data collection of individuals:

> The right to informational self-determination would not be compatible with a societal order and a corresponding legal order in which citizens can no longer ascertain who knows what about them, when and in which occasion. Who is uncertain as to whether deviant behaviour is taken note of at all times and whose

[801] Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' (n 162), 46.

[802] [Germany] FCC, BVerfG, 15. Dezember 1983 (Volkszählungsurteil), (n 145).

[803] Ibid, II (1) A), para 170.

[804] Ibid.

[805] Ibid, para 171.

> information is the permanently stored, used or transferred, will attempt to avoid standing out through such behaviour.[806]

This might go so far as the exercise of fundamental rights are avoided, for example participation in political protest. The FCC emphasized especially that this could heavily interfere with personal development and the common good: '…self-determination is an elementary prerequisite for a free and democratic community based on its citizens' abilities to act and participate in it.'[807]

With this judgment, the FCC not only created a powerful dignity and personal autonomy- based argument against uncontrolled information collection from citizens, it also formed the new right to informational self-determination in the German constitutional legal framework. This right was a direct response to technological development of massive data collection and derives from a general personality right in combination with human dignity. It should probably be noted that the German Basic Law does neither include a separately formulated right to privacy, nor a data protection clause.

What makes such an argument interesting and relevant for surveillance analyses in the context of European fundamental rights protection, is that the German FCC has formulated a dignity based criticism of mass surveillance: It applied its interpretation on a right to informational self-determination to a case contesting public video surveillance in the city of Regensburg in 2007.[808]

The city planned to install four video surveillance cameras including a video recording function in a public place. The purpose for the video surveillance was to monitor a street art project that the city had installed on that place, in which the relief of a medieval synagogue was made partially visible to the public. The FCC found that recorded video surveillance in public places *per se* constituted an interference with the right to informational self-determination. It argued, firstly, that the surveillance was indiscriminate and affected all individuals moving in the public place. However, as a matter of proportionality, interfering measures should foremost be directed at the

[806] Ibid, para 172 (own translation).

[807] Ibid, para 172 (own translation).

[808] See [Germany] FCC, BVerfG, Beschluss der 1. Kammer des Ersten Senats (Decision, 1st Chamber, 1st Senate), 23 February 2007, 1 BvR 2368/06.

perpetrators of criminal offences.[809] Secondly, the video recording enabled intensive processing of picture materials and the comparison and connection with other personal data. Thirdly, and probably most importantly, the surveillance at stake aimed at manipulating the behaviour of individuals in the public sphere.[810] As such, the video surveillance was found unconstitutional as it lacked adequate safeguards.[811]

This FCC judgment employed an argumentation based on the construction of a right to informational self-determination deriving from a personality right in combination with human dignity. The legal argumentation focused on the 'chilling-effect' of surveillance technologies on people in public places. Self-restriction and loss of freedom could result in a major damage for democratic activities. In a German constitutional context, such public place surveillance is only permissible when it has a strict and narrow purpose and when it is strictly regulated and safeguarded by adequate legal frameworks. What is interesting about the focus on manipulating behaviour is that it does not challenge the surveillance and its practices as such, but the attempt to target and manipulate individual behaviour in a public space. This means that the FCC made an argument explicitly challenging the intention to control public spaces.[812]

The construction of a right to informational self-determination as the 'constitutional anchor' of data protection in the German system[813] has not lost its actualities. In fact, it can serve as a powerful argument against unfettered data collection from public places. Connecting data protection to a personality right allows the addressing of a variety of problems stemming from surveillance technologies, and furthermore allows a response to technological developments severely affecting individuals in public spaces. A pure focus in individual expectations in public places, on the other hand, will not be able to address the technological sophistication of surveillance. The limits

[809] Ibid, para 51.

[810] Ibid, para 52.

[811] Ibid, para 56.

[812] See also [Germany] FCC, BVerfG, Urteil des Ersten Senats (Judgment, 1st Senate), 11 March 2008, 1 BvR 2074/05, where the FCC employed a similar line of argumentation in a case concerning ANPR. (esp. paras 61-69)

[813] See Hornung G, Schnabel C, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 28 Computer Law & Security Review 84, 86.

of an individual expectation approach are directly proportional to technological sophistication: The more complex and capable a technology becomes the more difficult it will be for an individual to grasp the whole complexity. Additionally, technological sophistication lowers the level of privacy expectation as such. If it is generally known that there exist the potential for a wide array of partly hidden sensors in public spaces, privacy expectations would essentially drop to zero, in turn, legitimating the use of surveillance technologies as such. A 'effect on personality'-approach, on the other hand, does address the possible effects of such public surveillance capabilities on a person's identity, personality and freedom.

3.2.4.3 EU, Dignity and Surveillance

Challenging privacy by employing perspectives deriving from dignity did not remain a German exclusivity. Some scholar argue that privacy is conceptualized in different ways between Europe and the US. While it is based essentially in individual expectations and liberty in the US, in Europe, conceptions of privacy are deeply rooted in the concept of human dignity.[814] In Europe, the right to informational self-determination, when it is understood as an essential capability for individuals to control the collection and sharing of personal information, is seen as essentially based on the perceived dignity of an individual in public, while in the US, legal interpretations of privacy are based on a freedom from interference through the State.[815] While this can certainly be interpreted in many ways, 'dignity', as a concept, plays a significant role in the fundamental rights framework of the European Union. The EU was founded, according to the preamble of its Charter of Fundamental Rights '…on the indivisible, universal values of human dignity, freedom, equality and solidarity' and '…is based on the principles of democracy and the rule of law'[816] and Article 1 of the same Charter reads: 'Human dignity is inviolable. It must be respected and protected.'[817] With this, dignity has to be seen as a central element to European fundamental rights interpretations.

[814] See for example Whitman JQ, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 The Yale Law Journal 1151.

[815] Ibid, 1161.

[816] Charter of Fundamental Rights of the European Union, 18.12.2000, OJ 2000/C 364/1, Preamble

[817] Ibid, Art 1.

The right to informational self-determination based on human dignity, however, has not found a direct way into the CJEU case law. The reason for this may be that in the EU context, privacy as well as data protection find more specific formulations and therefore making a *lex generalis* articulation less necessary. The EU legal framework has established very detailed regulations for privacy, and especially data protection, making it possible to address surveillance issues without taking a detour in establishing a fundamental right through dignity. Privacy and data protection are clearly defined as fundamental rights in the European Union and therewith mass surveillance issues can be directly addressed.

3.2.5 Conclusion

This section discussed mass surveillance as a separate issue in the surveillance scenario. Starting with the problems of admissibility and scope, it analysed three different legal arguments addressing mass surveillance in urban public contexts.

Firstly, a right to privacy as enshrined in European human rights regimes, and especially in the ECHR, can tackle mass surveillance in different ways, for example as individual expectation, as a more collective 'menace to society' and as an interfering with a right to establish relationships. Within the ECHR, it is important to note that the more difficult it is to focus on individuals being the direct subject of surveillance, the more a legal argument focuses on general analyses of the abstract features of surveillance systems and their communal effect. The argument that mass surveillance somehow would impede the right to form relationships appears constructed and not very convincing in the context of ECHR mass surveillance case law.

Secondly, this section discussed data protection as a legal argument addressing mass surveillance. It can be concluded that data protection appears, as already discussed above, as a bridging argument between individual and mass surveillance, because systematic data processing on a massive scale enables not only the addressing of interferences with an individual's rights, but also possible overall negative effects of data processing as a whole. Big data and massive data collection come with a variety of risks, provided it concerns data processing of at least somehow identifiable

individuals. Data protection has an additional relevance as it is very likely that mass surveillance data processing falls within the scope of the protection of the EU fundamental rights regime.

Thirdly, this section addressed the argument of privacy as a derivate of dignity. This offers a new perspective on addressing mass surveillance, namely through its societal effects. This argument derives from arguments on dignity made by the German FCC, because it is the one Court in Europe which has taken a strong stand in addressing the problem of mass surveillance through dignity and self-determination. This enables the construction of a privacy perspective based on communal interests, societal interest, and the exercise of control. Too much control in public spaces through mass surveillance appears as a constraining element which can be challenged with reference to societal values rather than individual liberty. In fact, the 'menace to society' argument appears as a similar argument that is less explicitly formulated.

There can therefore be three distinct approaches towards challenging the mass surveillance systems in Helberg. The first one, based on individual liberty and expectation, challenges the surveillance due to their technical sophistication. After all, the hidden and all-encompassing surveillance tools do not allow an individual to expect such a total surveillance.

The second argument allows a citizen of Helberg to challenge the mass surveillance with an argument based on informational privacy: In this interpretation, a right to control and determine information about oneself delivers a strong foundation for the protection of personal data.

Thirdly, an argument entirely based on dignity and personality allows for the articulation of a strong chilling-effect type of argument and therewith a focus on overall negative societal effects of mass surveillance.

The following two sections will now move to a discussion of two further issues relevant for surveillance in the Helberg scenario: namely private actor surveillance and, with an analysis of automation and prediction, a view into the future of urban surveillance.

3.3 Private Actor Surveillance Operations

3.3.1 Private Actors and Fundamental Rights

Public security surveillance traditionally is understood as an issue for public security actors. Public surveillance, understood as targeted or mass-surveillance has in this study been described as an issue of public law, conducted by state authorities. Particularly fundamental rights assessments of public surveillance essentially rely on the classic separation between public authorities and private individuals, where public authorities are bound by fundamental rights. After all, states are bound by fundamental rights, whereas individual natural persons are entitled to fundamental rights.

Within the context of public surveillance, however, much of these clear delineations have become blurred, for example because technologies capable of surveillance have proliferated in the private spheres. Video surveillance cameras, for example, are a standard security feature for private businesses. Private security companies operate vast public surveillance systems and sensors in mobile phones, small video cameras or drones are collecting large quantities of data from public spheres. Leaving aside a deep discussion on fundamental rights obligations in the private sphere and for non-state actors,[818] this section examines the legal consequences of private actors as operators of surveillance systems or as sensor data controllers.

The role of public and private actors in law in general lies at the core of modern theoretical conceptions of legal theory. The common story is, of course, well known and the lines of separation flow along a horizontal vs a vertical understanding of powers and regulation. This section analyses the applicability of European fundamental rights to private actors conducting certain surveillance operations. Hence, there are a couple of possible options that are relevant for an urban surveillance scenario: Private actor surveillance of public spaces, private actor surveillance of semi-public spaces and private actor surveillance of purely private spaces.

The operation of surveillance through private actors is a well-known phenomenon in modern urban environments –and is of special relevance to large-scale surveillance

[818] See e.g. Clapham A, *Human Rights in the Private Sphere* (Clarendon Press 1993); Clapham A, *Human Rights Obligations of Non-State Actors* (Oxford University Press 2006); see also Engle E, 'Third Party Effect of Fundamental Rights (Drittwirkung)' (2009) 5 Hanse Law Review, 165-173, and Walkila S, *Horizontal effect of fundamental rights contributing to the 'primacy, unity and effectiveness of European Union law'* (Diss, University of Helsinki, 2015).

systems.[819] That is because highly sophisticated surveillance systems are often operated by private security companies, on private commission and in functionally closed privately owned spaces such as shopping malls. Again, here, jurisdiction as well as the applicability of law plays a decisive role in the legal assessment.

This section examines the role of private individuals in surveillance operations in light of the scope of data protection in Europe. It particularly focusses on the so called 'household exemption' in European data protection law and its role in balancing the use and gathering of personal information by private individuals from public spheres.

3.3.2 Private Surveillance Operations in Public Areas

This section starts with an analysis of a small-scale surveillance operation: assuming a house-owner in Helberg would operate a video surveillance system primarily to monitor her own door entrance.

The legal framework applying in this case is of course the national legal system and here it depends on the State's regulation of privately owned and operated surveillance systems in private spaces. While human and fundamental rights protection mechanisms do not prima facie bind natural persons, the detailed regulation of video surveillance in public places derives from the relevant data protection regulations on the national level. National regulation, however require compliance with international fundamental rights obligations as well as EU law, particularly the EU Data Protection Directive and the directly applicable new General Data Protection Regulation (GDPR), as both explicitly apply in the private sphere.[820]

Generally, video surveillance is a form of processing personal data. Video surveillance contains data that enables the identification of an individual through physical identity and collects information that relates to this identified individual. Private individuals or corporations filming public areas therefore might be considered data controllers

[819] See e.g. Jones, T and Newburn, T, *Private Security and Public Policing. Clarendon Studies in Criminology* (Clarendon Press Oxford 1998); Wakefield A, 'The Public Surveillance Functions of Private Security' (2004) 2 Surveillance & Society 529; Marquis G, 'Private security and surveillance. From the "dossier society" to databanks networks.' In Lyon D (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003), 226-248.

[820] See Directive 95/46/EC (Data Protection Directive) (n 305), Regulation (EU) 2016/679, (GDPR), (n 303), Art 2(1).

pursuant to the GDPR and the Directive. The material scope of the GDPR is limited when the issue falls outside of Community Law, when it falls within Chapter 2 Title V of the TEU and when authorities process personal data for criminal and judicial matters.[821] Article 2 (2) GDPR additionally contains a scope limitation for data processing by 'natural person in the course of a purely personal or household activity'.[822] Also, the EU Data Protection Directive contains this so called 'household exemption'.[823]

The intention behind the household exemption is clear: There are certain information collected and retained by private individuals which clearly qualify as personal data, for example personal address books or a calendar containing birth dates of family and friends. Such information, used for purely personal activities should probably not be strictly regulated by the European data protection frameworks. With technological advancement, however, new questions have emerged, for example how the household exception should be applied to the publication of information on the internet.[824] Those questions are not particularly new and have been discussed previously: Article 29 Working Party, for example, has posed this question with regards to social network services (SNS) already in 2009. The Working Party stated that despite users as data subjects are generally exempt from the Data Protection Directive, there may be instances where users '…may not be covered by the household exemption and the user might be considered to have taken on some of the responsibilities of a data controller.'[825] Consequently, also the GDPR, albeit taking over the formulation of the household exemption from the Data Protection Directive, states in the recitals:

> This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no

[821] See Art 2 (2) a), b), d) Regulation (EU) 2016/679, (GDPR), (n 303).

