

FACULTY OF LAW
DEANERY
TIENSESTRAAT 41
3000 LEUVEN
Academic year 2020-2021



Big brother is watching you!

**How online police infiltration and online systemic police observation have
to be balanced with fundamental rights and freedoms**

A comparative analysis between Belgium and the United States

Supervising Professors: D. VAN DAELE & D. SCHANZER

Assistant: A. VEREECKE

Dissertation, written by SYLVIA LISSENS,

for the degree of MASTER IN

CRIMINOLOGICAL SCIENCES

Catholic University of Leuven

In cooperation with

Venice International University and Duke University

FACULTY OF LAW
DEANERY
TIENSESTRAAT 41
3000 LEUVEN
Academic year 2020-2021



Big brother is watching you!

**How online police infiltration and online systemic police observation have
to be balanced with fundamental rights and freedoms**

A comparative analysis between Belgium and the United States

Supervising Professors: D. VAN DAELE & D. SCHANZER

Assistant: A. VEREECKE

Dissertation, written by SYLVIA LISSENS,

for the degree of MASTER IN

CRIMINOLOGICAL SCIENCES

Catholic University of Leuven

In cooperation with

Venice International University and Duke University

Summary

Law enforcement investigation techniques have to be balanced with fundamental rights. In this comparative law research between Belgium and the United States, the investigation techniques of police infiltration (undercover operations), systemic police observation (police surveillance) and their online counterparts are analyzed in relation to the fundamental rights to privacy, a fair trial and the freedom of speech. Firstly, the legal frameworks of regular (offline) police infiltration and systemic police observation are discussed. Secondly, their online counterparts are analyzed. Finally, these investigation techniques are balanced with the right to privacy, the right to a fair trial and the freedom of speech. By employing the most-different approach, these two different policy systems, namely the Belgian and US legal systems, are analyzed in how they succeed to balance privacy and security.

Belgium only recently, in 2003, granted an official legal basis to these (offline) investigation techniques. Police infiltration's online counterpart received only in 2016 a legal basis and online systemic police observation has up until today not been officially regulated in Belgian criminal procedural law. The United States have been employing and developing these investigation techniques since the 1920s, and with the digital revolution they have been relatively quickly adapted to the digital world. These investigation techniques are mostly used in organized crime, terrorism and drug investigations which often have a cross-border dimension and are facilitated by the internet. Given the necessary cooperation in this kind of situations, it is useful that the Belgian and US regulations are compatible with each other.

Legal sources such as the Belgian Code of Criminal Procedure and US criminal law together with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations are analyzed in this research. The latter fulfill more or less the same role for the FBI in the United States as the Belgian Code of Criminal Procedure in regulating these investigation techniques. The fundamental rights are enshrined in the Belgian Constitution and European Convention on Human Rights on the one hand and the US Constitution on the other hand. The literature available at the (online) libraries of KU Leuven and Duke University was used to provide a better understanding on how these specific regulations function in everyday society. While researching, the snowball-method was employed according to which the references in the consulted articles were checked and the relevant ones were selected in order to continue the search for relevant articles. The case law was for Belgium (and Europe) consulted through the

online databases of Jura (Wolters Kluwer) and HUDOC for the European Court of Human Rights, and for the United States through the online databases of Justia and Casetext.

Receiving feedback from both Belgian and US supervisors was an added value for this dissertation and led to conclusions and interpretations that could otherwise not have been reached. The use of similar definitions, such as the Belgian and US definitions of off- and online undercover operations, are very useful for cross-border cooperation. The US Attorney General's Guidelines on FBI Undercover Operations could be granted a legally enforceable status, so they could be relied on in court by a suspect. The Belgian enumerated list of criminal offenses allowed to be committed during undercover operations may in some cases be too strict and therefore a middle ground between the Belgian and US legal system with broad categories of allowed criminal offenses would be preferable.

A warrant should be required for regular (offline) systemic police observation at all times, and therefore the US exception where the FBI may conduct long-term in person surveillance without a warrant should be deleted. Online publicly accessible information on the contrary is by definition publicly accessible and the US approach where a warrant is not required for systemic monitoring of this information could be interesting for Belgium, which current approach where a warrant is often required seems to be too protective. However, online non-publicly available information should only be accessed by law enforcement based on a warrant and this warrant requirement should in the United States not be circumvented by asking the suspect's virtual friends to show or share this private information with state officials. A warrant requirement could in the United States also be introduced for obtaining communication's location information and for requesting data to identify the sender or receiver, given that its reasoning for not requiring a warrant is based on an outdated analogy between smartphones and letters.

The fundamental rights to privacy, a fair trial and the freedom of speech have to be respected during undercover operations and police surveillance. Both investigation techniques should therefore only be initiated based on a prior warrant. In order to safeguard the defendant's trial rights, the United States could consider the Belgian approach of creating two investigation files, a public and a confidential one, of which the latter could only be reviewed by the judge and would contain sensitive information. It could be interesting for future research to interview people working in this field of law enforcement as well in Belgium as in the United States to obtain their insights and knowledge on the recommendations formulated in this research.

Acknowledgment

Writing this dissertation has brought me on an incredible journey of exchanges and meeting new people that I could not have imagined when I started my second master's degree. I would like to thank my supervising Professor Dirk Van Daele and Ms. Anke Vereecke at KU Leuven, Belgium for their feedback and support to help me write this dissertation. I would also like to thank Veerle Timmermans who is the coordinator of the exchange program at KU Leuven and who suggested me to join the Globalization Program at Venice International University in Italy. It was lovely to live in such a beautiful place as Venice and to meet Ms. Cristina Di Gioia and Dean Luca Pes at VIU, who also supervised this dissertation and granted me the opportunity to join the Worldwide Mobility Program thanks to which I could write my dissertation at Duke University in the United States. Unfortunately, it was not possible to conduct the exchange in person, but it was still very interesting for me to follow the online classes at Duke and receive feedback and additional information on the US law part of this dissertation from my supervising Professor David Schanzer. This feedback was very helpful and made me understand the US legal system much better and detailed than I could have understood from only reading the literature and case law.

The incredible twist that my life has made was however in the second half of 2020, when I was granted the opportunity to conduct the research exchange at Duke online as a solution for the impossibility of going to the United States in person. I ended up conducting this exchange in Bielsko-Biała, Poland, the city where my mother originally grew up. Moving here connected me again to my family and learned me to appreciate how important it is to have them close to me. Their everlasting positive attitude and helpfulness meant and means a lot to me, so thank you all for that. Living here also brought my love for nature back that I first learned to appreciate while living in Helsinki, Finland during my first exchange. It was lovely to write my dissertation in the beautiful mountain surroundings and to be connected with nature again. This journey has finally also brought me back to one of my favorite sports, which is martial arts. I would like to thank all the guys from my Jiu-Jitsu club for their kindness and friendship. Especially meeting one person there made 2020 become not such a bad year as it seemed to be. I would like to thank you Marcin for all the trainings, the mountain hikes, the great moments and for just always being my sunshine on a rainy day. Dziękuję Ci słoneczko. I would also like to thank my brother Renaat and his best friend Cassandra for pre-reading my dissertation. I know it was a lot, but your feedback was highly appreciated. Mercikes voor alles. Finally, I would of course

want to thank my mother who was always happy and supportive when I called her about all my exchange plans. It was always enough to just tell you that I'm hopping on a plane for another exchange and even though I know you had a hard time seeing me leave every time, you were always supporting me on every new adventure I decided to start. Thank you for your support and patience, and thank you for always encouraging me to follow my dreams and my heart. Dziękuję Ci, dankjewel.

Thank you, kiitos, grazie mille, dankuwel, dziękuję...to everyone.

Table of contents

Summary i

Acknowledgment i

List of abbreviations.....vii

Introduction 1

Part I: An introduction to police infiltration, observation and fundamental rights 2

Chapter 1: The investigation techniques of police infiltration and systemic police observation 2

§1. General overview of police infiltration 2

§2. General overview of systemic police observation 8

Chapter 2: The investigation techniques of police infiltration and systemic police observation in the digital age..... 11

§1. Law enforcement investigation techniques and the digital revolution 11

§2. Cybercrime, social media and law enforcement 14

§3. Police infiltration and systemic police observation in the digital age 18

Chapter 3: Fundamental rights..... 21

§1. Secrecy vs. transparency..... 21

§2. Secrecy vs. right to privacy 22

§3. Anonymity vs. right to privacy..... 23

§4. Anonymity vs. freedom of expression 25

Part II: Methodology..... 27

Chapter 1: Justification for comparative law research 27

Chapter 2: Research Questions..... 30

Chapter 3: Choice of countries..... 32

Chapter 4: Selection of sources for comparative law research 33

Chapter 5: Research quality and limitations 34

Part III : Police infiltration and undercover operations	36
Chapter 1: Historical overview of police infiltration	36
<i>§1. Pre-9/11 undercover operations</i>	36
a) Pre-9/11 undercover operations in Belgium and Europe	36
b) Pre-9/11 undercover operations in the United States	40
c) Pre-9/11 undercover operations compared	43
<i>§2. Post-9/11 undercover operations</i>	44
a) Post-9/11 undercover operations in Belgium and Europe	44
b) Post-9/11 undercover operations in the United States	44
c) Post-9/11 undercover operations compared	46
Chapter 2: Legal framework on police infiltration	47
<i>§1. Belgian legal framework on police infiltration</i>	47
<i>§2. US legal framework on police infiltration</i>	54
<i>§3. Legal framework on police infiltration compared</i>	58
Chapter 3: Legal framework on police infiltration in the digital age	60
<i>§1. Belgian legal framework on police infiltration in the digital age</i>	60
<i>§2. US legal framework on police infiltration in the digital age</i>	64
<i>§3. Legal framework on police infiltration in the digital age compared</i>	67
Chapter 4: The four principles compared	69
<i>§1. Subsidiarity</i>	69
a) Subsidiarity in Belgium	69
b) Subsidiarity in the United States	70
c) Subsidiarity compared	72
<i>§2. Proportionality</i>	73
a) Proportionality in Belgium	73
b) Proportionality in the United States	75
c) Proportionality compared	75