[822] Ibid, Art 2 (2) c).

[823] Art 3 (2) Directive 95/46/EC (Data Protection Directive) (n 305).

[824] For further discussions see e.g. Wong R, Savirimuthu J, All or Nothing: This is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet (2008) 25 John Marshall Journal of Computer & Information Law; and Warso Z, 'There's more to it than data protection – Fundamental rights, privacy and the personal/household exemption in the digital age' (2013) 29 Computer Law & Security Review 491.

[825] See Article 29 Data Protection Working Party (Art 29 WP), Opinion 5/2009 on online social networking, Adopted 12.06.2009, 01189/09/EN WP 163, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf accessed 1 February 2017, 5,6.

> connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.[826]

The GDPR recital appears in line with previous case law on the household exemption and the Data Protection Directive. In *Lindquist*, the Court referred to recital 12 of the 1995 Directive's Preamble in order to find that publications and dissemination of personal data through private individuals are not covered by the household exemption and do hence fall within the scope of the Directive.[827] According to the Court, the exemption only covers activities '…which are carried out in the course of private or family life of individuals.'[828] Consequently, also in *Satamedia*, the Court followed that view and excluded the collection, processing and publication of publicly available personal tax information from falling under the household exemption.[829]

The rather strict application of the household exemption extends also explicitly to surveillance operations by private individuals.

In *Ryneš*, a CJEU judgment from December 2014, the 4th Chamber had to address the question, if a video surveillance system installed by a private individual on private ground for the purpose of protecting property, health and life of the owners of the home would fall within the household exemption of Art 3(2) of Directive 95/46/EC, despite the fact that the camera also captured partly public areas.[830]

František Ryneš, a Czech national, installed a fixed video camera in his family home which recorded the entrance of his home, a public footpath as well as the entrance of the opposite house after the windows of his family home were repeatedly broken by unknown perpetrators.[831] After another attack on his home, the video surveillance data was handed over to the police and two suspects were identified and criminal

---

[826] Regulation (EU) 2016/679, (GDPR), (n 303), Recital 18.

[827] See Case C-101/01 *Lindquist*, Judgment (Court), 6 November 2003, ECLI:EU:C:2003:596, paras 46-48.

[828] Ibid, para 47.

[829] See Case C-73/07 *Satakunnan Markkinapörssi and Satamedia*, Judgment (Grand Chamber), 16 December 2008, ECLI:EU:C:2008:727, paras 43-45.

[830] See Case C-212/13 *Ryneš*, (n 107), para 18.

[831] Ibid, para 13.

proceedings initiated, in which the video surveillance material was used as evidence. Subsequently, one of the suspects challenged the lawfulness of the installed video surveillance system before national Courts.

In answering the referred question, the CJEU concluded that such a system did not fall within the household exemption and hence fell into the scope of the Directive.[832] The Court emphasized that in order to fall within the household exemption, the activity would need to lay 'purely' within a personal or household area, such as communications or address books.[833] However, as the video surveillance equipment was partially filming and recording a public space, and hence it was

> …directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46.[834]

The Court, however, also stated that

> …Directive 95/46 makes it possible, where appropriate, to take into account (…) legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself (…).[835]

In reaching this conclusion, the Court also took a turn towards a fundamental rights approach to data protection. In its opinion, '…Directive 95/46 is intended to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data…'[836] and referred to Case C-131/12 *Google Spain* when stating that

> …Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter….[837]

It becomes clear that the household exemption needs to be narrowly construed and interpreted when determining the scope of the Data Protection Directive and the

[832] Ibid, para 35.

[833] Ibid, paras 31, 32.

[834] Ibid, para 33.

[835] Ibid, para 34.

[836] Ibid, para 27.

[837] Ibid, para 29 and Case C-131/12 *Google Spain* (n 315), paras 66, 68.

GDPR. Furthermore, the CJEU has more and more taken an approach in which it has made very clear that Directive 95/46/EC needs to be interpreted in light of the established fundamental rights standards in the European Union. In *Ryneš*, it appeared that the Court was very reluctant to leave data processing outside the scope of the European Data protection framework, the moment it touches upon spheres that reach outside of what can be considers to be within a private and household sphere. Therewith, the Court construed the sphere in which data protection frameworks do not apply to private individuals very narrowly. It can even be concluded that processing data as a private individual does not serve as a shield against responsibilities concerning data protection obligations. Any surveillance systems operated by private individuals hence falls within the scope of EU data protection frameworks once it affects persons outside a narrowly construed private sphere. Considering this narrow interpretation as well as the special emphasis of high fundamental rights standards when it comes to data protection, it can be concluded that surveillance systems operated by private entities will fall within the scope of European data protection law and its strong fundamental rights- based approach.

Here, new technology is especially affected, due to three issues that have become especially relevant in the recent years and that seem to have played a decisive role in interpreting the scope of the Directive and therewith the scope of the EU data protection framework. Firstly, obtaining and retaining personal data from (at least partially) public or semi-public places as it happened in the *Ryneš* -case. Secondly, the retention and transferal of personal data to a third party –e.g. to a security authority such as the police, or an insurance company, and thirdly, the publication of the personal data either in publicly available media (such as online video platforms) or on social media/social network services, where the dissemination might be a little more limited. In the *Ryneš*-case, for example, the data has been transferred to the police and used as evidence.

Those questions become even more pressing, once one considers the recent spread of data recording and data dissemination devices available to private individuals. Recently, debates on the legality and use of so called dash-cams have gained attention in some EU Member States.

Dash-cams, are small video and audio recorders that can be mounted on a windscreen of a car. Typically, those devices record images and sound for a certain time, until the storage capacities are full at which point the device starts recording over the oldest data. Those recording times vary according to the sophistication of the device, but they can have from one hour up to 24h recording times, depending on the drive-space in the device. Usually, dash-cams are installed for several purposes, from filming nice landscapes up to securing evidence and protection of legal interests in case of accidents. Similarly, small weather-proof and outdoor-safe recording devices, so called action-cams, can be mounted on people's helmets, bikes, motorbikes, hats and cars, enabling editing and publication of all kinds of activities, from skate-boarding to motor-bike tours. This has the effect that in case of accidents or other incidents, those recordings can be handed over to the police or insurance companies as evidence and/or can be uploaded and published on social media and video platforms. Considering the overall proliferation of wearable devices such as, for example, smart watches or glasses, it goes without saying that those questions will become very relevant for modern data protection regulation and fundamental rights.

Regarding the above-mentioned judgments as well as the turn towards and emphasis of fundamental rights elements in data protection law, it is difficult to argue that filming public space for the purpose of publication or transferal would not fall under the scope of the data protection directive. The regulation of dash-cams is far from unified in the European Union, being illegal in some States while legal in others.[838] A legal argument often associated with States in which dash cams are considered unproblematic is that video recording in public places should not be banned unless it explicitly violates privacy where people can reasonable expect to have privacy.[839] On the other side, arguments claim that video surveillance requires areal limitation and special permission.[840] Unsurprisingly, a particularly strong legal argument against the use of dash-cams be found in Germany: The Düsseldorf-circle, a part of the conference of German DPAs on federal as well as the 'Länder'- level dealing with data-protection

[838] See Štitilis D and Laurinaitis M, 'Legal regulation of the use of dashboard cameras: Aspects of privacy protection' (2016) 32 Computer Law & Security Review 316.

[839] Ibid, 323.

[840] Ibid.

on the non-public level, for example, regards the use of private video surveillance from vehicles on public roads as being not in accordance with data protection standards.[841] Their argument emphasized that the employment of dash-cams in vehicles is not permissible unless it clearly falls within the household-exemption. If the employment does not fall into the household exemption, the use has to be in line with German Data Protection Law according to which the processing needs a clear and legitimate purpose and the interests of the controller needs to outweigh the negative effects on the affected data subject.[842] The car driver's interest to operate dash-cams, recording video and audio for the primary purpose of providing evidence in case of accidents or traffic incidents, does not justify the mass violation of the right to informational self-determination of the subjects recorded on the video.[843] The interest hence does not justify the interference into the right of individuals to move freely in public space, '…without having to be afraid to unwillingly and causelessly become subject to video surveillance.'[844] This argument was even supported by a regional Administrative Court decision in 2014. In the case, the regional data protection authority ordered the removal of a dash-cam installed and operated by a lawyer in his personal vehicle and requested the deletion of all recorder material. The lawyer challenged the order in front of the administrative court.[845] Although the order was not upheld due to some formal and procedural flaws it contained, the Court confirmed the view of the data protection authority that the installation and operation of a dash-cam constitutes a grave violation of data protection laws and that it does not fall within the household-exemption.[846] The Court regarded surveillance of a public area using a dash-cam installed in a vehicle as a form of control that affects large

[841] See Düsseldorfer Kreis, Beschluss vom 26.02.2014 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams), http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/26022014_UnzulaessigkeitDashcams.pdf?__blob=publicationFile&v=1 accessed 15 March 2015.

[842] Ibid, 1; and §6b (1) 3., §6b (3), Bundesdatenschutzgesetzes (BDSG) [Germany], 14. Januar 2003, BGBl. I S. 66, das zuletzt geändert durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162).

[843] Düsseldorfer Kreis, Beschluss vom 26.02.2014, (n 841), 1.

[844] Ibid, 1 (own translation).

[845] See [Germany], Verwaltungsgericht (VG) Ansbach, Judgment, 12. August 2014, Az. AN 4 K 13.01634.

[846] Ibid, paras 56, 66.

numbers of individuals who had no possibility to foresee the surveillance. Therewith, the personality rights and right to informational self-determination clearly outweigh the interests of the dash-cam operator.[847]

In dash-cam cases, one additional problem is the weighting of interests. Naturally, in case of a serious accident involving for example bodily harm, the interest of the injured persons might outweigh data protection or personality rights of possible bystanders. In that sense, a necessity and proportionality assessment can help in balancing rights and interests. Nevertheless, as Balzer and Nugel rightly notice, while recording just before and during an accident might be qualified as necessary and proportional, the daily recordings that happen throughout time that are not connected to the incident are the real challenge to data protection.[848] Furthermore, permanent recordings from cars might create a permanent surveillance-pressure ('Überwachungsdruck') for the affected public for '[a]s long as the traffic participant [the operator, own insertion] has the possibility to manually retain and view the recordings permanently'.[849]

This is an interesting general argument against mass surveillance in public areas based on an understanding of data protection and privacy on dignity/personality rights. The mass data gathering with a variety of sensors from public areas could create a 'surveillance pressure' which manipulates and suppresses all sorts of behaviours and expressions within a physical public place. The German arguments against dash-cams therefore offer a vivid legal explanation on a possible chilling effect of surveillance. But they also form a legitimate expectation argument, as the question arises if it could be presumed that individuals can expect a holistic and ever present surveillance in public spaces.

It is ever more important to discuss the effects and possible responses to private data collection in public since many more cases that fall within this category will probably appear in the future. Wearable sensors and cameras, such as for example the famous, although for now discontinued Google's 'Glass' project, which was basically a

[847] Ibid, paras 75-82.

[848] Balzer T and Nugel M, 'Minikameras im Straßenverkehr - Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen' (2014) Neue Juristische Wochenschrift 1622, 1627, 1628.

[849] Ibid 1627 (own translation).

smartphone shaped and worn as glasses, or other wearable sensors gathering data about individuals in public. Those devices would enable the permanent micro-surveillance of public areas. Another example is the integration of cameras and sensors in driving assistance systems of cars and their increased automation, or the retention car sensor data in 'black-boxes'.[850]

Generally, what makes all those situations more complicated, is that in many of those cases, sensor data is transferred, retained and processed also by third-party service providers, may that be an insurance or the police in case of a traffic accident. Technological sophistication, networking and proliferation of sensor technologies will unavoidably here and there collect –even if involuntarily- personal data of people in public places. This may lead to serious interferences with privacy and data protection rights, requiring adequate legal responses

***

Another important technological trend that might play a decisive role in future surveillance is the tendency towards smart surveillance and the use of data from sensors implemented in the direct private environment of surveillance subjects. The so called 'internet of things' with its ever-expanding proliferation of small devices that collect and send data and that create networks might ultimately be used or even integrated into surveillance systems. While the internet of things can be used for data gathering in public spaces, it will ultimately expand the possibility of data gathering into the sphere of the home, and therewith into a closed private sphere originally anticipated as the very essence of private life.

In February 2005, a EU FP6 Project called SWAMI: 'Safeguards in a World of Ambient Intelligence' started their project on the 'Internet of Things' which they described as a future

> …world of smart dust with networked sensors and actuators so small as to be virtually invisible, where the clothes you wear, the paint on your walls, the

[850] See Duri S and others, Framework for security and privacy in automotive telematics, in: (2002) Proceedings of the 2nd International Workshop on Mobile Commerce, 25–32, http://www.cc.gatech.edu/projects/disl/courses/8803/backup/readinglist_files/p25-duri.pdf accessed 7 March 2015, 25.

> carpets on your floor, and the paper money in your pocket have a computer communications capability.[851]

The project analysed technological advancements and proliferation of computer and network technology into everyday environments and private households, focusing on threats and vulnerabilities[852] as well as possible safeguards of these technologies.[853] The project mainly assessed the technological components of data gathering throughout public and private spheres, and the fact that all this data can be useful for surveillance purposes. Also, the EU ISTAG group had an expressed their vision on ambient intelligence in 2003:

> …humans will, in an Ambient Intelligent Environment, be surrounded by intelligent interfaces supported by computing and networking technology that is embedded in everyday objects such as furniture, clothes, vehicles, roads and smart materials - even particles of decorative substances like paint. AmI implies a seamless environment of computing, advanced networking technology and specific interfaces. This environment should be aware of the specific characteristics of human presence and personalities; adapt to the needs of users; be capable of responding intelligently to spoken or gestured indications of desire; and even result in systems that are capable of engaging in intelligent dialogue.[854]

More than 12 years after the report, some of the visions have materialized: Although home-automatization, such as the 'smart' fridge, which communicates that there is a cucumber rotting away in the back of the fridge and automatically orders a fresh one on the internet, is still not an everyday household device, it is clear that devices will increasingly become networked and 'smart'.

What is interesting, at this point, is how far such developments amount to data collection activities through private individuals. For example, a home video surveillance system including facial recognition capabilities which connects to data from the 'smart' fridge could keep track of the consumption of alcohol in a household. Would the controller of the system then be a data controller pursuant to the GDPR?

---

[851] Wright D and others (eds), *Safeguards in a World of Ambient Intelligence* (Springer 2010), 1.

[852] Ibid, Chapter 4.

[853] Ibid, Chapter 5.

[854] IST Advisory Group: Ambient Intelligence: from vision to reality, For participation – in society & business. https://cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf accessed 26 February 2017, 8.

What if the system collected data of third parties e.g. party guests? Considering *Ryneš*, it might be highly likely that such operations would fall within the scope of data protection laws, especially when it concerns third parties outside of the closed private sphere. Taking into consideration the recent developments in European data protection laws and the turn to fundamental rights, it is clearly not a purely personal or household operation if a person creates a sophisticated surveillance system within their own private space if that surveillance affects third-party individuals Another interesting factor in the household exemption would be the intention to spy on other members of the household, e.g. the children without their explicit knowledge or consent. The outcome of such possible cases is far from clear, however, there is at least a clear fundamental rights and data protection problematic in the employment of sophisticated surveillance technologies even within private spaces. It remains to be noted, that, as mentioned above, third party platform and technology providers will not fall within the household exemption when they process such personal data.

3.3.3 Conclusion

This section examined the applicability of fundamental rights, particularly data protection, to the operation of surveillance systems through private individuals. While generally fundamental rights only indirectly apply to the private sphere, data protection both as a right and as a regulatory instrument apply to all sorts of data processing activities, especially when commercial interests are involved, when the personal data is gathered from public places, and when personal data is disseminated. The EU data protection framework appears to be based on a rather strict interpretation of possible exclusions from its scope. With this, particularly the CJEU has argued in favour of a clear inclusion of data gathered from public areas and from third party individuals into the data protection framework.

A dignity based approach to privacy and data protection, although not directly visible in the CJEU jurisprudence, can clearly be seen in the discussion on dash-cams. The argument that widespread collection of sensor data in public spaces and the consequential availability of that data for law enforcement and other purposes could create a high ‘surveillance pressure’ in public places, is an attractive argument from a fundamental rights perspective, particularly because it lends strong reasons for

preferring the communal privacy approaches over individual interests. This shows once again some ambiguities of privacy, in which an individual interest to privacy collides with a collective right not to be subject to control. This ambiguity becomes very visible when discussing individual and private actor surveillance. Dignity based communal approaches and individual-centred approaches appear to take fundamentally different stands. It is clear, that particularly within European Fundamental Rights, the protection mechanisms appear to favour a strict interpretation of the applicability of data protection to private actor surveillance. Not only public actor surveillance, but also private actor surveillance interferes with the European rights to privacy and data protection and therefore require adequate regulation, which can reach deep into the activities of individuals. The upcoming years will show if interpretations of the GDPR will follow those tendencies.

3.4 Automation and Prediction

The last issue which shall be discussed in this study is an outlook into the future. This section addresses certain legal issues arising from the scenario that relate to the automation of surveillance and the prediction of incidents. The scenario as such contains a variety of fundamental rights issues, foremost related to either direct targeted individual surveillance or untargeted mass surveillance. Furthermore, the analysis focusses on actors and space in the classical dichotomy between public and private, in its many meanings.

This last issue focusses on two specific surveillance capabilities of the technology employed in the Helberg scenario: the automation of recognition of incidents and the automatic prediction of events. Both capabilities are a result of highly sophisticated analytics technologies operating within the surveilled space. In this sense, automation of recognition means that certain incidents can be automatically detected and reported via data processing in the system.

Prediction means that security relevant incidents in public spaces can be detected before they happen. The basic idea is that massive data analytics could identify common characteristics of security relevant incidents, e.g., by using automated detection mechanisms and creating algorithms which are, with a high probability, able to predict what is likely to happen in the future.

Both of the capabilities are playing an important role in making modern surveillance tools more efficiently especially in the area of public surveillance, where the amount of gathered data often overstrains the capacities for manual and visual analyses. Additionally, security organizations with the mission to prevent terrorism naturally strive for employment and development in this direction. In light of this research, this section addresses technological automation of control in public areas and its legal consequences.

3.4.1 Automation

Automated detection of incidents in public areas lies at the core of what is often referred to as ‘smart surveillance’. Research on so called ‘smart surveillance’ has been conducted for over a decade, ever since the shift from analogue to digital technologies paired with the increase in computing powers made mass data analytics possible,

feasible and more or less efficient. The most common story-line in such research starts off with the remarkable technological changes that lead to technology starting to be able to recognize things and identify people, for example through facial recognition technology.[855] In fact, much of the academic research focuses on smart visual surveillance and CCTV, as one of the first sensors capable of certain analytical processing.[856] Möllers and Hälterlein also track a variety of terms describing the use of analytics in video surveillance, such as 'algorithmic surveillance', 'semantic video surveillance', 'second generation CCTV', and 'smart CCTV'.[857] CCTV, however, is not the only sensor in public security systems. The future of such systems lies in their multiple integration: In systems where data from visual, audio, temperature, chemical and radiation sensors can be combined and processed in one system, enabling a multitude of uses and information extraction. With the expansion of surveilled space comes the expansion of multiple sensors and the integration of many data sources into one centrally connected surveillance system.[858]

Furthermore, such surveillance systems could also integrate data collection from other digital sources, for example social networks, mobile phone networks or travel records of public transport systems. With this, data collected and retained from 'physical' public spaces could be combined with information gathered from the virtual net of information in a 'virtual' public space. The visual recognition of people on a square, for example, and the combination of such information with mobile phone location data, could give valuable information on the flow of commuters or the size and movement of political demonstrations. The integration of the various sources of sensor data is therefore essential in enabling automatic detection functions.

---

[855] See Introna LD and Wood D, 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems' (2004) 2 Surveillance & Society 177, 178. For an early analysis of the global growth of video surveillance see Norris C, McCahill M and Wood D, 'Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space' (2004) 2 Surveillance & Society 110 and Norris C, 'Accounting for the global growth of CCTV' in Lyon D, Haggerty KD and Ball K (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012).

[856] See Möllers N and Hälterlein J, 'Privacy issues in public discourse: the case of "smart" CCTV in Germany' (2012) 26 Innovation: The European Journal of Social Science Research 57, 59.

[857] Ibid, 59.

[858] See also Kremer J, 'On the end of freedom in public spaces: legal challenges of wide-area and multiple-sensor surveillance systems' in Davis FF, McGarrity N and Williams G (eds), *Surveillance, counter-terrorism and comparative constitutionalism* (Routledge 2014).

An early example demonstrating the technical aspiration in the development of such systems in Europe is INDECT, an EU funded former FP7 project which attempted to build a surveillance system enabling automatic threat detection by combining CCTV streams as well as computer network data analytics.[859] The vision of the project was to create a functioning and efficient surveillance system which would automatically detect many sorts of incidents and threats in public urban areas. The INDECT project raised much critical public attention and the actual technical project results are far from presenting a successfully and effectively functioning total surveillance system.[860] The main visions and ideas of such technologies are, however, of strong interest for this study

The growing importance of sensors and analytics for surveillance systems is also due to the ever-increasing masses of data gathering. Wide-area persistent surveillance systems can produce an amount of data that is impossible to analyse manually, for example when high resolution video data is gathered form tens of square kilometres of terrain from the sky, such as with the ARGUS IS system.[861] The main question arising from the collection of vast amounts of sensor data is what effect the automation of the detection of certain pre-defined incidents have on legal analyses of the surveillance scenario.

It is uncontested that surveillance sensor data mostly consists of personal data. Personal data as information about an identified or identifiable individual, clearly comes into existence once sensors gather visual data on individuals. Also, mass-surveillance data can fall into the category of personal data, provided that information can somehow be related to an individual for example to her behavioural patterns. There are also a variety of problems relating to the principles of data protection when it comes to mass-data collection, retention and analyses in the sense that a general

[859] See INDECT Intelligent information system supporting observation, searching and detection for security of citizens in urban environment, FP7-2007-SEC-218086, http://www.indect-project.eu/ accessed 9 Mai 2016.

[860] The project, albeit a FP7 funded research project, caused public stir in some and political debates due to heavy privacy concerns, leading to a change in communication strategy and led to a debate in the European Parliament on the project. See Parliamentary questions, 24 September 2010 E-7521/2010, OJ C 243 E, 20.08.2011; and Johnston I, EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour" (n 70).

[861] See description of Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), (n 77).

prohibition of data processing and a strict purpose limitation manifestly contradict unfettered mass surveillance. Yet, even if mass surveillance in the form of mass data gathering generally contradicts certain principles of data protection, there might be permissible limitations of the right to privacy within Europe's fundamental rights frameworks.[862] In many ways, automated data processing for automated surveillance systems are not distinguishable from data processing for non-automated surveillance systems. They both constitute an interference with the fundamental rights to private life in the ECHR and an interference with the right to data protection in the EUCFR, provided the surveillance falls within the scope of EU law. Consequently, such interferences require adequate justification in order to be permissible.

Yet, there is a certain element of uniqueness which comes with automation and fundamental rights assessments. What automation achieves, is that it has the potential to limit effects, and therewith interferences on individuals. From a fundamental rights perspective, it could be argued that automation, in fact, would reduce the graveness of interferences.

That is because individuals in public are more being left alone when surveillance is conducted by a machine which makes automated decisions of behaviours or incidents. Automated security systems could therefore be seen as less intrusive than non-automated systems.[863] In that sense, one could argue that automation of data processing can lead to privacy improvements. Body-scanners at airports, for example, were made more 'privacy-friendly' by separating analytics and searching procedures: if the person analysing the scanned images of passengers passing through airport security is placed separately from the officer communicating with the passenger, the passenger's 'naked' images would not be exposed to the person in direct contact, and privacy intrusions would be minimized. In a similar way, it could be argued that automatic recognition of incidents intrudes to a lesser degree into privacy, because no actual imagery might ever be accessible by security authorities, unless the system identifies a relevant incident.

[862] See the discussion on permissible limitations above.

[863] See for example Vermeulen M and Bellanova R, 'European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination?' (2012) Security and Human Rights 297, 310.

Automation, on the other hand, could also be seen as more problematic than non-automated surveillance. In a 2004 Opinion, the Article 29 Working Party stressed the need to pay greater attention to additional safeguard and privacy compliance assessment of video surveillance that employs automation features such as individual identification, location tracking and automated decision making.[864] Also the Venice Commission takes the stand that automation poses greater dangers for rights intrusions than manual surveillance. Firstly, because such sophistication makes technology more functional and efficient and secondly, because automation can significantly expand the scope of surveillance.[865]

Additional legal authority for an argument in favour of a critical perspective on automation comes from the EU data protection framework, in which 'automated individual decisions' explicitly require additional safeguards. Article 15 of the 95/46 Data Protection Directive and article 22 of the GDPR state a general rule that a data subject shall not be subjected to decisions which are solely based on automated processing and profiling.[866] Additionally, similar principles are repeated in the area of police and judicial cooperation, particularly in article 7 of the 2008/977/JHA Council Framework Decision[867] and article 11(1) of the new 'Police' Directive which states that

> Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms

[864] See Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11 February 2004, 11750/02/EN, WP 89, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf accessed 1 February 2017, 24.

[865] European Commission for Democracy through Law (Venice Commission) Opinion on Video Surveillance (n 101), paras 17, 18.

[866] Art 20(1) Regulation (EU) 2016/679, (GDPR), (n 303): '1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.', Art 15 Directive 95/46/EC (Data Protection Directive) (n 305) states: '1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.'

[867] EU Framework Decision 2008/977/JHA (n 589), 60–71.

> of the data subject, at least the right to obtain human intervention on the part of the controller.[868]

It is furthermore emphasized that automated decision making employing special categories of personal data requires strict necessity and appropriate safeguards.[869]

In effect, this shows that the argument which regards automated systems as less intrusive than non-automated systems is fundamentally flawed. Data protection instruments appear to be built on the premise that automatic processing of personal data is more problematic than manual processing. Increased efficiency, widened scope and proliferation of automated surveillance in fact lead to an ever-present system of surveillance which, even if no person accesses surveillance data until a 'real' security incident happens. This can only be seen as a lesser degree of intrusion, if the understanding of privacy is purely based on the notion of 'legitimate expectation'. If a person's individual expectation of enjoying privacy are generally very low in public spaces, then automation could in some sense increase the individual's perception of privacy intrusion. If the person's actions do not trigger the system to recognize and report an anomaly to the security controller, there will not be any digital trace or records of that person, and the person's rights would not be interfered with.

Once the understanding of privacy is based on dignity, personality and self-determination, however, a scenario in which an automated system monitors and controls large areas of public space will be seen as a privacy nightmare. That is because the focus of the argument lies on external control rather than on internal individual expectations and the controlling of space presses individuals into conforming to pre-defined norms of behaviour.

Another aspect of automation of systems is that by eliminating the human decision making factor, at least in theory, discriminatory treatment could be eliminated. After all, machines base their decisions on allegedly neutral data and not on other potentially discriminating factors. There are however, two problems with such an assertion.

---

[868] Art 9 Directive (EU) 2016/680 (n 303).

[869] Those special categories are '…data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, (…) genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation'. See Art 8 Directive (EU) 2016/680 (n 303).