§3. <i>The prohibition of provocation</i>	76
a) The prohibition of provocation in Belgium	77
b) The prohibition of provocation in the United States	78
c) The prohibition of provocation compared	84
§4. <i>The prohibition to commit criminal offenses</i>	85
a) The prohibition to commit criminal offenses in Belgium	86
b) The prohibition to commit criminal offenses in the United States	87
c) The prohibition to commit criminal offenses compared	89
Part IV: Systemic police observation and surveillance	91
Chapter 1: Legal framework on systemic police observation	91
§1. <i>Belgian legal framework on systemic police observation</i>	91
§2. <i>US legal framework on systemic police observation</i>	95
§3. <i>Legal framework on systemic police observation compared</i>	99
Chapter 2: Legal framework on systemic police observation in the digital age	101
§1. <i>General legal framework on systemic police observation in the digital age</i>	101
a) Belgian general legal framework on systemic police observation in the digital age ...	101
b) US general legal framework on systemic police observation in the digital age	104
c) General legal framework on systemic police observation in the digital age compared	105
§2. <i>Online publicly accessible information: legal framework</i>	105
a) Belgian legal framework on online publicly accessible information	106
b) US legal framework on online publicly accessible information	107
c) Legal framework on online publicly accessible information compared	108
§3. <i>Online non-publicly accessible information: legal framework</i>	109
a) Belgian legal framework on online non-publicly accessible information	109
b) US legal framework on online non-publicly accessible information	112
c) Legal framework on online non-publicly accessible information compared	114

Part V: Privacy, fair trial and freedom of speech	115
Chapter 1: The right to privacy and (online) police infiltration / systemic observation.....	116
<i>§1. Privacy vs. (online) police infiltration / systemic observation in Belgium and Europe</i>	<i>116</i>
<i>§2. Privacy vs. (online) police infiltration / systemic observation in the United States</i>	<i>119</i>
<i>§3. Privacy vs. (online) police infiltration / systemic observation compared</i>	<i>124</i>
Chapter 2: The right to a fair trial and (online) police infiltration / systemic observation	125
<i>§1. Fair trial vs. (online) police infiltration / systemic observation in Belgium and Europe ..</i>	<i>125</i>
<i>§2. Fair trial vs. (online) police infiltration / systemic observation in the United States.....</i>	<i>126</i>
<i>§3. Fair trial vs. (online) police infiltration / systemic observation compared.....</i>	<i>129</i>
Chapter 3: Freedom of speech and (online) police infiltration / systemic observation	130
<i>§1. Freedom of speech vs. (online) police infiltration / systemic observation in Belgium and Europe</i>	<i>130</i>
<i>§2. Freedom of speech vs. (online) police infiltration / systemic observation in the United States</i>	<i>131</i>
<i>§3. Freedom of speech vs. (online) police infiltration / systemic observation compared.....</i>	<i>134</i>
Part VI: Analysis	136
Part VII: Conclusion	147
Bibliography	149

List of abbreviations

ECHR	European Convention on Human Rights.
ECtHR	European Court of Human Rights.
EU	European Union.
BOM, SIM	Bijzondere OpsporingsMethode, Belgian Special Investigation Method.
BS	Belgisch Staatsblad, Belgian Official Gazette.
Cass.	Hof van Cassatie, Belgian Court of Cassation.
Gw.	Grondwet, Belgian Constitution.
GwH	Grondwettelijk Hof, Belgian Constitutional Court.
KB	Koninklijk Besluit, Royal Decree.
KI	Kamer van Inbeschuldigingstelling, Belgian Indictment Chamber.
MvT	Memorie van Toelichting, Explanatory Memorandum.
Sv.	Wetboek van Strafvordering, Belgian Code of Criminal Procedure.
V.T.Sv.	Voorafgaande Titel van het Wetboek van Strafvordering, Chapter preceding the Belgian Code of Criminal Procedure.
Sw.	Strafwetboek, Belgian Criminal Code.
WPA	Wet op het Politieambt, Belgian law on law enforcement.
CSLI	Cell-site location information.
DEA	The US Drug Enforcement Administration.
DIOG	FBI Domestic Investigations and Operations Guide.
FBI	Federal Bureau of Investigation.
U.S.C.	United States Code.

Introduction

In a world of spies and informants it was hard to trust anyone and you never knew who your friends or enemies were. You had to look over your shoulder, make sure no one was following you and be very careful with whom you were talking. Your friends from yesterday could after all turn out to be your enemies of today and share your valuable information with people you wish had never known what you knew... Undercover operations and police surveillance were initially unpopular as investigation techniques since they were associated with exactly these scenarios. Over time their use regained legitimacy, since crime rates were increasing and the population demanded a response from law enforcement. On a path of overenthusiastic use and scandals, they finally arrived in the digital age where they had to make their way through laptops, smartphones and servers. The spies and informants of the past had to learn the IT skills of today. The scandals demanded the development of a legal framework for the use of these investigation techniques and law enforcement had to realize that they were not allowed to surveil anyone who they deemed suspicious. Spies and informants have however always been trained to be invisible and could easily adapt to new circumstances. Countries and borders were without meaning and the world was their playground. This has nowadays become even more true, since they only need a computer in order to access a whole new virtual world. A world where merely all information can be found, where private as well as professional conversations are being held and where all this information is being stored. Some of this information can be accessed by anyone when it is publicly available. Other information will only be accessible by law enforcement based on a warrant. Belgium and the United States have regulated these investigation techniques and had moreover to make sure that they complied with the fundamental rights and freedoms. Even though Belgium has only recently granted a legal basis to (online) police infiltration and systemic police observation operations, whereas the United States have been employing these investigation techniques since the 1920s, this functional comparative law research will show that based on the literature and the analysis of the Belgian and US legal frameworks, they have a lot in common. These commonalities are useful in a globalizing world where cross-border cooperation has become essential. Finally, sometimes the Belgian and sometimes the US regulation will serve as an example and provide a better answer to the main question of this research; how the investigation techniques of online police infiltration and online systemic police observation are successfully balanced with the fundamental rights to privacy, a fair trial and the freedom of speech.

Part I: An introduction to police infiltration, observation and fundamental rights

Chapter 1: The investigation techniques of police infiltration and systemic police observation

Law enforcement has different possibilities and methods to use in their fight against crime.¹ This research will focus on the investigation techniques of police infiltration, systemic police observation and their online counterparts. These investigation techniques are well-known and have been employed by law enforcement for a long period of time (*Part III, Chapter 1*). It is therefore interesting to see how these well-embedded investigation methods are employed in and adapted to the virtual world in which we are living today.

§1. General overview of police infiltration

Police infiltration, also known as covert police operations or undercover operations, can be employed in different cases, forms and with different aims.² Police infiltrators may aim at being present when a crime occurs or try to gather evidence that is necessary for criminal prosecution of the suspect.³ Undercover agents will for example play the role of buyers or sellers of stolen

¹ D.J. KORF, E. KLEEMANS, T. DECORTE and T. BOEKHOUT VAN SOLINGE, “Drugs en drugshandel in Nederland en België”, *Tijdschrift voor Criminologie* 2006, Vol.48(2), (115) 121.

² M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 87; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 163; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 50; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1114; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; P. VANWALLEGHEM, “Infiltratie mag ook om verdachte te arresteren”, *De Juristenkrant* 2014, Vol.4, (2) 2.

³ H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 370-371; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/22-216/28; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3 and 87; T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 233; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 106; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 163; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 63-65; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3),

or illegal goods, pretend to be a potential victim or act as a corrupt government official in cases of fraud or extortion.⁴ Infiltration may also have an intelligence gathering aim, when the infiltrator wants to collect as much information as possible in order to prevent a crime from occurring or to establish the relations and network of a suspect.⁵ This last strategy will most often be used in important and serious cases that can endanger the national security of a country, like cases of terrorism.⁶

Three constitutive elements are usually present in order to define an undercover operation; secrecy, deception and participation in criminal activities.⁷ In most cases, undercover agents

(1111) 1111; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; P. VANWALLEGHEM, "Infiltratie mag ook om verdachte te arresteren", *De Juristenkrant* 2014, Vol.4, (2) 2.

⁴ A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1085; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 57; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 106; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 246; S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 32; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 7 and 63-67; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 241-242; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1111-1116; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240 and 249-250.

⁵ H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/22-216/26 and 216/35; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3 and 87; T. FORAN, "Covert Operations on the Internet" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 233; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 163-164; I. LEIGH, "Undercover: Police Surveillance in America By G.T. Marx: Reviewed", *British Journal of Criminology* 1991, Vol.31(1), (100) 101; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 9 and 61-63; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 262; G. PATAKI, "Conducting Reactive and Proactive Internet Investigations" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 256; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240.

⁶ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 87; G. PATAKI, "Conducting Reactive and Proactive Internet Investigations" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 256; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240.

⁷ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 750; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/73-216/74; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 8-9; F. HUTSEBAUT and K. VAN CAUWENBERGHE, "De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?", *Orde van de dag* 2003, Vol.4, (7) 8; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 156-158 and 181 and 190; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een

will operate under disguise (secrecy) and use a false identity (deception) in order to obtain the information or evidence that is needed.⁸ The use of a false identity is however not anymore required for online police infiltration, since it is also possible to access websites or conversations anonymously.⁹ Undercover agents are sometimes required to take part in the criminal activities that they are investigating in order to convince the suspects or persons of interest to trust and rely on them (participation).¹⁰ Under these conditions, they will infiltrate

noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 50; I. LEIGH, “Undercover: Police Surveillance in America By G.T. Marx: Reviewed”, *British Journal of Criminology* 1991, Vol.31(1), (100) 100; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 29; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1149-1150; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 205; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 401 and 410.

⁸ B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 750; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/73-216/74; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 87; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 53; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 8; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 157 and 165-167 and 190; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 246; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 50; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 29; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1149-1150; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 241-243; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 205; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 410.

⁹ C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; S. ROYER, “Wet 25 december 2016 digitaal spuurwerk op twee punten vernietigd (noot onder GwH 6 december 2018)”, *NJW* 2019, Vol.398, (212) 212; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 400.

¹⁰ H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 34; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/73-216/74; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 34; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62-63; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 165-167; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 50; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242-243; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 499 and 538; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”,

criminal organizations and try to obtain the information necessary for their investigation and prosecution.¹¹ The crimes for which police infiltration can be employed are mainly situated in the field of organized crime and serious criminal offences.¹² Organized crime can according to the U.S. Department of Justice's Law Enforcement Strategy to Combat International Organized Crime be defined as "self-perpetuating associations of individuals, often structured and hierarchical, supported by ethnic solidarity, language, custom, social or family connections, who operate (internationally) for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence".¹³ Law enforcement may also use this technique to investigate (suspected) cases of drugs and drug trafficking, smuggling, money laundering, stock exchanges, forgery, fencing of stolen goods, street crime, fraud, corruption, smuggling of persons, prostitution, sex offenses, arms and ammunitions trafficking, and suspected cases of terrorism.¹⁴ After the terrorist attacks of 9/11 in New York in 2001, the main focus of law

Annu.Rev.Law Soc.Sci. 2008, Vol.4, (239) 240 and 252; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 401.

¹¹ H. BERKMOES, "De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden", *Orde van de dag* 2003, Vol.4, (25) 34; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 370-371; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/73-216/74; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 53; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003, Vol.11, (1134) 1135; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242-243; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1148; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; P. VANWALLEGHEM, "Infiltratie mag ook om verdachte te arresteren", *De Juristenkrant* 2014, Vol.4, (2) 2; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 410.