Firstly, while automation generally takes over the pre-selection of security relevant incidents, the final decision of action is still determined by a human being, so that the automated decision making process is verified by personnel on the ground. This, some argue, leaves an uncertainty in the overall process which should be replaced with proper oversight over machine decision making processes, maybe even by being based on statistical data.[870]

Secondly, another important aspect which is often overlooked is that the programming of the algorithms determining what constitutes incidents, events and behaviours which trigger notifications or actions, could be problematic in themselves. The INDECT Project, for example attempted to define what constituted anomalies or noteworthy incidents, by asking end-users such as police officers about what could constitute an 'abnormal' behaviour.[871]

Ultimately, the decision on what is 'abnormal', and therewith security relevant behaviour, lies with the programmers of the algorithms. It goes without saying that this requires defining certain social norms in public places which is heavily problematic from a political and democratic perspective.

Once again, the positive aspects of automation in combatting discrimination only stand when employing viewpoints that base the argument on an individual's expectations rather than self-determination and communal interest. Automatic selection necessarily employs pre-defined criteria which are always somewhat exclusive. In this sense, automated selection is similar to profiling, unless the automatic selection is somehow completely randomized.[872]

---

[870] See Vermeulen M and Bellanova R, 'European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination?' (2012) Security and Human Rights 297, 311.

[871] See INDECT Consortium 2012, D1.1 Report on the collection and analysis of user requirements, European Seventh Framework Programme FP7-218086-Collaborative Project, 24 January 2012, http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_D1.1_v20091029a.pv.pdf/view accessed 5 December 2016.

[872] Bruce Schneier has argued that randomization in Airport security screening makes sense, because profiling produces discrimination, is biased and less efficient. See Schneier, B, 'The Trouble with Airport Profiling' in *Forbes*, 9 May 2012 and Schneier on Security, https://www.schneier.com/essays/archives/2012/05/the_trouble_with_air.html accessed 7 April 2016. See also the discussion by Harris S and Schneier B, 'To Profile or Not to Profile? A Debate between Sam Harris and Bruce Schneier' in *Schneier on Security*, https://www.schneier.com/essays/archives/2012/05/to_profile_or_not_to.html accessed 7 April 2016.

It has to be concluded that automation in security systems requires closer scrutiny in its fundamental rights assessments and data protection compliance analyses. Both, the ECHR as well as the EU Fundamental Rights system have yet to respond to fully automated surveillance systems. It is likely, however, that essential answers can be given within the developed perspectives on a right to private life and particularly the right to data protection. In order to grasp automated surveillance systems conducted by law enforcement authorities, the Courts might have to look at current interpretations in data protection law, and transfer some of the core principles, for example from the General Data Protection Regulation into the European Fundamental Rights framework.

3.4.2 Prediction

Prediction in surveillance systems is a fairly new phenomenon. Prediction technologies use large quantities of data in connection with statistical and probability information in order to foresee the occurrence of security relevant incidents. Prediction of incidents is the logical continuation of surveillance data analytics and automatic recognition. Once surveillance data is big enough, it might be possible to identify certain patterns which, with a high probability, might lead to the occurrence of an event.

An example of such technology is the Pre Crime Observation System (PRECOBS), developed by the German Institut für musterbasierte Prognosetechnik Verwaltungs-GmbH (IfmPt). PRECOBS essentially analyses data through the mapping of occurred crimes and the near-repeat methods from criminology research in order to predict possible future crimes.[873] Another example of the use of prediction and prevention technologies in surveillance is TrapWire, a system designed to forecast terror attacks.[874] By gathering incident reports from multiple sources, TrapWire operates on the assumption that sophisticated crimes and attacks require preparations including

[873] See Brühl J, Fuchs F, Gesucht: Einbrecher der Zukunft‘ in *Süddeutsche Zeitung, sueddeutsche.de*, 12 September 2014, http://www.sueddeutsche.de/digital/polizei-software-zur-vorhersage-von-verbrechen-gesucht-einbrecher-der-zukunft-1.2115086 accessed 7 April 2016.

[874] See Botsch D and Maness MT, ‘Trapwire. Preventing Terrorism’ (2006) 22 Crime & Justice International 39, 41.

the gathering of intelligence by criminals or terrorist. Analysing surveillance data of previous incidents and detecting such preparatory behaviours might then reveal patterns which could be found in other occasions prior to an actual incident. Once sophisticated enough, the hope is to be able to predict and prevent crimes targeting certain areas or buildings.[875]

Continuing this thought, vast surveillance systems gathering data through ubiquitous sensors might very well be able to detect patterns prior to certain incidents. Pattern recognition and predictive modelling might therefore develop technological capabilities that enable efficient detection of incidents before they happen, and therewith allow for the allocation of security resources in order to prevent them. Once data is collected and processed on a massive scale and over long period of times, it will be possible to detect anomalies within this data. What adds to the functionality of predictive analytics in surveillance systems are generally highly sophisticated algorithms with self-developing capabilities, developments in Artificial Intelligence (AI) and Machine Learning.[876] Ultimately, drawing the surveillance scenario further, automation and predictive analyses could employ data from surveillance systems and their sensors, form social media, from mobile phone data, from public and private data bases and many more in order to detect anomalies and predict incidents that are deemed noteworthy by the controllers of such systems. While this is truly an extreme scenario, today mostly pictured in TV series and movies such as Steven Spielberg's 2002 'Minority Report' and CBS' crime TV Series 'Person of Interest', the question remains on how such developments could be addressed from a legal perspective.

Much of the functions of such systems would naturally fall into the scope of privacy law and fundamental rights. It is precisely such scenarios against which data protection regulations and privacy as a fundamental right have been drafted. Such technologies are therefore likely to be found to be incompatible in its entirety. Yet, privacy and data protection are not absolute rights. There might be reasons yet to be determined that could lead to a discussion on the possible justifications of such fictional systems. At least it has been shown since the NSA documents were released by Edward Snowden

[875] Ibid.

[876] See van Otterlo M, 'Automated experimentation in Walden 3.0: The next step in profiling, predicting, control and surveillance' (2014) 12 Surveillance & Society 255.

that certain intelligence agencies are making enormous efforts to build sophisticated tools for communication surveillance. Predictive analytics are enormously attractive tools for security authorities that have the prevention of certain incidents as their core mission.

Jessica Earle and Ian Kerr classify predictions into three categories: consequential predictions, preferential predictions and pre-emptive predictions.[877] Consequential prediction describes essentially the use of anticipatory algorithms in order to enable choices which avoid unfavourable outcomes in the future – Kerr and Earle specifically point out the profitability of reliable consequential predictions for individual actor centred risk management.[878] Preferential predictions, on the other hand, describe analytics which give a reliable estimation of an individual's likely choices and preferences; the prediction here focuses on, e.g., potential consumer choices of individuals.

As a third type of prediction, Kerr and Earle describe pre-emptive predictions as '…intentionally used to diminish a person's range of future options' and therewith '…assess the likely consequences of allowing or disallowing a person to act in a certain way.'[879] Pre-emptive predictions are therewith made in order to influence the possibilities of choices and actions for others in the future, in order to avoid certain unwanted effects.

While this distinction appears very much choice and actor–centred, it is useful in order to assess the types of predictions that are relevant for public surveillance, keeping an eye on the urban surveillance scenario. Predictions in security surveillance fall into the first and last category of predictions: consequential predictions in surveillance could foresee certain events, allowing the authorities to adjust certain measures in order to prevent incidents, and pre-emptive prediction naturally occurs in surveillance when surveillance has a coercive or restricting effect on individuals in public.

From a fundamental rights perspective, both consequential prediction as well as pre-emptive prediction raises serious legal problems. When some individuals use

[877] Kerr I and Earle J, 'Prediction, preemption, presumption: How Big Data threatens big picture privacy.' (2013) 66 Stanford Law Review Online 65, 67, 68.

[878] Ibid, 67.

[879] Ibid.

consequential predictions in order to avoid future risks, those with no access to such information might be subject to avoidable risk. In such a scenario, access to information on risks deriving from predictive systems is crucial for risk managing capabilities. This poses serious ethical as well as legal problems such as e.g. discrimination and protection obligations.

Pre-emptive prediction is particularly problematic, when legal systems are based on repressive rather than preventive measures. The turn to prevention poses serious issues for understandings of justice particularly in democratic judicial systems.[880] This poses a general problem for the classic balancing between repression and prevention. While preventive measures appear to be a less fundamental rights intrusive than repressive measures, with sophisticated pre-emptive prediction, this balance might be on the verge of shifting. While pre-emptive prediction might be disguised as preventive and a less intrusive measure, it might in fact qualify as a collective repressive mechanism, with significant impact on fundamental rights and freedoms.

The detailed legal analyses of predictive analytics in urban surveillance system will have to be done by future research. What can certainly be predicted for now is that those analytical tools will pose a major challenge for law makers and privacy lawyers in the future.

[880] See e.g. Lyon D, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) Big Data & Society 1, 5.

4. Concluding Remarks

This study analysed fundamental rights problems deriving from modern surveillance technologies. It asked, how the existing European fundamental rights to privacy and data protection address the increasing and unprecedented surveillance capabilities in public spaces in Europe.

Privacy, as well as data protection, have become two essential fundamental rights in the construction of the European legal space. Three elements were of crucial importance for answering this question. Firstly, the question after the underlying conceptions of privacy (and data protection) as fundamental rights. Secondly, the assessment of surveillance technologies and their capabilities and therewith a short description of existing and future surveillance technologies. Thirdly, in order to assess the legal implications of surveillance technologies on the European public space, this study required fundamental rights analyses of specific issues deriving from public surveillance.

Part one of this study has shown that while the theoretical birthplace of privacy is essentially based in liberal individualism, modern and particular European understanding of privacy is also based on a right to personality, dignity, individual autonomy, and an overall perspective of community, particularly with regards to the strengthening of European data protection law. This also goes in line with the analyses of a right to security in Europe: while a right to security does not seem to have been very successful in European fundamental rights jurisprudence, data protection, the protection of democracy and rule of law appear as clear focal point particularly in EU fundamental rights. In that regard, it also seems that privacy jurisprudence appears to favour a turn of legal analytics of privacy from a liberty-based approach to a 'dignity' based approach – an approach in which privacy is understood as a derivate of dignity and community. While the concepts of dignity and privacy naturally have their ambiguities, from a fundamental rights perspective the latter offers attractive tools to address complex legal problems deriving from surveillance technologies.

This study was structured in two main parts. Part one discussed framework and conceptions, and part two analysed specific issues in the light of fundamental rights protection of the European public space. The first part analysed the theoretical background of the research question. It provided an insight into the legal theoretical

conceptualization of privacy, security and data protection. Within the analyses of a right to privacy, privacy was analysed as a legal concept, laying the foundation for the distinction between privacy as a concept of liberty and privacy as a concept of dignity. It furthermore addressed the concept of a European public space and the problem of privacy in public areas.

Privacy as expression of liberty and privacy as a derivate of dignity produce two different answers to the many questions deriving from surveillance technologies. Understood as from a perspective of individual liberty, privacy protection depends on individual choices and expectations. Here, the legitimate expectation doctrine occasionally employed by the ECtHR can serve as a prime example for such a concept. Consent-based data protection regulation functions in a similar way. From such as perspective, individuals have less fundamental rights protection when they enter the public sphere.

Privacy conceptualized as a personality right and as a derivate of dignity and autonomy, enables different answers to pressing questions of privacy in public. Here, the public space is essentially constructed as communal space, and a fundamental right to privacy has the task to protect such communitarian spaces. Privacy is then interfered with, once an entity, may it be public or even private manipulates or coerces individuals, groups, or behaviours in public spaces. The same applies to virtual public spaces as well as personal information: not losing control over one's information in such a way that it leads to fear, a certain surveillance pressure or a change in behaviour is a fundamental rights problem, and can be addressed as such.

Naturally, neither privacy rights based on dignity, nor privacy rights based on individual freedom are absolute rights and they can be subjected to permissible limitations. The acceptance of such limitation through the Courts, however, then depends on the employed privacy perspective.

Data protection, in this study appears as connecting individual freedom rights with dignity approaches. On the one hand, individuals enjoy the freedom to not be the subjects of unconsented data processing and therewith should be in control of their information. On the other hand, an uncontrolled permanent processing of personal data can very well violate human dignity, autonomy and personality rights. In this

light, it is somehow remarkable that particularly the CJEU has begun to emphasize the importance of data protection as a fundamental right.

Furthermore, this study gave a brief overview over specific surveillance technologies and their capabilities and gave a glimpse into potential near-future application of such surveillance technologies. Technologies have progressed to a point where it is and will be increasingly difficult for the Courts in Europe to assess all potential fundamental rights implications. It appears therefore more important than ever to clearly understand the function of a fundamental right to privacy in modern democratic societies, namely on the one hand to protect individual liberties, but on the other hand as a tool to address the potentially devastating effects of modern surveillance effects on democratic societies.

This study has shown that privacy as a fundamental right in Europe is more than just about liberal freedoms. It is in fact about the way that communities and whole societies will be organized in the future, in a world which will be interwoven and controlled with all sorts of technologies capable of controlling human and societal life.

***

The research question outlined in the introduction of this study asked about the scope and limitations to privacy in public places. The first result of this study is therefore that the definition of a scope of privacy in public depends on the conception of privacy. The ECHR, for example, especially in its early case law, has repeatedly applied a conception of privacy in public which, at least to a certain extent, considers individual legitimate expectations as determining the scope of privacy protection in public. Willingly participating in public events, for example, appeared to lower individual protection against being subject to surveillance. This, of course, makes some sense. To a certain extent, being in a public place means being subject to a different type of scrutiny, control and surveillance, then if one is inside an apartment. This understanding of privacy therefore rests on a conception of a right to be let alone when one choses seclusion and solitude, but one does not enjoy such a right to be let alone once sojourning in a place shared with other individuals.

The underlying assumption of this conception also comes with a specific perception of individual control. The position of legitimate expectation therefore not only

contains an element of individual choice, but also an element of individual control. Privacy, conceptualized from such a perspective therefore is based in individual freedom, in the sense that it is the freedom of the individual to choose certain behaviours and to control certain circumstances. Basing fundamental right interferences on legitimate expectation and individual freedom, of course, opens privacy to critique. Understood in such a way, privacy naturally becomes an exclusive concept for the people who possess the material means to choose and control.

The discussions in this study showed that there are other ways of approaching the problem of privacy in public. Again, ECtHR case law also indicates that interferences with privacy can be caused by public surveillance, once personal data about individuals has been processed. This argumentation then is based on the idea that privacy is also about controlling information about oneself, and therewith about a right to informational self-determination. In fact, the inclusion of data protection in the scope of privacy in the ECHR appears to argue along this line: once information about individuals is systematically processed, this has been regarded as a privacy issue. Including this argument in its case law enables the ECtHR to address surveillance in public spaces, and especially mass-surveillance, with an argument different from that of legitimate individual expectation. Control of personal data, but also the potential societal effect of a highly controlled environment can be used as counter arguments against large-scale surveillance and data processing. The focus on information processing enables the inclusion of the public space into the realm of privacy protection, and lead to a special role of data protection in Europe.

Data protection is an important regulatory instrument in Europe and it may even be regarded as a separate fundamental right next to privacy, as discussed in this study. The core of data protection could therewith contain both an element of freedom (choice and control) and an element of community, dignity and self-determination. Therewith, data protection can deliver arguments that a right to privacy based on individual liberty lacks: it addresses surveillance in public with reference to the need for individual control of information paired with a communal concern that systematic information processing can have an enormous coercing and repressing effect on societies. Data protection as a fundamental right therewith comes with a core of societal values of freedom and dignity. This is also what appears to make data

protection a strong argument in Europe, not only within the ECHR, but also with the EUCFR, the EU data protection reform and the corresponding case law.

The third line of argument which addresses privacy in public in this study, derives from the concept of dignity and right to personality. While those are concepts originally coming from classical individual liberalism, one of the core finding in this study is that they can be used as a legal argument addressing the surveillance in public places from yet another perspective: namely as a communal value. Interestingly, there are some legal arguments addressing surveillance in public places that focus on the negative societal and communal effects of control and coercion by referring to human dignity and a right to personality. In such a perspective, privacy becomes a societal value deriving from classical liberal dignity, and this enables the construction of a very strong fundamental rights argument against public surveillance. In such a perception, the negative societal and coercive effects of surveillance pose high risks and a strong interference with rights, particularly in public places. Security authorities' attempts to manipulate behaviour in public places is as such a problem with human dignity and therewith interferes with individual rights. It appears that by challenging public surveillance with references to dignity and personal autonomy, and therewith labelling control and coercion as a societal problem, privacy arguments gain a communitarian perspective. In that sense, liberal individual rights have found a way to address the complex societal problems of surveillance. This is especially visible when it comes to mass surveillance issues: the reference to surveillance as a 'menace to society' and the overcoming of particular procedural hurdles allowed, for example, the ECtHR to address such issues in its fundamental rights interpretations.

The last aspect of the conclusion in this study is related to the technological aspects of surveillance. The capabilities of surveillance and control of public spaces appear more and more limitless. This is not only due to the advancements of technologies but also to the increased political will to employ surveillance. Furthermore, with enhanced data processing in virtual (public) spaces, the opportunities for the intrusion of coercion and control in many spheres of modern life appear limitless. This is a problem for fundamental rights, because fundamental rights are also built as (utopian) mechanisms against control and coercion. The control of public, as well as private space, is therewith fundamentally at odds with liberal individual concepts, but also communal

conceptions of rights. The results of this study show that current fundamental right mechanisms in Europe have the tools to address mass surveillance as a substantive problem. Consequently, it is up to these mechanisms to define the limits of surveillance, the limits of control, and also the permissible limits to fundamental rights. It may be advisable, however, to keep in mind the societal and community perspective in the times of ever more present sophisticated mass surveillance systems. Otherwise, the European public space may lose its potential for fostering communication, democracy, and freedom.

Table of Cases

European Court of Human Rights (ECtHR)

10 Human Rights Organisations and Others v the United Kingdom, App no. 24960/15, Communicated Case (pending), 24.11.2015.

Amann v Switzerland, App no. 27798/95, Judgment (Grand Chamber), 16.02.2000.

Anderberg v Sweden, App no. 13906/88, Decision (Commission), 29.06. 1992.

Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria, App. No 62540/00, Judgment (Court), 28.06.2007.

B.B. v France, App no. 5335/06, Judgment (Court), 17.12.2009.

Baka v Hungary, App no**.** 20261/12, Judgment (Grand Chamber), 23.06.2016.

Bărbulescu v Romania, App no. 61496/08, Judgment (Court), 12.01.2016.

Big Brother Watch and Others v the United Kingdom, App no. 58170/13, Communicated Case (pending), 07.01.2014.

Botta v Italy, App no. 21439/93, Judgment (Court), 24.02.1998.

Brunet v France, App no. 21010/10, Judgment (Court), 18.09.2014.

Bureau of Investigative Journalism and Alice Ross v the United Kingdom, App no. 62322/14, Communicated Case (pending), 05.01.2015.

Burghartz v Switzerland, App no. 16213/90, Judgment (Court), 22.02.1994.

Bykov v Russia, App no. 4378/02, Judgment (Grand Chamber), 10.03.2009.

C.G. and Others v Bulgaria, App no. 1365/07, Judgment (Court), 24.04.2008.

C.R. v the United Kingdom, App no. 20190/92, Judgment (Court), 27.09.1995.

Centrum För Rättvisa v Sweden, App no. 35252/08, Communicated Case (pending), 14.10.2014.

Christie v the United Kingdom, App no. 21482/93, Decision (Commission), 27.06.1994.

Christine Goodwin v the United Kingdom, App no. 28957/95, Judgment (Grand Chamber), 11.07.2002.

Copland v the United Kingdom, App no. 62617/00, Judgment (Court), 03.04.2007.

Esbester v the United Kingdom, App no. 18601/91, Decision (Commission), 02/04/1993.

Fernández Martínez v Spain, App no. 56030/07, Judgment (Grand Chamber), 12.06.2014.

Friedl v Austria, App no. 15225/89, Judgment (Court), (Struck out of the List), 31.01.1995.

Friedl v Austria, App no. 15225/89, Report (Commission) 19.05.1994.

Friend and Others v the United Kingdom, App nos. 16072/06, 27809/08 Decision (Court) 24.11.2009.

Gardel v France, App no. 16428/05, Judgment (Court) 17.12.2009.

Grafström v Sweden, App no. 16792/90, Commission Decisions 29.06.1992.

Halford v the United Kingdom, App no. 20605/92, Judgment (Court), 25.06.1997.

Handyside v The United Kingdom, App no. 5493/72, Judgment (Court), 07.12.1976.

Herbecq and the Association Ligue des droits de l 'homme v Belgium, App no. 32200/96, Inadmissibility Decision (Commission), 14.01.1998.

Hilton v The United Kingdom, App no. 12015/86 (Commission Decision), 06.07.1988.

Hutcheon v the United Kingdom, App no. 28122/95, Decision (Commission), 27.11.1996.

Iordachi and Others v Moldova, App no. 25198/02, Judgement (Court), 14.09.2009.

J.P.D. v France, App no. 55432/10. Decision (Court), 16.09.2014.

Kennedy v the United Kingdom, App no. 26839/05, Judgment (Court), 18.05.2010.

Khan v the United Kingdom, App no. 35394/97, Judgment (Court), 12.05.2000.

Kinnunen v Finland, App no. 24950/94, Decision (Commission) 15.05.1996

Klass and Others v Germany, App no. 5029/71, Judgment (Court), 06.09.1978.

Kopp v Switzerland, App no. 23224/94, Judgment (Court), 25.03.1998.

Kurt v Turkey, App no. 24276/94, Judgment, Court, 25.05.1998.

Leander v Sweden, App no. 9248/81, Judgment (Court) 26.03.1987.

Liberty and Others v the United Kingdom, App no. 58243/00, Judgment (Court), 01.07.2008.

Lüdi v Switzerland, App no. 12433/86, Judgment (Court), 15.06.1992.

Lundvall v Sweden, App no. 10473/83, Decision (Commission), 11.12.1985.

Lupker and Others v the Netherlands, App no. 18395/91, Decision (Commission), 07.12.1992.

M.B. v France, App no. 22115/06, Judgment (Court), 17.12.2009.

M.K. v France, App no. 19522/09, Judgment (Court), 18.04.2013.

Malone v The United Kingdom, App no. 8691/79, Judgment (Court) 02.08.1984.

Niemietz v Germany, App no. 13710/88, Judgment (Court), 16.12.1992.

P.G. and J.H. v the United Kingdom, App no. 44787/98, Judgment (Court), 25.09.2001.

Peck v The United Kingdom, App no. 44647/98, Judgment, Court (Fourth Section), 28.01.2003.

Perry v the United Kingdom, App no. 63737/00, Judgment (Court), 17.07.2003.

Peruzzo and Martens v Germany, App nos. 7841/08, 57900/12, Decision (Court), 04.06.2013.

Petrina v Romania, App no. 78060/01, Judgment (Court), 14.10.2008.

Pretty v The United Kingdom, App no. 2346/02, Judgment, Court (Fourth Section), 29.04.2002.

Redgrave v the United Kingdom, App no. 20271/92, Decision (Commission), 01.09.1993.

Refah Partisi (the Welfare Party) and Others v Turkey, App nos. 41340/98, 41342/98, 41343/98 and 41344/98, Judgment (Grand Chamber), 13.02.2003.

Roman Zakharov v Russia, App no. 47143/06, Judgment (Grand Chamber), 04.12.2015.

Rotaru v Romania, App no. 28341/95, Judgment (Grand Chamber), 04.05.2000.

S and Marper v the United Kingdom, App nos. 30562/04, 30566/04, Judgment (Grand Chamber) 04.12.2008.

S.A.S. v France, App no. 43835/11, Judgment, Court (Grand Chamber) 01.07.2014.

Shimovolos v Russia, App no. 30194/09, Judgment (Court), 21.06.2011.

Silver and Others v The United Kingdom, App nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Judgment (Court), 25.03.1983.

Sunday Times v The United Kingdom (no. 1), App no. 6538/74, Judgment (Court), 26.04.1979.

Szabó and Vissy v Hungary, App no. 37138/14, Judgment (Court), 12.01.2016.

Taraneks v Latvia, App no. 3082/06, Judgment (Court), 02.12.2014.

Uzun v Germany, App no. 35623/05, Judgment (Court), 02.09.2010.

Von Hannover v Germany, App no. 59320/00, Judgment (Court), 24.06.2004.

Von Hannover v Germany (no. 2), App nos. 40660/08, 60641/08, Judgment (Grand Chamber), 07.02.2012.

Von Hannover v Germany (no. 3), App no. 8772/10, Judgment (Court), 19.09.2013.

Weber and Saravia v Germany, App no. 54934/00, Decision (Court), 29.06.2006.

X v Austria, App no. 8170/78, Commission Decision, 04.05.1979.

X v Federal Republic of Germany, App no. 8334/78, Commission Decision, 07.05.1981.

X v The United Kingdom, App no. 9702/82, Commission Decision 6.10.1982.

X v the United Kingdom, App no. 5877/72, Decision (Commission) 12.10.1973.

Court of Justice of the European Union (CJEU)

Case C-101/01 *Lindquist*, Judgment (Court), 6 November 2003, ECLI:EU:C:2003:596.

Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 9 July 2012, ECLI:EU:C:2014:317.

Case C-145/09, *Tsakouridis*, Judgment of the Court (Grand Chamber) of 23 November 2010, ECLI:EU:C:2010:708.

Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, Judgement, Court (Fourth Chamber), 11 December 2014, ECLI:EU:C:2014:2428.

Case C-292/97, *Kjell Karlsson and Others***,** Judgment (Sixth Chamber), 13 April 2000, ECLI:EU:C:2000:202.

Cases C-293/12 and C‑594/12, *Digital Rights Ireland*, Judgment of the Court (Grand Chamber), 8 April 2014, ECLI:EU:C:2014:238.

Case C-4/73, *Nold v Commission*, Judgment of the Court, 14 May 1974, ECLI:EU:C:1974:51

Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others*, Judgment, 20 May 2003, ECLI:EU:C:2003:294.

Case C-5/88 Wachauf, Judgment (Third Chamber), 13 July 1989*,* ECLI:EU:C:1989:321

Case C-554/13, *Zh. and Others*, Judgment of the Court (Third Chamber) of 11 June 2015, ECLI:EU:C:2015:377.

Case C-601/15, *J. N. v Staatssecretaris voor Veiligheid en Justitie*, Judgment of the Court (Grand Chamber) of 15 February 2016, ECLI:EU:C:2016:84.

Case C-617/10 *Åklagaren v Hans Åkerberg Fransson*, (Grand Chamber), 26 February 2013, ECLI:EU:C:2013:105.

Case C-73/07 *Satakunnan Markkinapörssi and Satamedia*, Judgment (Grand Chamber), 16 December 2008, ECLI:EU:C:2008:727.

International Court of Justice

Advisory Opinion Concerning Reservations to the Convention on the Prevention and Punishment of the Crime of Genocide, International Court of Justice (ICJ), 28 May 1951, ICJ Reports 1951, p. 15.

National Case Law

Germany

FCC, BVerfG, Urteil (Judgment), 16 July 1969, BVerfGE 27,1, Az. 1 BvL 19/63, (Mikrozensus).

FCC, BVerfG, Urteil (Judgment), 15 December 1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil).

FCC, BVerfG, Beschluss der 1. Kammer des Ersten Senats (Decision, 1st Chamber, 1st Senate), 23. February 2007, 1 BvR 2368/06.

FCC, BVerfG, Urteil des Ersten Senats (Judgment, 1st Senate), 11 March 2008, 1 BvR 2074/05.

Verwaltungsgericht (VG) Ansbach, Judgment, 12. August 2014, Az. AN 4 K 13.01634.

United States

Katz v. United States, 389 U.S. 347 (1967), (Judge Harlan, concurring).

Table of Legislation

Council of Europe

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Council of Europe, 8 November 2001, ETS No.181.

Committee of Ministers, Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies).