¹² M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 9; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 128; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1115; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 493 and 508; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

¹³ J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 516-517; U.S. DEPARTMENT OF JUSTICE, *Overview of the Law Enforcement Strategy to Combat International Organized Crime*, <https://www.justice.gov/sites/default/files/criminal-icitap/legacy/2015/04/23/04-23-08combat-intl-crime-overview.pdf>, 2 (consultation 25 October 2020).

¹⁴ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 746; H. BERKMOES, "Bijzondere

enforcement shifted towards fighting Islamic terrorism, which is the type of terrorism best characterized by this event.¹⁵ These terrorist attacks are in recent years mainly committed by first- and second-generation immigrants in the United States and Europe, so-called home-grown terrorists.¹⁶ On top of the focus on Islamic terrorism and the prevention of terrorist attacks, the fight against organized crime still remains an important topic as well.¹⁷ Undercover operations nowadays are therefore mainly focused on organized crime and terrorism cases.¹⁸ Even though the criticisms of and concerns about undercover operations (*see below*) are still present, they became silenced based on the need to fight terrorism.¹⁹ Consequently, in both Europe and the United States an expansion of the use of police infiltration occurred.²⁰ Combatting terrorism

opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/73-216/74; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 9; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 128 and 140-141; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 241-242; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1115-1118; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 493 and 508; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240 and 260.

¹⁵ P.A. FERNANDEZ-SANCHEZ, *International Legal Dimension of Terrorism*, Leiden, Martinus Nijhoff Publishers, 2009, 9-10; INTERNATIONAL BAR ASSOCIATION, *International terrorism: legal challenges and responses: a report by the International bar association's task force on international terrorism*, London, International bar association, 2003, 5-7; R. LETSCHERT, A. PEMBERTON and I. STAIGER, *Assisting Victims of Terrorism*, The Netherlands, Springer, 2010, 2-7; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 493; A. SCHBLEY, “Defining Religious Terrorism: A Causal and Anthological Profile”, *Studies in Conflict & Terrorism* 2003, Vol.26(2), (105) 105-106; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 4; T. TURAN, “War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties”, *Uluslararası Hukuk ve Politika* 2006, Vol.7, (111) 111.

¹⁶ C. BAIL, F. MERHOUT and P. DING, “Using Internet search data to examine the relationship between anti-Muslim and pro-ISIS sentiment in U.S. counties”, *Science Advances* 2018, Vol.4(6), (1) 1.

¹⁷ S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 9; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 4.

¹⁸ S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 9; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 159; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1115; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 493; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

¹⁹ E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 159; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 263.

²⁰ E. LICHTBLAU and W.M. ARKIN, *More Federal Agencies Are Using Undercover Operations*, <https://www.nytimes.com/2014/11/16/us/more-federal-agencies-are-using-undercover-operations.html> (consultation 25

and the investigation technique of police infiltration have moreover something in common, they want to prevent crimes and harm from occurring.²¹

The use of police infiltration is however not without criticism due to its dubious character. The secrecy and deception used in this technique may sometimes lead to an unpredictable outcome of the investigation.²² Undercover operations can for example take longer than expected and police infiltrators can get too deep into the operation what might entail the risk of them siding with the criminal organization instead of with law enforcement.²³ Scandals like the François case in Belgium (*Part III, Chapter 1, §1, a*) and the ABSCAM case in the United States (*Part III, Chapter 1, §1, b*) may occur.²⁴ Undercover agents might also be discovered by criminals and in those situations the suspects may make the agents believe that they are part of the criminal organization, while actually knowing that they are part of law enforcement and provide them on purpose with false information. Another issue is that undercover operations offer law enforcement the opportunity to shape the events to a certain extent themselves.²⁵ In those

October 2020); J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 493; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 263.

²¹ H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/26 and 216/35; P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 680; J. SHERMAN, “A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations”, *Journal of constitutional law* 2009, Vol.11(5), (1475) 1475; S. SINGLETON, “Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques”, *Ohio Northern University Law Review* 2004, Vol.30(3), (417) 417; T. TURAN, “War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties”, *Uluslararası Hukuk ve Politika* 2006, Vol.7, (111) 115 and 124; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390.

²² C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 139; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 61.

²³ D. KOWALCZYK and M.J. SHARPS, “Consequences of Undercover Operations in Law Enforcement: a Review of Challenges and Best Practices”, *Journal of Police and Criminal Psychology* 2017, Vol.32, (197) 198; G.T. MARX, “Who really gets stung? Some issues raised by the New Police Undercover Work”, *Crime & Delinquency* 1982, Vol.28(2), (165) 177.

²⁴ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 55; G. DWORKIN, “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), (17) 24; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 53-54.

²⁵ ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/60-216/61; G. DWORKIN, “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), (17) 24; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1568-1569; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 163-164; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; I. LEIGH, “Undercover: Police Surveillance in America By G.T. Marx: Reviewed”, *British Journal of Criminology* 1991, Vol.31(1), (100) 101; G.T. MARX, *Undercover:*

situations, they are not only investigating (suspected) crimes, but sometimes also helping to create them.²⁶ It is understandable that both the suspect and the undercover agent (also called agent provocateur) influence each other, and as the name says can ‘provoke’ each other, having an impact on their mutual behavior (*Part III, Chapter 4, §3*).²⁷ Lastly, the allowance of participation in criminal activities by undercover agents may also lead to some difficulties, which in the most extreme cases might lead to a complete dismissal of charges (*Part III, Chapter 4, §4*).²⁸

§2. General overview of systemic police observation

In real life, it is relatively easy to make a distinction between situations of police infiltration and situations of police observation. Where during police infiltration operations undercover agents infiltrate the suspect’s world, the suspect will only be surveilled without his knowledge during police observation operations.²⁹ Law enforcement surveils someone when they only

police surveillance in America, Berkeley, University of California press, 1988, 65-67 and 130-132; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 244-245; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1112-1114 and 1148; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 497 and 511-519 and 537; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239 and 249 and 260; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2870.

²⁶ *Ibid.*

²⁷ ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/60-216/61; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 130-132; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1112-1115 and 1144-1148; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 497 and 537; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240 and 249-252 and 260; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2869-2870.

²⁸ J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 539; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240-241 and 257-260; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2870.

²⁹ D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 274; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot,

remotely observe the suspect and do not attempt to influence his or her behavior.³⁰ The use of deception (*Part I, Chapter 1, §1*) to reveal private information about the suspect is, in contrast to police infiltration, not allowed.³¹ The main goal consists of gathering information about the suspect's activities.³² Long-term or systemic police surveillance can be defined as "the planned, round-the-clock observation of the activities of a suspect, with the intention of gaining a comprehensive insight into his everyday life".³³ The elements of consistency and a certain period of time in order to be able to recognize patterns in someone's life are therefore a necessary requirement.³⁴ Short-term police surveillance consists, on the contrary, of single observations which do not allow law enforcement to gain a (detailed) insight into someone's life.³⁵ The latter type of surveillance happens in most cases only for a single moment, a day, or some days spread over a period of one month.³⁶ Given that the main focus of this research consists of the online counterparts of police infiltration and observation, only systemic or long-term police observation will be discussed, since both police infiltration and systemic police observation take place over a long-lasting period of time, are characterized by some form of consistency and aim at gaining insight into someone's life.³⁷ The online counterpart of systemic

Ashgate, 1998, 10 and 121; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 55-59; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 211-214; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246.

³⁰ S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 121; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 81.

³¹ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 59; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 106.

³² S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 121; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 81.

³³ *Ibid.*

³⁴ J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 742-743; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 542-547; E.W. MARSHALL, J.L. GROSCUP, E.M. BRANK, A. PEREZ and L.A. HOETGER, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; M. RADLER, "Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1213-1214 and 1229-1236.

³⁵ T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 547; M. RADLER, "Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1236.

³⁶ *Ibid.*

³⁷ C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 217 and 224; C. CONINGS, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr.* 2019, Vol.5, (257) 261; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 29; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003,

police observation is sometimes difficult to distinguish from online police infiltration, in contrast to an incidental or short-term observation, and the interference with mainly the fundamental right to privacy might therefore be more severe. New technologies allow law enforcement to passively surveil potential suspects without their knowledge on a much broader scale.³⁸ Where in the past a specific suspect was targeted and put under police surveillance, nowadays' technologies allow this on a much broader scale with the consequence of possibly turning every person into a potential suspect.³⁹

Vol.11, (1134) 1149-1150; B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 205 and 280; P. VANWALLEGHEM, "Infiltratie mag ook om verdachte te arresteren", *De Juristenkrant* 2014, Vol.4, (2) 2; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264.

³⁸ D.A. DRIPPS, "At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense", *University of Illinois Law Review* 1993, Vol.2, (261) 274; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 10; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 55-59; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 211-214; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246.

³⁹ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 59; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 2 and 211-214; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246.

Chapter 2: The investigation techniques of police infiltration and systemic police observation in the digital age

§1. Law enforcement investigation techniques and the digital revolution

Given that the internet is relatively new (it has mainly developed in the last twenty years) and very quickly evolving, this means that not everyone has the adequate technological knowledge to understand all of its possibilities.⁴⁰ This is no different for law enforcement, where among most police officers there is a lack of knowledge of the multiple opportunities the digital world has to offer.⁴¹ As a consequence, there are not enough human and technical resources in order to track down and investigate all the online gathered data relating to criminal offenses or to conduct online investigation techniques such as online police infiltration.⁴² It is insufficient that only a small group of experts is specialized in cybercrime, which in most cases only focuses on organized crime.⁴³

⁴⁰ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 61-66; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 126-127; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologie neutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 21; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 1 and 13.

⁴¹ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 61; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 126-127; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 231 and 242; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 243-245; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 254-255; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 13; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 25-27 and 37.

⁴² *Ibid.*

⁴³ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 62; E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 315; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 243; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 27.

The internet is moreover capable of connecting people that would in real life probably not or less easily have connected, such as people with and without a criminal background, or those who are and are not part of a criminal environment.⁴⁴ Self-organized terrorist groups have in recent years for example formed and grown through linkages to an ISIS or jihadi ideology related Facebook page.⁴⁵ On these Facebook pages one can find other people with the same or similar ideologies.⁴⁶ In this way, they can form groups which in the worst cases can evolve into terrorist cells and networks.⁴⁷ However, in contrast to suspending these accounts and pages, it can sometimes be more useful for law enforcement to monitor these pro-ISIS users' communications and gather important intelligence information about these people and their networks.⁴⁸

The internet has also created new means of communication due to which the distance between people has become irrelevant.⁴⁹ These communication techniques are more difficult to monitor, since they are often well-encrypted or make use of highly secured networks.⁵⁰ Terrorist

⁴⁴ E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; E. DE PAUW, "Sociale controle in onlinemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 5-9; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 997; T. SPAPENS, E. KOLTHOFF and W. STOL, "Georganiseerde misdaad in de 21^{ste} eeuw", *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 6; J. VAN KOKSWIJK, "Sociale controle in onlinemeenschappen: voordelen van zelfregulering op internet", *Orde van de dag* 2010, Vol.3, (23) 24; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 389.

⁴⁵ N.F. JOHNSON, M. ZHENG, Y. VOROBYEVA, A. GABRIEL, H. QI, N. VELASQUEZ, P. MANRIQUE, D. JOHNSON, E. RESTREPO, C. SONG and S. WUCHTY, "New online ecology of adversarial aggregates: ISIS and beyond", *Science* 2016, Vol.352(6292), (1459) 1459; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 400.

⁴⁶ E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; J. VAN KOKSWIJK, "Sociale controle in onlinemeenschappen: voordelen van zelfregulering op internet", *Orde van de dag* 2010, Vol.3, (23) 24; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 389 and 400.

⁴⁷ J. VAN KOKSWIJK, "Sociale controle in onlinemeenschappen: voordelen van zelfregulering op internet", *Orde van de dag* 2010, Vol.3, (23) 24.

⁴⁸ A.V. LIEBERMAN, "Terrorism, the Internet, and Propaganda: A Deadly Combination", *Journal of National Security Law & Policy* 2017, Vol.9(1), (95) 123.

⁴⁹ R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 997; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 372; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 245; T. SPAPENS, E. KOLTHOFF and W. STOL, "Georganiseerde misdaad in de 21^{ste} eeuw", *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 3-6; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 389.

⁵⁰ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 53-54; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 372; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 245; C. ROSMAN,

organizations have for example also used PlayStation as a means of communication and were able to hide their intentions under the excuse that it was just a game they were talking about.⁵¹ The internet is a worldwide web that does not solely operate within the borders of one country.⁵² In most cases, there will be a cross-border dimension which will require that the police has to cooperate with other police and private instances, nationally as well as internationally.⁵³ This can cause difficulties in evidence gathering and admissibility before court, because it will not always be clear which police department will have the authority to investigate.⁵⁴ This creates

Terroristen communiceren ongestoord via Spelcomputer, <https://www.ad.nl/nieuws/terroristen-communiceren-ongestoord-via-spelcomputer~ac9839ad/?referrer=https%3A%2F%2Fwww.google.com%2F> (consultation 25 October 2020); T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 3-6; J. VAN HORENBEEK and R. MEEUS, *Rekruteert IS nu ook jongeren via PlayStation? Hoe dan?*, <https://www.demorgen.be/nieuws/rekruteert-is-nu-ook-jongeren-via-playstation-hoe-dan~bb8de0fb/> (consultation 25 October 2020); D. VERLAAN, *Hoe IS de PlayStation 4 inzet om aanslagen voor te bereiden*, <https://www.rtlnieuws.nl/geld-en-werk/artikel/778301/hoe-de-playstation-4-inzet-om-aanslagen-voor-te-bereiden> (consultation 25 October 2020); W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 389; 4Gamers, *Waarom terroristen Playstation 4 als communicatiemiddel gebruiken*, https://www.nieuwsblad.be/cnt/blgpe_01972626 (consultation 25 October 2020).

⁵¹ C. ROSMAN, *Terroristen communiceren ongestoord via Spelcomputer*, <https://www.ad.nl/nieuws/terroristen-communiceren-ongestoord-via-spelcomputer~ac9839ad/?referrer=https%3A%2F%2Fwww.google.com%2F> (consultation 25 October 2020); J. VAN HORENBEEK and R. MEEUS, *Rekruteert IS nu ook jongeren via PlayStation? Hoe dan?*, <https://www.demorgen.be/nieuws/rekruteert-is-nu-ook-jongeren-via-playstation-hoe-dan~bb8de0fb/> (consultation 25 October 2020); D. VERLAAN, *Hoe IS de PlayStation 4 inzet om aanslagen voor te bereiden*, <https://www.rtlnieuws.nl/geld-en-werk/artikel/778301/hoe-de-playstation-4-inzet-om-aanslagen-voor-te-bereiden> (consultation 25 October 2020); W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 389; 4Gamers, *Waarom terroristen Playstation 4 als communicatiemiddel gebruiken*, https://www.nieuwsblad.be/cnt/blgpe_01972626 (consultation 25 October 2020).

⁵² L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 52 and 63-65; M. CHAWKI, A. DARWISH, M.A. KHAN and S. TYAGI, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 20; E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 232; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 15; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 258-259; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 25-27 and 37.

⁵³ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 52-65; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 20; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 15; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 258-259; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 74; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 25-27 and 37.

⁵⁴ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 58-65; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 20; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een

the risk that evidence may be declared inadmissible because it was obtained in an illegal way.⁵⁵ As a consequence, it will not be possible to convict a suspect, since he cannot be convicted based on illegally obtained evidence.⁵⁶ This situation is also referred to as ‘fruit of the poisonous tree’.⁵⁷ In recent years, it has however become more easy to monitor these new techniques of communication, since law enforcement has recruited more computer science specialists with the adequate technological knowledge in order to focus more on cybercrime.⁵⁸

§2. Cybercrime, social media and law enforcement

The information age in which we are living today has made technology indispensable in our everyday lives.⁵⁹ The majority of people uses the internet and social media on a daily basis.⁶⁰

technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 15; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 69; W.P.H. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 25-27 and 37.

⁵⁵ T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 69-71.

⁵⁶ *Ibid.*

⁵⁷ *Ibid.*

⁵⁸ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 62; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 10; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 2 and 212; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 14; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 6.

⁵⁹ C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 99; E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 315; E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; E. DE PAUW, “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, (5) 5-6; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 10; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 523; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 1; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 389.

⁶⁰ J. CLEMENT, *Global social networks ranked by number of users 2020*, <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (consultation 18 November 2020); J. CLEMENT, *Number of global social network users 2017-2025*, <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/> (consultation 18 November 2020); E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 315 and 324; E. DE PAUW, “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, (5) 5; S. KEMP, *Digital 2019: Global internet use accelerates*, <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates> (consultation 18 November 2020); R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018,

There is no generally accepted definition of the concept ‘social media’, but based on the consulted literature, social media will in this research be considered as “internet websites and applications which make it possible to create ‘user generated content’”.⁶¹ Facebook, Twitter and YouTube are examples of this type of social media, where users are generating the content of these websites and where as a result a large amount of information can be found.⁶² BOYD and ELLISON’s definition of “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system” is more accurate for Facebook than for example for YouTube.⁶³ The definition of ‘user generated content’ is therefore chosen, given its broader range of applicability to different social media sites.

The possibilities that the internet, also called cyberspace, has to offer are not only beneficial to people with good intentions, but also to (cyber)criminals.⁶⁴ Based on the consulted literature,

Vol.61(3), (523) 523-524; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 1.

⁶¹ W. BRUGGEMAN, “Politie, justitie en (nieuwe) sociale media”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (199) 199; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 206; E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; E. DE PAUW, “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, (5) 7-8; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 232-243; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 259; S. ZOURIDIS and P. TOPS, “Sociale media: vehikels voor collectieve wijsheid of sociale verstoring?”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (246) 248.

⁶² E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 324; E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; E. DE PAUW, “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, (5) 7-8; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 232-239; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 523-524.

⁶³ E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 316.

⁶⁴ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 51; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 3; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 205; E. DE PAUW, *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 3; E. DE PAUW, “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, (5) 6; B.-J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research” in B. AKHGAR and B. BREWSTER, *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Switzerland, Springer International Publishing, 2016, (3) 6-7; M. WASCHKE, *Personal Cybersecurity: How to avoid and recover from cybercrime*, Berkeley, Apress, 2017, 1; W. YPERMAN, S. ROYER and F.

cybercrime can be defined as “an activity in which computers or computer networks are used as a tool, a target or a location for committing criminal acts”, however there is no consensus about one common definition.⁶⁵ Cybercrime has evolved from a relatively new type of crime to a daily phenomenon that is capable of having severe consequences on a large scale.⁶⁶ It can also occur on a smaller unorganized scale, but can still have severe consequences.⁶⁷ Generally speaking, two types of cybercrime can be identified; 1) *non-virtual* or *cyber-enabled crimes* that are committed by making use of the internet, but which consist of already existing forms of crime, like stalking or fraud, and 2) *virtual* or *cyber-dependent crimes* that can only be committed in the virtual world, like hacking.⁶⁸ In addition to regular cyberspace that people commonly use, there also exists a darkweb which is not as easily accessible as regular cyberspace, since it requires the provision of a specific URL or an invitation from an already existing member and not just a search term like regular websites do.⁶⁹ On the darkweb, also known as darknet or deepweb, many illegal goods and services are offered, like drugs or weapons.⁷⁰ The darknet will however not be discussed in this research (*Part II, Chapter 1*).

Law enforcement has to follow this technological progress and has to be active, overt and covert, on the internet and on social media as well.⁷¹ From the police’s perspective, social media

VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 389.

⁶⁵ M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 3-6; M. WASCHKE, *Personal Cybersecurity: How to avoid and recover from cybercrime*, Berkeley, Apress, 2017, 3.

⁶⁶ M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 7; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 206; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 26.

⁶⁷ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 206; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 26-27.

⁶⁸ M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 5; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 205-207; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 2; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 5 and 14.

⁶⁹ C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politie internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3.

⁷⁰ *Ibid.*

⁷¹ E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 317; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 10; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 523-524; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 257; W. YPERMAN,

offer a relatively easy platform in order to reach an enormous amount of people in a very short amount of time.⁷² They can take advantage of this through informing the population about their work and projects, but also through providing objective information in case a crisis situation occurs.⁷³ Informing the population via for example Facebook or Twitter may be a very useful tool.⁷⁴ It also offers the possibility to more easily stimulate the participation of the population in police investigations.⁷⁵ When they are looking for a missing person, they can post this on social media with the request to share the message, or when they just implemented a new regulation, they can ask their followers for feedback and suggestions. This may result in the creation of a more effective and wider accepted provision of services by the police.⁷⁶ Social

S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 389 and 400.

⁷² E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 317-318; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 235-239; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 257; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 259-260.

⁷³ S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 234-239; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 257; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 259.

⁷⁴ E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 317-318; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 234-239; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 257-258; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 259-260.

⁷⁵ E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 317-318; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 234; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 257-258; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 259-260; S. ZOURIDIS and P. TOPS, “Sociale media: vehikels voor collectieve wijsheid of sociale verstoring?”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (246) 252.