Committee of Ministers, Resolution (74) 29 on the protection of individuals vis-à-vis electronic data banks in the public sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (CoE Data Protection Convention), Council of Europe, 28 January 1981, entry into force 1 October 1985, ETS No.108

Council of Europe Recommendation R(87)15 & ETS Convention 108, Data Protection Vision 2020: Options for improving European policy and legislation during 2010-2020; Appendix 3, http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf accessed 21.November 2015.

Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS. No. 108, Strasbourg, 28.1.1981.

Council of Europe, Recommendation No. Rec (2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin, of 15 March 2006.

Council of Europe, Recommendation, CM/ Rec (2016) 6 of the Committee of Ministers to Member States on research on biological materials of human origin, 11 May 2016.

European Commission for Democracy through Law (Venice Commission), Opinion on the Protection of Human Rights in Emergency Situations adopted by the Venice Commission at its 66th Plenary Session, 17-18 March 2006, No. 10, CDL-AD (2006)015.

European Commission for Democracy through Law (Venice Commission), Opinion on Video Surveillance In Public Places by Public Authorities and the Protection of Human Rights, 23 March 2007, No. 404/2006, CDL-AD(2007)014.

European Commission for Democracy through Law (Venice Commission), Opinion on the Draft Constitutional Law on 'Protection of the Nation' of France, Adopted at its 106th Plenary Session, 11-12 March 2016, No. 838, CDL-AD(2016)006.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, (ECHR) Council of Europe, 4 November 1950, ETS No. 5.

European Union

Article 29 Data Protection Working Party (Art 29 WP), Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11 February 2004, 11750/02/EN WP 89, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf accessed 1 February 2017.

Article 29 Data Protection Working Party (Art 29 WP), Opinion 4/2007 on the concept of personal data, 20 June 2007, 01248/07/EN WP 136, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf accessed 10 October 2016.

Article 29 Data Protection Working Party (Art 29 WP), Opinion 5/2009 on online social networking, adopted 12.06.2009, 01189/09/EN WP 163, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf accessed 1 February 2017.

Article 29 Data Protection Working Party (Art 29 WP), Working Document on surveillance of electronic communications for intelligence and national security purposes, 5 December 2014, 14/EN WP 228, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf accessed 10 January 2016.

Article 29 Data Protection Working Party (Art 29 WP), Working document on data protection issues related to RFID technology, 19 January 2005, 10107/05/EN WP 105, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf accessed 13 October 2016.

Charter of Fundamental Rights of the European Union (EUCFR), 18.12.2000, OJ 2000/C 364/1.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441, OJ L 215, 25.8.2000, p. 7–47.

Consolidated version of the Treaty on European Union (TEU)**,** OJ C 326, 26.10.2012, p. 13–390.

Consolidated version of the Treaty on the Functioning of the European Union (TFEU), OJ C 326, 26.10.2012, 47–390.

Council of the European Union, Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, 63–84.

Council of the European Union, Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, 1–11 (Prüm).

Council of the European Union, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, 60–71.

Council of the European Union, Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ L 121/37, 15.5.2009, 37–66.

Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281, 31.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31/07/2002, 37-47.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), Invalidated 8.4.2014, OJ L 105, 13.4.2006, 54-63.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services,

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance) OJ L 337, 18.12.2009, 11-36.

Directive 2013/33/EU of the European Parliament and of the Council of 26 June 2013 laying down standards for the reception of applicants for international protection (recast), OJ L 180/96, 29.6.2013.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, 89–131.

Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, 17-35.

Parliamentary questions, 24 September 2010 E-7521/2010, OJ C 243 E, 20.08.2011.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10. January 2017, COM(2017) 10 final, 2017/0003 (COD).

Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, 1-22.

Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4.5.2016, OJ L 119/1.

United Nations

International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

UN General Assembly, Convention on the Rights of the Child, 20 November 1989, UNTS vol. 1577, 3.

UN General Assembly, Guidelines for the regulation of computerized personal data files, Adopted by General Assembly Resolution 45/95 of 14 December 1990, A/RES/45/95.

UN General Assembly, International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, 18 December 1990, A/RES/45/158.

UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

UN Human Rights Committee (HRC), CCPR General Comment No. 27: Article 12 (Freedom of *Movement)*, 2 November 1999, CCPR/C/21/Rev.1/Add.9.

UN Human Rights Committee (HRC), Concluding observations on the fourth periodic report of the United States of America, 23 April 2014, CCPR/C/USA/CO/4.

UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, Martin Scheinin, 28 December 2009, A/HRC/13/37.

UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, 17 April 2013, A/HRC/23/40.

UN Human Rights Council, The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights, 30 July 2014, A/HRC/27/37.

UN Economic and Social Council, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, E/CN.4/1985/4, Annex (1985).

Universal Declaration of Human Rights (UDHR), 10 December 1948, UNGA Res 217 A(III).

Vienna Convention on the Law of Treaties (VCLT*)*, 23 May 1969, UNTS vol. 1155, p. 331.

OECD

OECD, *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation accessed 20 February 2017.

National Legislation

France

Loi no. 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 6 January 1978.

Loi no. 2010-1192 du 11 Octobre 2010 interdisant la dissimulation du visage dans l'espace public. JORF no. 0237, 12 October 2010.

Germany

Bayerisches Straßen- und Wegegesetz (BayStrWG), BayRS V, S. 731, 5 October 1981.

Allgemeine Verwaltungsvorschrift (General Administrative Order) zur Straßenverkehrs-Ordnung (VwV-StVO), vom 22. Oktober 1998, in the version of 11 November 2014.

Hessisches Datenschutzgesetz (State of Hesse, Data Protection Law), GVBl. II 300-10, 625.

Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, BGBl. S. 1, zuletzt geändert durch Artikel 1 des Gesetzes vom 23.12.2014 (BGBl. I S. 2438).

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, (Artikel 10-Gesetz), 26 June 2001, BGBl. I S. 1254, 2298; 2007 I S. 154.

Bundesdatenschutzgesetzes (BDSG), 14. January 2003, BGBl. I S. 66, das zuletzt geändert durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162).

Straßenverkehrs-Ordnung (StVO), Verordnung vom 06.03.2013 (BGBl. I S. 367), in force since 01.04.2013, (BGBl. I S. 1635, m.W.v. 30.10.2014).

South Africa

Bill of Rights (Chapter 2 of the Constitution of the Republic of South Africa), Act No. 108, 1996.

Sweden

Datalag (1973:289), Svensk författningssamling 1973:289, t.o.m. SFS 1998:377.

United Kingdom

UK Public Order Act 1936 (1 Edw 8 and 1 Geo 6, Chapter 6).

Bibliography

Abrahamsen R, Hubert D and Williams MC, 'Guest Editors' Introduction' (2009) 40 Security Dialogue 363.

Agre P and Rotenberg M (eds), *Data Protection in Europe* (MIT Press 1997).

Alén-Savikko A and Pitkänen O, 'Rights and Entitlements in Information: Proprietary Perspectives and Beyond' in Bräutigam T and Miettinen S (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia 2016), 3-33.

Alexy R, *Theorie der Grundrechte* (Nomos Verlagsgesellschaft 1985).

Allen AL, *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield 1988).

Allen AL, 'Coercing Privacy' (1999) 40 William & Mary Law Review 723.

Allen AL, *Unpopular Privacy: What must we hide* (OUP 2011).

Bainbridge D, *Introduction to Information Technology Law* (6th edn, Longman 2008).

Balzer T and Nugel M, 'Minikameras im Straßenverkehr - Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen' (2014) Neue Juristische Wochenschrift 1622.

Barnard C and Peers S (eds), *European Union Law* (Oxford University Press 2014).

Bennett CJ and Raab CD, *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate, 2003).

Bennett CJ, *The Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press 2008).

Bjorge E, 'Been There, Done That: The Margin of Appreciation and International Law' (2015) 4 Cambridge Journal of International and Comparative Law 181.

Bloustein EJ, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962.

Blume P (ed), *Nordic Data Protection Law* (Kauppakaari, DJØF 2001).

Booth K, 'Security and Emancipation' (1991) 17 Review of International Studies 313.

Booth K, *Theory of World Security* (Cambridge University Press 2007).

Bossuyt, MJ, *Guide to the 'Travaux Préparatoires' of the International Covenant on Civil and Political Rights* (Marinus Nijhoff Publishers 1987).

Botsch D and Maness MT, ‘Trapwire. Preventing Terrorism’ (2006) 22 Crime & Justice International 39.

Boyd D and Crawford K, ‘Critical Questions for Big Data’ (2012) 15 Information, Communication & Society 662.

Bräutigam T and Miettinen S (eds), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia 2016).

Brennan-Galvin E, ‘Crime and violence in an urbanizing world’ (2002) 56 Journal of International Affairs 123.

Burgess JP, *The Ethical Subject of Security: Geopolitical Reason and the Threat against Europe* (Routledge 2011).

Buzan B, Weaver O and de Wilde J, *Security: A New Framework for Analysis* (Rienner 1998).

Buzan B and Hansen L, *The Evolution of International Security Studies* (Cambridge University Press 2009).

Bygrave LA, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002).

Bygrave LA, *Data privacy law: An International Perspective* (Oxford University Press 2014).

Byrne R, Benito-Lopez F and Diamond D, ‘Materials science and the sensor revolution’ (2010) 13 Materials Today 16.

Cameron I, *An introduction to the European Convention on Human Rights* (5th edn, Iustus 2006).

Cameron I, *National Security and the European Convention on Human Rights* (Iustus 2000).

Campisi P (ed), *Security and Privacy in Biometrics* (Springer 2013).

Cannataci JA, *Privacy and Data Protection Law: International Development and Maltese Perspectives* (Norwegian University Press 1986).

CASE Collective, ‘Critical Approaches to Security in Europe: A Networked Manifesto’ (2006) 37 Security Dialogue 443.

Chandler D, ‘Review Essay: Human Security: The Dog That Didn't Bark’ (2008) 39 Security Dialogue 427.

Clapham A, *Human Rights in the Private Sphere* (Clarendon Press 1993).

Clapham A, *Human Rights Obligations of Non-State Actors* (Oxford University Press 2006).

Clarke R, 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498.

Cohen JE, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review 1373.

Cooley, Thomas M, *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract* (Chicago 1880).

Currie DP, 'Positive and Negative Constitutional Rights' (1986) 53 University of Chicago Law Review 864.

Dandeker C, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day* (Polity 1990).

De Hert P and Others, 'Legal Safeguards for Privacy and Data Protection in Ambient Intelligence' (2008) 13 Personal and Ubiquitous Computing 435

De Hert P and Papakonstantinou V, 'The New Police and Criminal Justice Data Protection Directive. A First Analysis' (2016) New Journal of European Criminal Law 7,

De Hert P, 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in Campisi P (ed) *Security and Privacy in Biometrics* (Springer 2013), 369-413.

Douzinas C, *The End of Human Rights: Critical Legal Thought at the Turn of the Century* (Hart 2000).

Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge, 2012).

Edwards L, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) European Data Protection Law Review 28.

Eijkman Q and Weggemans D, 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?' (2012) Security and Human Rights 285.

Engle E, 'Third Party Effect of Fundamental Rights (Drittwirkung)' (2009) 5 Hanse Law Review 165.

Etzioni A, 'Communitarian Perspective on Privacy, A Commentary' (1999) 32 Connecticut Law Review 897.

Etzioni A, *The Limits of Privacy* (Basic Books 1999).

European Union Agency for Fundamental Rights (FRA), Council of Europe (CoE), *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2014).

Ferenbok J and Clement A 'Hidden Changes: From CCTV to 'smart' Video Surveillance' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge 2012).

Fichera M and Kremer J (eds), *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia 2013).

Finn L, Wright D and Friedewald M, 'Seven Types of Privacy' in Gutwirth S and others (eds), *European Data Protection: Coming of Age* (Springer 2013).

Fischer-Lescano A and Teubner G, *Regime- Kollisionen. Zur Fragmentierung des globalen Rechts* (Suhrkamp 2006)

Floridi L, 'Four challenges for a theory of informational privacy' (2006) 8 Ethics and Information Technology 109.

Flynn PJ, Jain AK and Ross AA (eds), *Handbook of Biometrics* (Springer 2008).

Frantziou E, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761.

Fried C, 'Privacy' (1968) 77 Yale Law Journal 475.

Fuchs C, 'Social media, riots, and revolutions' (2012) 36 Capital & Class 383.

Galtung J, 'Violence, Peace, and Peace Research' (1969) 6 Journal of Peace Research 167.

Gavison R, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421.

Georgieva I, 'The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR.' (2015) Utrecht Journal of International and European Law 104.

Gomez-Arostegui HT, 'Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations' (2004-2005) 35 California Western International Law Journal 153.

González-Fuster G and Gutwirth S, 'Opening up personal data protection: A conceptual controversy' (2013) 29 Computer Law & Security Review 531.

González-Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2015).

Goold BJ and Lazarus L (eds), *Security and Human Rights* (Hart 2007).

Gragl P, *The Accession of the European Union to the European Convention on Human Rights* (Hart Publishing 2013).

Greenwald G, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books/Henry Holt 2014).

Gross H, 'The Concept of Privacy' (1967) 42 New York University Law Review 34.

Gutwirth S, *Privacy and the Information Age (*Rowman & Littlefield Publishers 2002).

Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009).

Gutwirth S and others (eds), *European Data Protection: Coming of Age* (Springer 2013).

Hartman JF, 'Derogation from Human Rights Treaties in Public Emergencies-A Critique of Implementation by the European Commission and Court of Human Rights and the Human Rights Committee of the United Nations' (1981) 22 Harvard International Law Journal 1.

Harwood E, *Digital CCTV: A Security Professional's Guide* (Elsevier/Butterworth-Heinemann, 2008).

Hoofnagle CJ and Urban JM, 'Alan Westin's Privacy Homo Economicus' (2014) 49 Wake Forest Law Review 261.

Hoofnagle CJ, 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement.' (2004) 29 North Carolina Journal of International Law and Commercial Regulation 595.