⁷⁶ S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 234; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 257-258; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*

media can also be used to monitor individual suspects (online systemic police observation) or to build online profiles and networks (online police infiltration) in order to come in contact with certain suspects.⁷⁷

§3. Police infiltration and systemic police observation in the digital age

In the virtual world, the distinction between police infiltration and systemic police observation becomes more difficult to make. The main criterion in order to distinguish online systemic police observation from online police infiltration is whether personal information is being shared.⁷⁸ As mentioned in the previous chapter, one of the constitutive elements of police infiltration, namely secrecy by adopting a fictitious identity, will not always be necessary in the online world. It is perfectly possible to anonymously gain access to a website or to use a nickname without providing any personal information.⁷⁹ Those situations are not considered to be police infiltration, but only observation.⁸⁰ The observer gains (anonymously) access to a website and ‘observes’ its content.⁸¹ However, in case a law enforcement officer will join an online conversation or will have to provide personal information in order to gain access to a website, this will be qualified as police infiltration.⁸²

2012, Vol.33(3), (258) 259; S. ZOURIDIS and P. TOPS, “Sociale media: vehikels voor collectieve wijsheid of sociale verstoring?”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (246) 251.

⁷⁷ R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 523; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 241-245; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 258.

⁷⁸ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 64; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 215-224; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politiezone internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264-265; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 391.

⁷⁹ *Ibid.*

⁸⁰ *Ibid.*

⁸¹ *Ibid.*

⁸² *Ibid.*

The internet is a source that is publicly accessible for everyone, also for the police.⁸³ However, they are only allowed to use publicly accessible data to gather information unrestrictedly.⁸⁴ For non-publicly accessible data, a stricter regime is applicable which will be discussed in *Part IV, Chapter 2, §3*. Law enforcement can for example check the Facebook page of a suspect and determine which type of relations he has with certain people based on publicly accessible information.⁸⁵ When law enforcement analyzes the information on social media, they are mainly focused on two types of content.⁸⁶ First of all, the content that the user himself shares, like photos, files or thoughts (on his Facebook page or via a tweet).⁸⁷ Some people post photos of or comments about their crimes on social media, so in those cases it is very easy for the police to track them down and arrest them for the crimes they committed.⁸⁸ Secondly, users

⁸³ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 65; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 216; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 28-29; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390-391.

⁸⁴ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 65; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 216; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331-332; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 999; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 258; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; W.PH. STOL, E.R. LEUKFELDT and H. KLAP, “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), (25) 29; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 269; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390-391.

⁸⁵ C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331-332; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 258; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 260-269.

⁸⁶ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 207; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 12.

⁸⁷ *Ibid.*

⁸⁸ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 206; S. DE SMET, “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (231) 237; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 530

also leave certain digital traces behind due to which it is possible to identify and locate them.⁸⁹ This second type of information might for example provide a person with an alibi that he was not on the crime scene based on his location during that time.⁹⁰ It can also be used for tracking down missing persons, based on the GPS function in their cell phones.⁹¹

and 541-542; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 12; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 260.

⁸⁹ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 207-211; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 99-100; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 553-554; T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 12; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 389-390.

⁹⁰ *Ibid.*

⁹¹ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 208; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 99-100; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 536; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 553-554.

Chapter 3: Fundamental rights

The dubious character of the investigation technique of police infiltration with its secrecy and deception has an important influence on the privacy and fair trial rights of the suspect. An undercover agent will after all come into close contact with his suspect and aim at gaining his confidence. As a consequence, the suspect might say much more to the undercover agent than he would if he would know that he is in fact part of law enforcement. The investigation technique of systemic police observation might also endanger the suspect's privacy and fair trial rights, given that in these situations technical means will be applied for surveillance instead of an undercover agent, but with the same aim of gaining (personal) information about the suspect. Moreover, some people might fear to exercise their right to freedom of speech and association, since this might attract the attention of law enforcement.

§1. Secrecy vs. transparency

Nowadays' secrecy is being restricted by the request of transparency on the one hand and the right to privacy of citizens on the other hand.⁹² A government is considered to be more efficient and increasing its economic and technological power when it can provide its citizens with freedom of information.⁹³ The debate between secrecy and transparency has existed for a long time.⁹⁴ Transparency is often presented as a reaction against secrecy, even though it actually functions as an element of it, and also as an element of democracy, in order to maintain its law and order.⁹⁵ Advocates of their full and extreme version, as in 'everything should be a secret' or 'everything should be transparent' are both protecting their interests.⁹⁶ The population is

⁹² C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 8.

⁹³ T. BLANTON, "The World's Right to Know", *Foreign Policy* 2002, Vol.131, (50) 50.

⁹⁴ C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 10-11; T. BLANTON, "The World's Right to Know", *Foreign Policy* 2002, Vol.131, (50) 50.

⁹⁵ C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 12; E. BRAAT, "In voor- en tegenspoed: Het huwelijk tussen parlement en inlichtingen- en veiligheidsdiensten", *Justitiële verkenningen* 2018, Vol.44(1), (33) 34-46; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 370.

⁹⁶ C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 8; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 370.

worried that it does not know what the government is doing or what it knows about them, so it is clear that there is information that the population would like to keep private.⁹⁷ The government as well might fear that when too much information is being disclosed to the population, its classified operations could become too transparent and this could in some cases have severe consequences.⁹⁸ Law enforcement will for example not be able to use covert techniques anymore once they will become publicly known. An undercover agent's life or family could also be in danger if the suspect would find out his real identity. Most citizens accept therefore that a balance between the security of the state (secrecy) and the rights of its citizens (transparency) is necessary in order to promote and protect the liberty of both parties.⁹⁹

§2. Secrecy vs. right to privacy

Secrecy and covert police surveillance are also restricted by the right to privacy.¹⁰⁰ Regular (offline) police surveillance was concerned with privacy issues, like for example how long someone could be under surveillance.¹⁰¹ With the aid of modern technologies and the internet, large amounts of information have become easily available and accessible, what as a consequence has lowered bureaucratic barriers and conditions to privacy intrusions.¹⁰² Law

⁹⁷ C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 8; S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 30; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 370.

⁹⁸ C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 8; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 370.

⁹⁹ C. BIRCHALL, "Introduction to 'Secrecy and Transparency': The Politics of Opacity and Openness", *Theory, Culture & Society* 2011, Vol.28, (7) 14; A.N. GUIORA, "Transnational Comparative Analysis of Balancing Competing Interests in Counter-Terrorism", *Temple International & Comparative Law Journal* 2006, Vol.20(2), (363) 363; P. ROSENZWEIG, "Civil Liberty and the Response to Terrorism", *Duquesne Law Review* 2004, Vol.42(4), (663) 663.

¹⁰⁰ E. BRAAT, "In voor- en tegenspoed: Het huwelijk tussen parlement en inlichtingen- en veiligheidsdiensten", *Justitiële verkenningen* 2018, Vol.44(1), (33) 33; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 11; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 129; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 1; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 524; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-241.

¹⁰¹ R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 524.

¹⁰² E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 13; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 524; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 2.

enforcement has to first of all learn to understand the limits between what is publicly available and what is private on social media, like on Facebook and Twitter.¹⁰³ This will be further explained in *Part IV, Chapter 2, §2-§3*, where the distinction will be made between which information is considered to be publicly available and non-publicly available on the internet.

§3. Anonymity vs. right to privacy

The internet offers the possibility of being anonymous, which can be useful for activists and whistleblowers, but also for people with criminal intentions. In the first case, people can be afraid to address certain issues using their own identity.¹⁰⁴ The internet offers these people the possibility to do this anonymously, so they do not have to fear for their safety or for negative repercussions towards them or their relatives.¹⁰⁵ Anonymous online profiles cannot only be used by activists in order to call for rebellion or riots against the government, it can also be used by the government to identify these activists, spread fake news or propaganda and discover the activists' networks.¹⁰⁶ The government might in addition set up fake activist networks in order to track down and identify activists that will try to become a member.¹⁰⁷ The use of anonymous online profiles is however restricted by social media.¹⁰⁸ Facebook has for example a 'real name

¹⁰³ E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 13.

¹⁰⁴ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 53; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 97-100; E. MOROZOV, "WikiLeaks and the Perils of Extreme Glasnost", *New Perspectives Quarterly* 2011, Vol.28(1), (7) 7; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 268.

¹⁰⁵ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 53; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 97-100.

¹⁰⁶ Y.-L. CHIN, "Evgeny Morozow, The Net Delusion: How Not to Liberate the World: Reviewed", *New Media & Society* 2012, Vol.14(5), (890) 891; D. CLEMENTE, "The net delusion: how not to liberate the world by Evgeny Morozow: reviewed", *International Affairs* 2013, Vol.89(1), (197) 198; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1004; S. ZOURIDIS and P. TOPS, "Sociale media: vehikels voor collectieve wijsheid of sociale versterking?", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (246) 246-247 and 255.

¹⁰⁷ S. ZOURIDIS and P. TOPS, "Sociale media: vehikels voor collectieve wijsheid of sociale versterking?", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (246) 255.

¹⁰⁸ R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 551; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 268.

policy' according to which its users are required to use their own name.¹⁰⁹ When someone wants to register for a Facebook account, he has to acknowledge and agree to the Terms and Community Standards, which prohibit the creation and use of fake accounts.¹¹⁰ Facebook considers this the most important requirement in order to protect its users from harm and to create a safe community where people can interact.¹¹¹ Therefore, it can disable accounts which are violating this principle.¹¹² These Terms and Community Standards apply not only to civilians, but also to law enforcement officers (*Part III, Chapter 3, §2*).¹¹³

The European Court of Human Rights (ECtHR) has also already made clear, in the case of *K.U. vs. Finland*, that there is no absolute right to online anonymity.¹¹⁴ *K.U.* was a twelve year old boy who was the subject of an advertisement of a sexual nature posted about him, without his knowledge, on an internet dating site. Given that his contact details were also posted on the advertisement, this constituted a criminal act since the little boy could become a target for pedophiles. The service provider refused to disclose the identity of the person who had posted the advertisement, since there was no legal basis in Finnish law that could force the service provider to disregard his professional secrecy. The ECtHR concluded that “the Finnish legislature should have provided a legal framework for reconciling the confidentiality of

¹⁰⁹ FACEBOOK, *Servicevoorwaarden*, <https://www.facebook.com/legal/terms> (consultation 27 October 2020); FACEBOOK, *Welke namen zijn toegestaan op Facebook?*, https://www.facebook.com/help/112146705538576?helpref=faq_%20content (consultation 27 October 2020); T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 248-249; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 551-552; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1001; J. SULLIVAN, *Facebook letter to DEA*, <https://www.documentcloud.org/documents/1336541facebook-letter-to-dea.html> (consultation 27 October 2020); M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 268.

¹¹⁰ T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 248-249; J. SULLIVAN, *Facebook letter to DEA*, <https://www.documentcloud.org/documents/1336541facebook-letter-to-dea.html> (consultation 27 October 2020).

¹¹¹ *Ibid.*

¹¹² *Ibid.*

¹¹³ T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 248-249; K. HEATHER, *Police embrace social media as crime-fighting tool*, <https://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html> (consultation 18 November 2020); J. SULLIVAN, *Facebook letter to DEA*, <https://www.documentcloud.org/documents/1336541facebook-letter-to-dea.html> (consultation 27 October 2020)

¹¹⁴ ECtHR 2 December 2008, nr. 2872/02, *K.U./Finland*, AM 2009, Vol.1-2, 123, *Juristenkrant* 2009, Vol.181, 5, *RDTI* 2009, Vol.34, 93, *T.Strafr.* 2009, Vol.1, 38; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 214; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 268.

internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others”.¹¹⁵ This is however not the same as saying that there is a prohibition of online anonymity.¹¹⁶ The court is well-aware that in some situations, like for activists or whistleblowers, guaranteeing their anonymity is necessary for their own safety, but this has to be balanced with the rights of both parties.¹¹⁷

§4. Anonymity vs. freedom of expression

In the *K.U. vs. Finland* case not only the right to privacy, but also the freedom of expression was discussed by the court. In its final conclusion, the ECtHR decided that both rights are not absolute and can be restricted. It stated that “although freedom of expression and confidentiality of communications are primary considerations and users of (...) internet services must have a guarantee that their own privacy and freedom of expression will be respected, this right is not absolute”.¹¹⁸ The main idea behind this reasoning is that the anonymity that internet services offer may also be (mis)used by people who hold prejudiced or extreme views or by criminals, like in the *K.U. vs. Finland* case or by ISIS terrorists, in order to evade detection by law enforcement.¹¹⁹ The latter can recruit new members, communicate anonymously and

¹¹⁵ ECtHR 2 December 2008, nr. 2872/02, *K.U./Finland*, *AM* 2009, Vol.1-2, 123, *Juristenkrant* 2009, Vol.181, 5, *RDTI* 2009, Vol.34, 93, *T.Strafr.* 2009, Vol.1, 38; A. BODNAR and D. PUDZIANOWSKA, *Violation of the right to respect for private and family life in the case of K.U. vs. Finland*, <https://humanrightshouse.org/articles/violation-of-the-right-to-respect-for-private-and-family-life-in-the-case-of-k-u-v-finland/> (consultation 27 October 2020).

¹¹⁶ ECtHR 2 December 2008, nr. 2872/02, *K.U./Finland*, *AM* 2009, Vol.1-2, 123, *Juristenkrant* 2009, Vol.181, 5, *RDTI* 2009, Vol.34, 93, *T.Strafr.* 2009, Vol.1, 38; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 214; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 269.

¹¹⁷ ECtHR 2 December 2008, nr. 2872/02, *K.U./Finland*, *AM* 2009, Vol.1-2, 123, *Juristenkrant* 2009, Vol.181, 5, *RDTI* 2009, Vol.34, 93, *T.Strafr.* 2009, Vol.1, 38; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 53; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 214; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 269.

¹¹⁸ ECtHR 2 December 2008, nr. 2872/02, *K.U./Finland*, *AM* 2009, Vol.1-2, 123, *Juristenkrant* 2009, Vol.181, 5, *RDTI* 2009, Vol.34, 93, *T.Strafr.* 2009, Vol.1, 38; A. BODNAR and D. PUDZIANOWSKA, *Violation of the right to respect for private and family life in the case of K.U. vs. Finland*, <https://humanrightshouse.org/articles/violation-of-the-right-to-respect-for-private-and-family-life-in-the-case-of-k-u-v-finland/> (consultation 27 October 2020).

¹¹⁹ C. BAIL, F. MERHOUT and P. DING, “Using Internet search data to examine the relationship between anti-Muslim and pro-ISIS sentiment in U.S. counties”, *Science Advances* 2018, Vol.4(6), (1) 2; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen

sometimes even prepare and organize terrorist attacks and other crimes through social media.¹²⁰ Police surveillance and undercover operations might also infringe people's freedom of expression or change their behavior, when as its consequence they will avoid certain places, gatherings or posting certain online comments out of fear for negative repercussions by the government.¹²¹ This will be explained more detailed in *Part V, Chapter 3, §2*.

in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 51-53; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 101-102; Y.-L. CHIN, "Evgeny Morozow, The Net Delusion: How Not to Liberate the World: Reviewed", *New Media & Society* 2012, Vol.14(5), (890) 891; E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 12; A.V. LIEBERMAN, "Terrorism, the Internet, and Propaganda: A Deadly Combination", *Journal of National Security Law & Policy* 2017, Vol.9(1), (95) 102-103; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242; M. WASCHKE, *Personal Cybersecurity: How to avoid and recover from cybercrime*, Berkeley, Apress, 2017, 27.

¹²⁰ C. BAIL, F. MERHOUT and P. DING, "Using Internet search data to examine the relationship between anti-Muslim and pro-ISIS sentiment in U.S. counties", *Science Advances* 2018, Vol.4(6), (1) 3; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 205; N.F. JOHNSON *et al.*, "New online ecology of adversarial aggregates: ISIS and beyond", *Science* 2016, Vol.352(6292), (1459) 1459.

¹²¹ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 56; D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 207-210 and 218-223 and 239; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 534-540; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 522-523 and 567; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 247 and 264; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 4 and 7-10 and 48; T. TURAN, "War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties", *Uluslararası Hukuk ve Politika* 2006, Vol.7, (111) 118; M.A. WASSERMAN, "First Amendment limitations on police surveillance: The case of the Muslim surveillance program", *New York University Law Review* 2015, Vol.90(5), (1786) 1787-1797 and 1817-1818.

Part II: Methodology

Chapter 1: Justification for comparative law research

In this dissertation the investigation techniques of (online) police infiltration and (online) systemic police observation were balanced with the fundamental rights and freedoms. More specifically, first the legal frameworks of regular (offline) police infiltration and systemic police observation were discussed. Secondly, their online counterparts were analyzed. And finally, these investigation techniques were balanced with the right to privacy, the right to a fair trial and the freedom of speech.

These topics were in this comparative law research analyzed for Belgium and the United States. The types of crime being investigated while making use of these techniques consist mainly of organized crime, terrorism and drug cases. They occur often cross-border and are facilitated by the worldwide web which does not operate within the borders of one country. Given the necessary cooperation in this kind of situations¹²², it was interesting to see whether the Belgian and US regulations on (online) police infiltration and (online) systemic police observation are compatible with each other, and, how they comply with the fundamental rights and freedoms. The fundamental rights to privacy and a fair trial, and the freedom of speech are protected in Belgium by the Belgian Constitution and the European Convention on Human Rights, and in the United States by the Bill of Rights. These three fundamental rights were selected based on the literature, since they appeared to be most relevant in the context of the investigation techniques of (online) police infiltration and (online) systemic police observation.¹²³ By

¹²² M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 4 and 143; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 141 and 151; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 262.

¹²³ *Everson v. Board of Education*, 330 U.S. 1 (1947); *United States v. Robel*, 389 U.S. 258 (1967); *Anderson v. Davila*, 125 F.3d 148 (3rd Cir. 1997); *Bland v. Roberts*, No. 12-1671 (4th Cir. 2013); *Hassan et al. v. City of New York*, No. 14-1688 (3rd Cir. 2015); H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/20; D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 207-210 and 218-223 and 239; E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 13; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 261-262; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties

comparing these fundamental rights and freedoms, it could be adjudicated whether they comprise of the same or similar ideas in both countries or, on the contrary, whether there are differences between them.¹²⁴ Conclusively, it was then possible to decide which regulations and definitions are more suitable and therefore preferable, while keeping in mind the special historical, social and legal circumstances of each country.

The type of research conducted in this dissertation was a functional comparative law research. Its aim is to find topics that can be compared based on the fact that they fulfill the same function in different legal systems.¹²⁵ It focuses on a specific social issue or an overarching factual problem in order to find similarities and differences between legal systems instead of focusing on norms and concepts that are country-specific for a certain legal system.¹²⁶ The investigation techniques analyzed in this research are for example named differently in Belgium and the United States. Where in Belgium the term ‘police infiltration’ is used, it is in the United States named as ‘undercover operations’. This is also the case for ‘systemic police observation’, which is a term used in Belgium, but which is in the United States named as ‘police surveillance’. The awareness of these concept differences was raised by supervising Professor David Schanzer from Duke University, United States when he pointed out in his feedback that he does not know the Belgian concepts which were used in the chapter titles of this dissertation (*Part II, Chapter 5*). Given that it was difficult to find a neutral term for these complex investigation techniques that would suit and adequately define these techniques for both countries, the US specific concepts were added to the part titles and placed next to the Belgian concepts. For this reason, the terms ‘police infiltration’ and ‘undercover operations’ on the one hand, and ‘systemic police observation’ and ‘police surveillance’ on the other hand will throughout this research be used as synonyms. Another important remark made by Professor Schanzer was the author’s fixation on the search for US legislation. In his feedback he pointed out that the Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations and the FBI’s internal Domestic Investigations and Operations Guide fulfill in the United States more or less the same

Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 4 and 7-10 and 48; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1787-1797 and 1817-1818.

¹²⁴ G. DANNEMANN, “Comparative Law: Study of Similarities or Differences?” in M. REIMANN and R. ZIMMERMANN, *The Oxford handbook of comparative law*, Oxford, Oxford University press, 2019, (391) 391.

¹²⁵ E. BILLIS, “On the methodology of comparative criminal law research: Paradigmatic approaches to the research method of functional comparison and the heuristic device of ideal types”, *Maastricht journal of European and comparative law* 2017, Vol.24(6), (864) 867.

¹²⁶ *Ibid.*

role for the FBI as the Belgian Code of Criminal Procedure (Sv.). Therefore, an additional focus on and discussion of these guidelines was also added to this research.