Hornung G and Schnabel C, 'Data protection in Germany I: The population census decision and the right to informational self-determination' (2009) 28 Computer Law & Security Review 84.

Horwitz MJ, 'The History of the Public/Private Distinction' (1982) 130 University of Pennsylvania Law Review 1423.

Hutchinson T, 'Doctrinal Research – Researching the Jury' in D Watkins M Burton (eds) *Research Methods in Law* (Oxon: Routledge 2013).

Introna LD and Wood D, 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems' (2004) 2 Surveillance & Society.

Jain AK and Kumar A 'Biometric Recognition: An Overview.' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012).

Jain AK and Ross A, 'Introduction to Biometrics.' in: Flynn PJ, Jain AK and Ross AA (eds), *Handbook of Biometrics* (Springer 2008).

Joh E, 'Beyond Surveillance: Data Control and Body Cameras' (2016) 14 Surveillance and Society 133.

Jones, T and Newburn, T, *Private Security and Public Policing. Clarendon Studies in Criminology* (Clarendon Press Oxford 1998).

Joseph S and Castan M, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary*, (3rd edn, Oxford University Press, 2013).

Kennedy D, 'The Stages of Decline of the Public/Private Distinction' (1982) 130 University of Pennsylvania Law Review 1349.

Kerr I and Earle J, 'Prediction, preemption, presumption: How Big Data threatens big picture privacy.' (2013) 66 Stanford Law Review Online 65.

Koops B-J and others, 'A Typology of Privacy', (2016) University of Pennsylvania Journal of International Law, Forthcoming; Tilburg Law School Research Paper No. 09/2016, https://ssrn.com/abstract=2754043 (accessed 10.01.2017).

Koskela H, '"The gaze without eyes" Video surveillance and the changing nature of urban space' in Holmes D (ed), *Virtual Globalization: Virtual Spaces/Tourist Spaces* (Routledge 2001).

Koskenniemi M, *From Apology to Utopia: The Structure of International Legal Argument* (Reissue with a new epilogue, Cambridge University Press 2005).

Kremer J, 'Exception, Protection and Securitization: Security Mindsets in Law.' in Fichera M and Kremer J (eds), *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia 2013).

Kremer J, 'On the end of freedom in public spaces: legal challenges of wide-area and multiple-sensor surveillance systems' in Davis FF, McGarrity N and Williams G (eds), *Surveillance, counter-terrorism and comparative constitutionalism* (Routledge 2014).

Kremer J, 'Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace' (2014) 23 Information & Communications Technology Law 220.

Kroener I, *CCTV: A technology under the radar?* (Burlington: Ashgate 2014).

Kruegle H, *CCTV Surveillance: Analog and Digital Video Practices and Technology* (Elsevier Butterworth Heinemann 2007)

Lazarus, L 'Mapping the Right to Security' in Goold BJ and Lazarus L (eds), *Security and Human Rights* (Hart 2007).

Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8 European Constitutional Law Review 375.

Lessig L, *Code: and other laws of cyberspace* (Basic Books 1999).

Leuschner S, 'EuGH und Vorratsdatenspeicherung: Erfindet Europa ein neues Unionsgrundrecht auf Sicherheit?' in Schneider F and Wahl T (eds.),

Herausforderungen für das Recht der zivilen Sicherheit in Europa (Nomos 2016), 17-46.

Lipschutz RD (ed), *On Security* (Columbia University Press 1995).

Lloyd IJ, *Information Technology Law* (6th edn, Oxford University Press 2011).

Luhmann N, *Das Recht der Gesellschaft* (Frankfurt a.M.: Suhrkamp 1995).

Lyon D, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001).

Lyon D (ed), *Surveillance as social sorting: privacy, risk, and digital discrimination* (Routledge 2003).

Lyon D (ed), *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing 2006).

Lyon D, 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique' (2014) 1 Big Data & Society 1.

Lyon D, *Surveillance Studies: An Overview* (Polity 2007).

Lyon D, Haggerty KD and Ball K (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012).

Macovei M, *The right to liberty and security of the person. A guide to the implementation of Article 5 of the European Convention on Human Rights* (Human rights handbooks, No. 5, Council of Europe 2002).

Maduro M, Sankari S and Tuori K (eds), *Transnational Law: Rethinking European Law and Legal Thinking* (Cambridge University Press 2014).

Margulis ST, 'On the Status and Contribution of Westin's and Altman's Theories of Privacy' (2003) 59 Journal of Social Issues 411.

Marquis G, 'Private security and surveillance. From the "dossier society" to databanks networks.' In Lyon D (ed), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination* (Routledge 2003), 226-248.

Marx G, 'Murky conceptual waters: The public and the private' (2001) 3 Ethics and Information Technology 157.

Mayer-Schönberger V, 'Generational Development of Data Protection in Europe' in Agre P and Rotenberg M (eds), *Data Protection in Europe* (MIT Press 1997).

Mayer-Schönberger V, 'Beyond Privacy – Towards a "System" Theory of Information Governance.' (2010) California Law Review 1953.

Mayer-Schönberger V and Cukier K, *Big Data: A revolution that will transform how we live, work, and think* (Houghton Mifflin Harcourt 2013).

McGoldrick D, 'A defence of the margin of appreciation and an argument for its application by the Human Rights Committee' (2016) 65 International & Comparative Law Quarterly 21

Micklitz H, 'Rethinking the Public/Private Divide' in Maduro M, Sankari S and Tuori K (eds), *Transnational Law: Rethinking European Law and Legal Thinking* (CUP 2014).

Micklitz H and Svetiev Y (eds), *A Self-sufficient European Private Law: A Viable Concept* (Fiesole: European University Institute Working Papers, 2012).

Mills JL, *Privacy: The Lost Right* (Oxford University Press 2008).

Mnookin RH, 'Public/Private Dichotomy: Political Disagreement and Academic Repudiation' (1982) 130 University of Pennsylvania Law Review 1429.

Modi SK, *Biometrics in Identity Management: Concepts to Applications* (Artech House 2011).

Möllers N and Hälterlein J, 'Privacy issues in public discourse: the case of "smart" CCTV in Germany' (2012) 26 Innovation: The European Journal of Social Science Research 57.

Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012).

Mordini E, Tzovaras D and Ashton H 'Introduction' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012).

Moreham NA, 'Privacy in Public Places' (2006) 65 Cambridge Law Journal 606.

Moser R, 'As If All The World Were Watching: Why Today's Law Enforcement Needs To Be Wearing Body Cameras' (2015) 7 Northern Illinois University Law Review 1.

Murray A, *Information Technology Law: The Law and Society* (2nd edn, Oxford University Press 2013).

Nilsson F and Axis Communications, *Intelligent Network Video: Understanding Modern Video Surveillance Systems* (CRC Press 2008).

Nissenbaum HF, 'Toward an Approach to Privacy in Public: Challenges of Information Technology' (1997) 7 Ethics & Behavior 207.

Nissenbaum HF, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.

Nissenbaum HF, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books 2010).

Norris C, 'Accounting for the global growth of CCTV' in Lyon D, Haggerty KD and Ball K (eds), *Routledge Handbook of Surveillance Studies* (Routledge 2012).

Norris C and Armstrong G, *The Maximum Surveillance Society: The Rise of CCTV* (Berg, 1999).

Norris C, McCahill M and Wood D, 'Editorial. The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space' (2004) 2 Surveillance & Society 110.

Nouwt S, Berend R. de Vries and Roel Loermans, 'Analyses of the Country Reports' in Nouwt S, de Vries BR, Prins C (eds*), Reasonable Expectations of Privacy?: Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser 2005) 323-358.

Nouwt S, de Vries BR, Prins C (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (TMC Asser 2005).

Ojanen T, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others' (2014) 10 European Constitutional Law Review 528.

Ojanen T, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter' (2016) 12 European Constitutional Law Review 318.

Omand D, Bartlett J and Miller C, 'Introducing Social Media Intelligence (SOCMINT)' (2012) 27 Intelligence and National Security 801.

Otterlo M, 'Automated experimentation in Walden 3.0: The next step in profiling, predicting, control and surveillance' (2014) 12 Surveillance & Society 255.

Peers S, 'Taking Rights Away? Derogations and Limitations.' in Peers S and Ward A (eds), *The European Union Charter of Fundamental Rights* (Hart 2004).

Peers S and Ward A (eds), *The European Union Charter of Fundamental Rights* (Hart 2004).

Peers S and others (eds), *The EU Charter of fundamental rights: A Commentary* (Hart 2014).

Peers S and Prechal S, 'Article 52 – Scope and Interpretation of Rights and Principles' in Peers S and others (eds), *The EU Charter of fundamental rights: A Commentary* (Hart 2014) 1455-1522.

Petman J, 'Egoism or altruism? The politics of the great balancing act' (2008) 5 No Foundations Journal of Extreme Legal Positivism 113.

Posner RA, ‘The Right of Privacy’ (1987) 12 Georgia Law Review 393.

Posner RA, *The Economics of Justice* (Harvard University Press 1981).

Post RC, ‘Three Concepts of Privacy’ (2000-2001) 89 Geo. L.J. 2087.

Powell RL, ‘The Right to Security of Person in European Court of Human Rights Jurisprudence.’ (2007) 6 European Human Rights Law Review 649.

Prosser WL, ‘Privacy.’ (1960) 48 California Law Review 383.

Reed C, *Computer Law* (Oxford University Press 2012).

Reidenberg JR, ‘Privacy in Public’ (2014) 69 U Miami L Rev 141.

Richards NM and Solove DJ, ‘Prosser's Privacy Law: A Mixed Legacy’ (2010) 98 California Law Review, 1888.

Richardson J, *Law and the philosophy of privacy* (Routledge 2016).

Roach K, ‘Sources and Trends in Post-9/11 Anti-Terrorism Laws’ in Goold BJ and Lazarus L (eds), *Security and Human Rights* (Hart 2007).

Rosas A and Armati L, *EU Constitutional Law: An Introduction* (2nd rev. edn, Hart Publishing 2012).

Rosen J, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House 2000).

Rosen J, ‘Privacy in Public Places’ (2000) 12 Cardozo Studies in Law and Literature 167.

Rosenfeld M, 'Judicial Balancing in Times of Stress: Comparing the American, British and Israeli Approaches to the War on Terror', (2006) 27 Cardozo Law Review 2079.

Rothstein MA (ed), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (Yale University Press 1997).

Rouvroy A, ‘Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence’ (2008) 2 Studies in Ethics, Law and Technology 1.

Rouvroy A and Poullet Y, ‘The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy’ in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009).

Rowland D, Kohl U and Charlesworth A, *Information Technology Law* (4th edn, Routledge 2012).

Rubin EL, ‘Law and Society & Law and Economics: Common Ground, Irreconcilable Differences, New Directions’ (1997) Wisconsin Law Review 521.

Saarenpää A, ‘Data protection: In pursuit of information some background to, and implementations of, data protection in Finland’ (1997) 11 International Review of Law, Computers & Technology 47.

Saarenpää, A ‘Finland’ in Blume P (ed), *Nordic Data Protection Law* (Kauppakaari DJØF 2001).

Scheinin M, ‘Terrorism and the Pull of 'Balancing' in the Name of Security’ in Scheinin M and others (eds) *Law and Security - Facing the Dilemmas*, (EUI Working Papers, LAW 2009/11, 2009).

Scheinin M and others (eds) *Law and Security - Facing the Dilemmas*, (EUI Working Papers, LAW 2009/11, 2009).

Scheppele KL, ‘Global Security Law and the Challenge to Constitutionalism after 9/11’ (2011) Public Law 352.

Schmitt C, *Politische Theologie* (4 Aufl., unveränderter Nachdruck der 1934 erschienene 2. Auflage, Duncker & Humblot 1985).

Schneier B, *Data and Goliath: The Hidden Battles to Collect your Data and Control your World* (W.W. Norton 2015).

Schneider F and Wahl T (eds), *Herausforderungen für das Recht der zivilen Sicherheit in Europa* (Nomos 2016).

Schütze R, *European Union Law* (Cambridge University Press 2015).

Schwartz PM, ‘Privacy and Democracy in Cyberspace’ (1999) 52 Vanderbilt Law Review 1607.

Schwerdtner P, *Das Persönlichkeitsrecht in der deutschen Zivilrechtsordnung: Offene Probleme einer juristischen Entdeckung* (Schweitzer 1976).

Seipel, P ‘Sweden’ in: Blume P (ed), *Nordic Data Protection Law* (Kauppakaari, DJØF 2001) 115-151.

Shany Y, ‘Toward a General Margin of Appreciation Doctrine in International Law?’ (2005) 16 European Journal of International Law 5.

Siemen B, *Datenschutz als europäisches Grundrecht* (Duncker & Humblot 2006).

Simitis S, ‘Reviewing Privacy in an Information Society’ (1987) 135 University of Pennsylvania Law Review 707.

Simmel G, *Soziologie* (Duncker & Humblot 1908).

Smith RE, 'Sometimes what's public is private. Legal rights to privacy in public spaces.' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance* (Routledge 2012) 370-379.

Solove DJ, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087.

Solove DJ, *Understanding privacy* (Harvard University Press 2008).

Solove DJ and Schwartz PM, *Privacy, Information, and Technology* (3rd edn, Wolters Kluwer Law & Business 2011).

Spaventa E, 'Fundamental Rights in the European Union' in Barnard C and Peers S (eds), *European Union Law* (Oxford University Press 2014).

Starr A and others, 'The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis' (2008) 31 Qualitative Sociology 251.

Stein SK, *Drittwirkung im Unionsrecht, Die Begründung einer Horizontalwirkung allein durch Vorrang und unmittelbare Anwendbarkeit* (Nomos 2016).

Štitilis D and Laurinaitis M, 'Legal regulation of the use of dashboard cameras: Aspects of privacy protection' (2016) 32 Computer Law & Security Review 316.

Sunstein CR, *Worst-case scenarios* (Harvard University Press 2009).

Svenonius O, *Sensitising Urban Transport Security: Surveillance and Policing in Berlin, Stockholm, and Warsaw* (Stockholm University 2011).