In order to determine how a specific regulation functions in everyday society, not only the legislation and legal doctrine (which in the United States consists mainly of case law) was analyzed, but also the literature (*Part II, Chapter 4*). The law has been created to fulfill a certain function in society and therefore both of these sources should be assessed and understood together.¹²⁷ The freedom of speech is in the United States for example a universal right. This means that speech can even be defamatory.¹²⁸ It is enshrined in the Bill of Rights, which is mainly focused on freedom (more than on security), given its historical aim to protect the citizens against unreasonable government interference.¹²⁹ Individuals in the United States should therefore be free to exercise their rights protected by the US Constitution (*Part V, Chapter 3, §2*). In Europe, the stress has been more on security and the rights of one party are as a consequence limited by the rights of the other party. Freedom of speech is therefore only allowed as long as it does not consist of defamation or hate speech (*Part V, Chapter 3, §1*). This understanding and interpretation of the law can only be reached if one has an understanding of the broader social structures in which the law is functioning. Therefore, this research also focused on the social background in which the relevant investigation methods are being used.¹³⁰ Finally, both the Belgian and US legal systems were compared and in accordance with their adaptability to the specific social situation of each country, it was determined which system seems to be the best one finding a balance with the fundamental rights and freedoms.¹³¹

Since the concepts “online police infiltration” and “online police observation” are very broad, some limitations in order to conduct this research were needed. In the literature study, the demarcation between short-term and long-term (systemic) police observation has already been explained (*Part I, Chapter 1, §2*). Since the aim of this research was to compare and analyze the relation between the investigation methods of police infiltration and police observation on the one hand, and, the fundamental rights and freedoms on the other hand, only systemic or long-term police observation was discussed and the investigation technique of short-term police

¹²⁷ R. MICHAELS, “The Functional Method of Comparative Law” in M. REIMANN and R. ZIMMERMANN, *The Oxford handbook of comparative law*, Oxford, Oxford University press, 2019, (346) 347-348.

¹²⁸ M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1818.

¹²⁹ H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 244.

¹³⁰ *Ibid.*

¹³¹ *Ibid.*

observation was not considered. The investigation method of police infiltration shows many similarities with the investigation method of systemic police observation, such as the requirement of consistency and the ability to gain insight into someone's private life. The investigation method of short-term police observation does not have these characteristics and the fundamental rights are therefore less endangered compared to its long-term counterpart. The right to privacy for example is more likely to be infringed by long-term observation when law enforcement is able to recognize patterns in someone's life than by a single short-term observation.

“Online” investigation techniques take place on the internet, but since “the internet” is a broad notion as well, this research focused mainly on social media and did not discuss the darknet. This is a choice of the author, who is more familiar with social media than with the darknet. Given that the majority of people uses social media and less people are active on the darknet, the latter mainly for illegal purposes, the author found it more relevant to discuss social media instead of the darknet.¹³²

Chapter 2: Research Questions

The main research question of this research was “How are the investigation techniques of online police infiltration and online systemic police observation balanced with the fundamental rights to privacy, a fair trial and the freedom of speech in Belgium and the United States?”. In order to answer this main research question, it had to be divided into three topics, namely police infiltration (and undercover operations), systemic police observation (and police surveillance) and the fundamental rights to privacy, a fair trial and the freedom of speech, leading to the following sub-questions:

- How is (online) police infiltration regulated in Belgium and the United States?
- How is (online) systemic police observation regulated in Belgium and the United States?

¹³² J. CLEMENT, *Global social networks ranked by number of users 2020*, <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (consultation 18 November 2020); J. CLEMENT, *Number of global social network users 2017-2025*, <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/> (consultation 18 November 2020); J. CLEMENT, *Share of internet users who have used technologies that allow access to the dark web as of February 2019, by country*, <https://www.statista.com/statistics/1015229/dark-web-access-technology-usage-by-country/> (consultation 10 December 2020).

- How do (online) police infiltration and (online) systemic police observation comply with the fundamental rights and freedoms in Belgium and the United States?
 - How do (online) police infiltration and (online) systemic police observation comply with the right to privacy in Belgium and the United States?
 - How do (online) police infiltration and (online) systemic police observation comply with the right to a fair trial in Belgium and the United States?
 - How do (online) police infiltration and (online) systemic police observation comply with the freedom of speech in Belgium and the United States?

The main research question of this research was a normative question and aimed to determine how the Belgian and US legal systems balance their investigation methods of online police infiltration and online systemic police observation with the fundamental rights and freedoms. This type of research question requires an evaluative approach in order to conclude which legal system, Belgian or US, is better suited in a certain situation. The two main criteria for conducting this analysis were effectiveness (for law enforcement) and the protection of the fundamental rights and freedoms (for the public). Based on an analysis of both legal systems, the legal system best suited to balance these criteria could be determined. This was also dependent on the specific situation and social circumstances in which that particular legislation is being applied.

In order to come to an evaluation, it was first necessary to analyze the relevant regulation and fundamental rights of both legal systems. Since the sub-questions consisted of descriptive questions (what is the legal framework, how is e.g. the right to privacy regulated and interpreted), a textual research had to be conducted.¹³³ A textual research consists mainly of the analysis of written documents like legislation and it requires additionally a consultation of the literature (books and articles) in order to determine the specific scope and interpretation of these written legal documents.¹³⁴ There are five types of interpretation which can be distinguished, namely: 1) grammatical interpretation and text analysis; 2) systemic or logic interpretation; 3) legal or legal historical interpretation; 4) teleological interpretation, and; 5) sociological interpretation.¹³⁵ In this research the second and fifth type of interpretation were applied. Systemic or logic interpretation consists of analyzing a rule of law based on its legal context.¹³⁶

¹³³ P. SCHOUKENS, K. HENDRICKX, E. TERRYIN and L. KESTEMONT, *Rechtswetenschappelijk schrijven*, Leuven, Acco, 2012, 38-39.

¹³⁴ *Ibid.*, 39.

¹³⁵ *Ibid.*, 41.

¹³⁶ *Ibid.*, 43.

In this research the specific legal rule had to be placed within the legal context of the legislation of which it was part in order to determine similarities and differences between the Belgian and US legal systems, since the aim was to compare and understand how legislation concerning (online) police infiltration and (online) systemic police observation functions in practice. Sociological interpretation analyzes the social context in which a legal rule is rooted, and also for this research it was considered to be important to situate a legal rule and the decision to introduce that rule within its wider social context.¹³⁷

Chapter 3: Choice of countries

Belgium is part of the European Union and has signed the European Convention on Human Rights (ECHR). As a member state, it has therefore the obligation to protect and guarantee the rights and freedoms set forth by the ECHR. If Belgium wants to make use of investigation techniques such as online police infiltration and online systemic police observation, it is as a consequence under a duty to be in conformity with the rules set out in the ECHR. In the United States, law enforcement has to respect and protect the rights enshrined in the Bill of Rights. Even though the right to privacy, the right to a fair trial and the freedom of speech seem at first hand very similar, there are differences in their meaning in both countries (*Part V*). The countries Belgium and United States have been selected based on their reversed use of the subsidiarity and proportionality principles in criminal investigations. Where in Belgium (and Europe at large) police infiltration can only be employed in cases of serious crime consisting mainly of deep cover long-term operations (*Part III, Chapter 4, §2, a*) and will only be used when all other investigation methods seem to be insufficient (*Part III, Chapter 4, §1, a*), it is in the United States, on top of deep cover long-term national security investigations, often also shortly employed during criminal investigations in order to obtain quick results (*Part III, Chapter 4, §1, b*). Vice versa this is also the case for systemic police observation, which in the United States can only be employed in cases of serious crime and only when all other investigation methods seem to be insufficient (*Part IV, Chapter 1, §3*). It was therefore interesting to see how both countries balance privacy and security based on the most-different approach where two different policy systems are being analyzed and compared.

¹³⁷ *Ibid.*, 44-45.

In Belgium, police infiltration and systemic police observation only received an official legal basis in 2003, and police infiltration's online counterpart only in 2016. It is therefore a relatively recent regulated authority. Online systemic police observation has up until today not been officially regulated in Belgium. Belgium has therefore been selected as country from the European Union for this comparison given that it only very recently granted a legal basis for these investigation techniques. In the United States, these investigation techniques have been employed and developed since the 1920s, and with the digital revolution they have been relatively quickly adapted to and employed in the digital world. When these investigation techniques were re-exported back to Europe after the United States' war on drugs, many European countries based their legal models on the model developed by the United States, which was considered a leading country for the use and development of these techniques and in particular of police infiltration (*Part III, Chapter 1, §1, a*).¹³⁸ By comparing both countries, it was possible to see which approach could be considered more suitable in which situations and some suggestions for both legal systems could be formulated.

Chapter 4: Selection of sources for comparative law research

For Part III (Police infiltration and undercover operations) and Part IV (Systemic police observation and surveillance), legal sources and legislative documents such as legislation and the FBI guidelines were analyzed. This consisted of a textual research which was mainly based on an analysis of the Belgian Code of Criminal Procedure, the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations and the FBI's internal Domestic Investigations and Operations Guide dealing with police infiltration and systemic police observation. For Part V (Privacy, fair trial and freedom of speech), the Belgian Constitution

¹³⁸ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3-4 and 87 and 109; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 31-32; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 2 and 15-20 and 142-146; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 53; L. LUSTGARTEN, "Undercover: police surveillance in comparative perspective: Reviewed", *Public Law* 1997, (575) 576; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 15; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 2 and 12 and 192-195 and 249; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 496 and 508; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 254 and 262-267.

and the European Convention on Human Rights (ECHR) on the one hand, and the US Constitution on the other hand were studied. In order to find this legislation and literature providing more information about it, the online libraries of KU Leuven and Duke University were consulted. More specifically, the topics “(online) police infiltration”, “(online) undercover operations”, “(online) systemic police observation”, “(online) police surveillance”, “the right to privacy, art. 8 ECHR”, “the Fourth Amendment”, “the right to a fair trial, art. 6 ECHR”, “the Fifth Amendment”, “the Fourteenth Amendment”, “the Sixth Amendment”, “the freedom of speech, art. 10 ECHR” and “the First Amendment” were used as keywords in order to conduct the online searches. In order to obtain as many relevant articles as possible, the snowball-method was employed. Based on this method, the references in the consulted articles were checked and the relevant ones were selected in order to continue the research based on those references.¹³⁹ The United States have a common law system and US case law was therefore also analyzed more in detail. The relevant case law of the United States was mainly consulted through the online database of Justia and alternatively also through the online database of Casetext. The relevant case law for Belgium (and Europe) was consulted through the online database of Jura (Wolters Kluwer) and the online database of the European Court of Human Rights named HUDOC. Since ‘the law in the books’ is often further interpreted by the courts and adjusted to the current time and circumstances in which the law has to be applied, the literature and case law, ‘law in action’, should also be discussed in order to provide a complete framework on how the particular legislation is functioning in everyday life. Its main purpose is to provide more information about the interpretation of the Belgian and US legal frameworks, its limitations and its applicability in practice.