Tene O and Polonetsky J, 'Privacy in the Age of Big Data. A Time for Big Decisions' (2012) 64 Stanford Law Review Online 63.

Tistarelli M, Susan E. Barrett SE , and Toole AJO, 'Facial Recognition, Facial Expression and Intention Detection' in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012).

Tuori K, *Ratio and Voluntas: The Tension between Reason and Will in Law* (Ashgate, Aldershot 2011).

Tuori K, 'On legal hybrids' in Micklitz H and Svetiev Y (eds), *A Self-sufficient European Private Law: A Viable Concept* (Fiesole: European University Institute Working Papers, 2012).

Tuori K, 'A European Security Constitution' in Fichera M and Kremer J (eds), *Law and Security in Europe : Reconsidering the Security Constitution* (Intersentia 2013).

United Nations Development Programme (UNDP), *Human Development Report 1994* (Oxford University Press, 1994).

Vainio N and Miettinen S, 'Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States' (2015) 23 International Journal of Law and Information Technology 290.

van Dijck, J 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology' (2014) 12 Surveillance & Society.

Vermeulen M and Bellanova R, 'European 'smart' surveillance: What's at stake for data protection, privacy and non-discrimination?' (2012) Security and Human Rights 297.

Von Silva-Tarouca Larsen B, *Setting the Watch: Privacy and the Ethics of CCTV Surveillance* (Hart Publishing 2011).

Wakefield A, 'The Public Surveillance Functions of Private Security' (2004) 2 Surveillance & Society 529.

Waldron J, 'Security and Liberty: The Image of Balance' (2003) 11 Journal of Political Philosophy 191.

Walkila S, *Horizontal effect of fundamental rights contributing to the 'primacy, unity and effectiveness of European Union law'* (Diss., University of Helsinki, 2015).

Walt SM, 'The Renaissance of Security Studies' (1991) 35 International Studies Quarterly 211.

Warren SD and Brandeis LD, 'The Right to Privacy' (1890) 4 Harvard Law Review 194.

Warso Z, 'There's more to it than data protection – Fundamental rights, privacy and the personal/household exemption in the digital age' (2013) 29 Computer Law & Security Review 491.

Watkins D and Burton M (eds), *Research Methods in Law* (Oxon: Routledge 2013).

Weaver, O, 'Securitization and Desecuritization' in Lipschutz RD (ed), *On Security* (Columbia University Press 1995).

Webster CWR, 'CCTV Policy in the UK: Reconsidering the Evidence Base' (2009) 6 Surveillance & Society 10.

Webster CWR and others (eds), *Video surveillance: Practices and Policies in Europe* (IOS Press 2012).

Welsh BC and Farrington DP, 'Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis' (2009) 26 Justice Quarterly 716.

Westin AF, *Privacy and Freedom* (Bodley Head 1967).

White R, Ovey C and Jacobs FG, *Jacobs, White and Ovey: The European Convention on Human Rights* (5th edn, Oxford University Press 2010).

Whitman JQ, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2003-2004) 113 The Yale law journal 1151.

Wong, R and Savirimuthu J, All or Nothing: This is the Question? The Application of Art. 3(2) Data Protection Directive 95/46/EC to the Internet (2008) 25 John Marshall Journal of Computer & Information Law.

Wright D and Others (eds), *Safeguards in a World of Ambient Intelligence* (Springer 2010).

Internet Sources

ADABTS Report Summary, Final Report Summary - ADABTS (Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces), European Commission, 12 December 2014 http://cordis.europa.eu/result/rcn/153868_en.pdf accessed 12 March 2016.

ADABTS, WP3, D 3.1 'Abnormal Behaviour Definition', 23 March 2011, https://www.informationsystems.foi.se/main.php/ADABTS_D3.1_Abnormal_Behaviour_Definition_Public_(PU)_final.pdf?fileitem=7340175 accessed 17 October 2016.

ADABTS WP5 D 5.1 'Vision-based Human Detection and Action Analysis', 21 December 2011, https://www.informationsystems.foi.se/main.php/ADABTS%20D5.1%20Vision-based%20Human%20Detection%20and%20Action%20Analysis.pdf?fileitem=7340162 accessed 16 October 2016.

ADABTS WP5 D 5.2, Task 5.3 and 5.4: 'Sound Source Localization and Analysis', 10 December 2012, https://www.informationsystems.foi.se/main.php/D5.2_Sound_Source_Localization_and_Analysis.pdf?fileitem=7340174 accessed 16 October 2016.

Aldhous P and Seife C, Spies in the Sky, *BuzzFeed.com*, 6 April 2016, http://www.buzzfeed.com/peteraldhous/spies-in-the-skies accessed 12 April 2016.

American Civil Liberties Union (ACLU), Privacy Rights in the Digital Age. A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union, (ACLU Foundation 2014) https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf accessed 5 Mai 2016.

BAE Systems Columbia, 'Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS)' CS-13-F97-ARGUS-IS-Brochure, 10/2013 http://www.baesystems.com/en-sa/download-en-sa/20151124113917/1434554721803.pdf accessed 15 April 2016.

Bigo D and others, 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law', CEPS Paper in Liberty and Security in Europe, No 61/ November 2013, https://ssrn.com/abstract=2360473 accessed 10 January 2017.

Boehm, F and Cole DM: Data Retention after the Judgement of the Court of Justice of the European Union, Study funded by the Greens/EFA Group in the European Parliament, Münster/Luxembourg, 30 July 2014, http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf accesses 5 October 2015

Brühl J, Fuchs F, Gesucht: Einbrecher der Zukunft‘ in *Süddeutsche Zeitung, sueddeutsche.de*, 12 September 2014, http://www.sueddeutsche.de/digital/polizei-software-zur-vorhersage-von-verbrechen-gesucht-einbrecher-der-zukunft-1.2115086 accessed 7 April 2016.

BSIA, ‘An Introduction to Video Content Analysis - Industry Guide (BSIA, August 2016), http://www.bsia.co.uk/Portals/4/Publications/262-introduction-video-content-analysis-industry-guide-02.pdf accessed 15 October 2016.

Burgmer C, ‘Warum einen öffentlichen Platz besetzen?’ Deutschlandfunk, Essay und Diskurs, 03 October 2014, <http://www.deutschlandfunk.de/protestbewegung-warum-einen-oeffentlichen-platz-besetzen.1184.de.html?dram:article_id=299327> accessed 8 October 2016.

Cannataci, JA, ‘Squaring the Circle of Smart Surveillance and Privacy, 2010 Fourth International Conference on Digital Society’ in Council of Europe Recommendation R(87)15 & ETS Convention 108, Data Protection Vision 2020: Options for improving European policy and legislation during 2010-2020; Appendix 3, http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf accessed 17. November 2015.

DARPA, Persistent Stare Exploitation and Analysis System (PerSEAS), Broad Agency Announcement (BAA) for Information Processing Techniques Office (IPTO) Defense Advanced Research Projects Agency (DARPA), DARPA-BAA-09-55, 18 September 2009, https://www.fbo.gov/utils/view?id=1d32b1d49cdf59a1e5f8790260c7a350 accessed 17 October 2016.

Duri S and others, Framework for security and privacy in automotive telematics, in (2002) Proceedings of the 2nd International Workshop on Mobile Commerce, 25–32, http://www.cc.gatech.edu/projects/disl/courses/8803/backup/readinglist_files/p25-duri.pdf accessed 7 March 2015.

Düsseldorfer Kreis, Beschluss vom 26.02.2014 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams), http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/26022014_UnzulaessigkeitDashcams.pdf?__blob=publicationFile&v=1 accessed 15 March 2015.

FRA, Surveillance by Intelligence Services, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf accessed 6 Mai 2015.

Gardiner B, ‘Engineers Test Highly Accurate Face Recognition’ *Wired* (24.03.2008),

http://www.wired.com/science/discoveries/news/2008/03/new_face_recognition accessed 17 November 2015.

Green H, 'Sensor Revolution: Bugging the World. Soon, sensor networks will track everything from weather to inventory.' *Bloomberg Business Week Magazine*, 24 August 2003, http://www.businessweek.com/stories/2003-08-24/tech-wave-2-the-sensor-revolution accessed 3 October 2014.

Harris S and Schneier B, 'To Profile or Not to Profile? A Debate between Sam Harris and Bruce Schneier' in *Schneier on Security*, https://www.schneier.com/essays/archives/2012/05/to_profile_or_not_to.html accessed 7 April 2016.

Hogan J, 'Smart software linked to CCTV can spot dubious behaviour' *New Scientist*, 11.6.2003 https://www.newscientist.com/article/dn3918-smart-software-linked-to-cctv-can-spot-dubious-behaviour/ accessed 10 March 2016.

INDECT Intelligent information system supporting observation, searching and detection for security of citizens in urban environment, FP7-2007-SEC-218086, http://www.indect-project.eu/ accessed 9 Mai 2016.

INDECT Consortium, D1.1 Report on the collection and analysis of user requirements, European Seventh Framework Programme FP7-218086-Collaborative Project, 24 January 2012, http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_D1.1_v20091029a.pv.pdf/view accessed 5 December 2016.

INDECT, Report Summary, 'Final Report Summary - INDECT (Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment)' European Commission, 20 January 2016, http://cordis.europa.eu/result/rcn/175782_en.pdf accessed 17 October 2016.

IST Advisory Group: Ambient Intelligence: from vision to reality, For participation – in society & business. https://cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf accessed 16 October 2016.

IST Advisory Group, Working Group on International Cooperation: ICT research and innovation in a globalized world. A contribution for thinking strategically the role of international cooperation in EU ICT research and innovation, March 2012, http://cordis.europa.eu/fp7/ict/istag/documents/ict-research-and-innovation-final-72pp.pdf accessed 3 October 2014.

Johnston I, 'EU funding 'Orwellian' artificial intelligence plan to monitor public for "abnormal behaviour"' *The Telegraph*, 19 September 2009, http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html accessed 17 October 2016.

Kaskinen T and others, 'The Future as Told Through the Garden and the Streets. Scenarios for the Hyperconnected Nordic Societies of 2015-2040' The Naked Approach, Demos Helsinki, 2015 http://www.demoshelsinki.fi/wp-content/uploads/2015/11/Naked-approach.pdf accessed 24 April 2016.

Koffeman NR, (The right to) personal autonomy in the case law of the European Court of Human Rights (External Research Report, Leiden: Leiden University 2010), 23-52 https://openaccess.leidenuniv.nl/bitstream/handle/1887/15890/N.R.%20Koffeman%20-%20%28The%20right%29%20to%20personal%20autonomy%20in%20the%20case%20law%20of%20the%20ECtHR%20%282010%29.pdf accessed 16 October 2016.

La Vigne NG and others, Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention (Final Technical Report, Urban Institute 2011), http://www.urban.org/sites/default/files/alfresco/publication-pdfs/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.PDF accessed 10 October 2016.

Lohr S, 'IBM Looks Ahead to a Sensor Revolution and Cognitive Computers.' *The New York Times: Bits*, 17 December 2012, http://bits.blogs.nytimes.com/2012/12/17/ibm-looks-ahead-to-a-sensor-revolution-and-cognitive-computers/ accessed 3 October 2014.

Meister A, Funkzellenabfrage: Die millionenfache Handyüberwachung Unschuldiger. *Netzpolitik.org*, 21 December 2012, https://netzpolitik.org/2012/funkzellenabfrage-die-millionenfache-handyuberwachung-unschuldiger/ accessed 2 November 2015

Privacy International, 'National Privacy Ranking 2007, Leading Surveillance Societies around the World', http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597&als[theme]=Data Protection and Privacy Laws accessed 17.11.2015.

Privacy International: 'What is mass surveillance?' https://www.privacyinternational.org/node/52 accessed 16 October 2016.

Schneier B, What our top spy doesn't get: Security and Privacy aren't opposites *Wired.com*, 24 January 2008 http://www.wired.com/2008/01/securitymatters-0124/ accessed 23 March 2016.

Schneier, B, 'The Trouble with Airport Profiling' in *Forbes*, 9 May 2012 and *Schneier on Security*, https://www.schneier.com/essays/archives/2012/05/the_trouble_with_air.html accessed 7 April 2016.

SPIEGEL Online, Demo in Dresden: Polizei wertete Tausende Handy-Daten aus, 19 June 2011, http://www.spiegel.de/netzwelt/web/demo-in-dresden-polizei-wertete-tausende-handy-daten-aus-a-769275.html accessed 2 November 2015.

Stanley, J, 'What to Make of the TrapWire Story?' ACLU Speech, Privacy & Technology Project, ACLU, 14 August 2012, https://www.aclu.org/blog/what-make-trapwire-story?redirect=blog/technology-and-liberty-free-speech-national-security/what-make-trapwire-story accessed 3 November 2015.

Stanley J, Drone 'Nightmare Scenario' Now Has A Name: ARGUS, American Civil Liberties Union ACLU, 21 February 2013 https://www.aclu.org/blog/drone-nightmare-scenario-now-has-name-argus?redirect=blog/technology-and-liberty-free-speech-national-security/drone-nightmare-scenario-now-has-physical accessed 15 April 2016.

Stanley J, 'Report Details Government's Ability to Analyze Massive Aerial Surveillance Video Streams' ACLU, 5 April 2013, https://www.aclu.org/blog/report-details-governments-ability-analyze-massive-aerial-surveillance-video-streams?redirect=blog/technology-and-liberty-free-speech-national-security/report-details-governments-ability-analyze accessed 15 April 2016.

The New York Times Editorial Board, 'Mass Surveillance Isn't the Answer to Fighting Terrorism' *The New York Times Online*, 17 November 2015) http://www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html accessed 17. November 2015.

Timberg, C 'New surveillance technology can track everyone in an area for several hours at a time' *The Washington Post*, 5 February 2014, https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html accessed 12 April 2016.

Wakefield J, 'Surveillance cameras to predict behaviour' *BBC News*, 1 May 2002 http://news.bbc.co.uk/2/hi/sci/tech/1953770.stm accessed 12 March 2016.