Chapter 5: Research quality and limitations

This research was conducted by a Belgian student who already obtained a law degree. Therefore, it might show a more legal than social perspective on some of the selected topics. Given the familiarity with Belgian and European Union law, this might be noticed in how this research was conducted. However, this is the second dissertation in the field of comparative law written by this student and therefore the legal bias of preference for one’s own system

¹³⁹ P. SCHOUKENS *et al.*, *Rechtswetenschappelijk schrijven*, Leuven, Acco, 2012, 34-35.

should be less present, since the conclusion of the previous dissertation already showed that in some situations other national legislation is better formulated and/or better suited a particular situation. The author is therefore aware that the Belgian legal system is not always the best one, albeit the author's more comprehensive knowledge about it, and has an open and positive attitude towards solutions for similar issues that are provided by other legal systems. During previous exchanges in Helsinki, Finland, Venice, Italy and Durham, United States, the author found that an exchange of perspectives on legal issues can lead to better and easier solutions instead of just focusing on one's own legal perspective.

In this dissertation the Belgian and US legal systems have been compared. The author did not have extensive previous knowledge about the US legal system, but the Worldwide Mobility Program granted by Venice International University remedied this obstacle. Thanks to this program, online research could be conducted in the US database and library of Duke University, and, it was possible to ask supervising Professor David Schanzer from Duke University for feedback and more information about the US law part of this dissertation. Professor David Schanzer is a professor of the practice at the Duke University Sanford School of Public Policy, where he teaches courses, conducts research and engages in public dialogue on counterterrorism strategy, counterterrorism law and homeland security.¹⁴⁰ As a graduate of Harvard College and Harvard Law School, he is currently also the director of the Triangle Center on Terrorism and Homeland Security.¹⁴¹ Thanks to his feedback and explanation, it was possible to double check the correctness of the information provided in this dissertation by a US professor who is more familiar with the US legal system.

¹⁴⁰ DUKE, *Faculty David H. Schanzer*, <https://sanford.duke.edu/people/faculty/schanzer-david-h> (consultation 25 April 2021).

¹⁴¹ *Ibid.*

Part III : Police infiltration and undercover operations

Chapter 1: Historical overview of police infiltration

§1. Pre-9/11 undercover operations

a) Pre-9/11 undercover operations in Belgium and Europe

Law enforcement in Europe started with using undercover operations in the political sphere.¹⁴² In Nazi-Germany, Mussolini-Italy, and the Soviet Union, state espionage was frequently used against civilians during the Second World War.¹⁴³ Given this historical use of police infiltration for political purposes, it was for a long time not a widely accepted investigation technique.¹⁴⁴ Only after the 1970s, law enforcement started again to use undercover operations, as a consequence of the expansion of organized crime and drug trafficking.¹⁴⁵ This investigation

¹⁴² J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1012; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 12 and 111; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 125-129; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 2 and 144 and 275; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 52; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 529 and 539; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 254-258 and 265.

¹⁴³ J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1012; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 12 and 111; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 125-129; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 15 and 275; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 52; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 193-194 and 225; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 503 and 529; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 241 and 254-258 and 265.

¹⁴⁴ J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1012; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 111; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 15 and 144 and 275; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 193-194 and 225; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 503; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 265.

¹⁴⁵ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3-4 and 109; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative*

technique was copied by the United States, developed during the ‘war on drugs’, and re-exported back to Europe in its new American version.¹⁴⁶ One of the reasons for this re-exportation was the necessary cooperation between different national law enforcement departments, like those of the EU and the US Drug Enforcement Administration, since drug trafficking and organized crime occur cross-border.¹⁴⁷ Many European Codes of Criminal Procedure were as a consequence modified and legalized some forms of undercover operations in drug trafficking and money laundering cases.¹⁴⁸ Also in Belgium an increase in the use of undercover operations and changes in law and policy took place, which were influenced by the evolutions in the United States.¹⁴⁹ This led to many undercover operations where drugs were

methods in Europe, Aldershot, Ashgate, 1998, 9 and 113; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 31-32; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 12-20 and 144-145; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 52; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 2; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 508; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240-241 and 254 and 262-265.

¹⁴⁶ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 109; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 31-32; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 2 and 15 and 142-144; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 53; L. LUSTGARTEN, “Undercover: police surveillance in comparative perspective: Reviewed”, *Public Law* 1997, (575) 576; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 15; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 2 and 12 and 192-193; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 254 and 262-265.

¹⁴⁷ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3-4 and 92 and 109; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 126; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 31-32; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 145-146; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 15; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 12 and 192-193 and 249; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 262-267.

¹⁴⁸ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3-4 and 87; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 31-32; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 20 and 145-146; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 12 and 192-195 and 249; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 496 and 508; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 254 and 262-267.

¹⁴⁹ S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 113; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 20 and 147; L. LUSTGARTEN, “Undercover: police

purchased by state officials in order to arrest suspects.¹⁵⁰ In 1979, the François scandal had an impact on the organization of law enforcement in Belgium.¹⁵¹ Officer François was the head of a police department that was illegally storing cocaine in order to sell it, and cover up their debt which was a result of a previous attempt to buy drugs that had gone wrong.¹⁵² During that operation officer François had paid for the drugs, but he had never received them.¹⁵³ When he was trying to sell the stored cocaine in order to make money and cover up the losses he had made, his buyer turned out to be a Dutch undercover agent...¹⁵⁴ Only recently after the 1990s, police infiltration regained its legitimacy, since it was more strictly regulated and it is now recognized as an acceptable investigation technique, as long as it takes certain privacy concerns and conditions into account (*Part III, Chapter 2, §1*).¹⁵⁵ A new protective requirement for allowing undercover operations was also introduced with the condition of obtaining a warrant prior to the investigation (*Part III, Chapter 2, §1*).¹⁵⁶

surveillance in comparative perspective: Reviewed”, *Public Law* 1997, (575) 576; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 12 and 194-195.

¹⁵⁰ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3-4 and 109; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 31-32; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 12-15 and 144; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 52-53; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 2 and 192-193; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 241 and 254 and 262-265.

¹⁵¹ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 55; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 114; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 127; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 20 and 150; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 54; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 232.

¹⁵² C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 47-51; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 54.

¹⁵³ *Ibid.*

¹⁵⁴ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 51 and 140; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 54.

¹⁵⁵ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 193-194 and 225; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 265.

¹⁵⁶ J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 257.

Organized crime and drug trafficking have in Europe moreover the advantage of the four freedoms, namely the free movement of goods, persons, capital and services throughout the Schengen-area.¹⁵⁷ Criminal organizations can therefore operate relatively easy on a large and transnational scale.¹⁵⁸ The founders of the Schengen-area were well-aware of that and launched therefore the Convention implementing the Schengen Agreement in 1990.¹⁵⁹ Its aim was to strengthen the fight against cross-border organized crime through the expansion of cross-border authorities of the national police.¹⁶⁰ Police authorities from the contracting states have the possibility of cross-border surveillance, can continue a hot pursuit in the territory of another

¹⁵⁷ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 143; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 4.

¹⁵⁸ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 143; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-240; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 3-4 and 14.

¹⁵⁹ Title III: Police and Security, Chapter 1: Police cooperation & Chapter 2: Mutual assistance in criminal matters of The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *Official Journal L 239, 22/09/2000 P. 0019 – 0062*; A. CUNHA, M. SILVA and R. FREDERICO, *The borders of Schengen*, Brussels, P.I.E. Peter Lang, 2015, 9-10; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 143; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 128; C. FIJNAUT, “The Schengen Treaties and European Police Co-operation”, *European Journal of Crime, Criminal Law and Criminal Justice* 1993, Vol.1(1), (37) 37; C. FIJNAUT, *Een vreedzame revolutie*, Mortsels, Intersentia, 2018, 154-160; C.B. SIO-LOPEZ, “Dialogues beyond the ‘Fortress Europe’: Tracing back the genesis and evolution of the ‘free circulation of persons’ concept through EP Schengen Area debates, 1985-2015” in A. CUNHA, M. SILVA and R. FREDERICO, *The borders of Schengen*, Brussels, P.I.E. Peter Lang, 2015, (32) 36-42; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 4; K. TEMMERMAN, *Terreurbestrijding in België en Europa: de interactie tussen inlichtingendiensten, politie en justitie*, Antwerp, Maklu, 2007, 151; D. ZIMMERMANN, “The European Union and Post-9/11 Counterterrorism: A Reappraisal”, *Studies in Conflict & Terrorism* 2006, Vol.29(2), (123) 125.

¹⁶⁰ Title III: Police and Security, Chapter 1: Police cooperation of The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *Official Journal L 239, 22/09/2000 P. 0019 – 0062*; A. CUNHA, M. SILVA and R. FREDERICO, *The borders of Schengen*, Brussels, P.I.E. Peter Lang, 2015, 9-10; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 143; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 128; C. FIJNAUT, “The Schengen Treaties and European Police Co-operation”, *European Journal of Crime, Criminal Law and Criminal Justice* 1993, Vol.1(1), (37) 37; C. FIJNAUT, *Een vreedzame revolutie*, Mortsels, Intersentia, 2018, 154-160; C.B. SIO-LOPEZ, “Dialogues beyond the ‘Fortress Europe’: Tracing back the genesis and evolution of the ‘free circulation of persons’ concept through EP Schengen Area debates, 1985-2015” in A. CUNHA, M. SILVA and R. FREDERICO, *The borders of Schengen*, Brussels, P.I.E. Peter Lang, 2015, (32) 36-42; T. SPAPENS, E. KOLTHOFF and W. STOL, “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), (1) 4; K. TEMMERMAN, *Terreurbestrijding in België en Europa: de interactie tussen inlichtingendiensten, politie en justitie*, Antwerp, Maklu, 2007, 151; D. ZIMMERMANN, “The European Union and Post-9/11 Counterterrorism: A Reappraisal”, *Studies in Conflict & Terrorism* 2006, Vol.29(2), (123) 125.

contracting state and can assist each other for the purposes of preventing and detecting criminal offenses.¹⁶¹

b) Pre-9/11 undercover operations in the United States

Until the beginning of the 20th century, there were no federal investigation agencies conducting undercover operations in the United States.¹⁶² The population was reluctant towards introducing a centralized police power, since during the United States' historical struggle for independence this was associated with informants and spies.¹⁶³ This changed in 1908, with the creation of the Federal Bureau of Investigation (FBI) as a reaction to the increasing crime in the rapidly grown cities.¹⁶⁴ In the 1920s and 1930s, the FBI started with undercover operations in the political sphere, mainly focusing on the fight against espionage and sabotage by communist and fascist organizations.¹⁶⁵ Ever since, the use of undercover agents has been very popular and largely employed in the United States, mainly in criminal investigations (*Part III, Chapter 4, §1, b*).¹⁶⁶

¹⁶¹ Art. 39-41 of The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *Official Journal L 239, 22/09/2000 P. 0019 – 0062*.

¹⁶² C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 142; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 52.

¹⁶³ C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 10; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 52; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 195.

¹⁶⁴ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 136; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 11; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 52; R. ROIPHE, "The Serpent Beguiled Me: A History of the Entrapment Defense", *Seton Hall Law Review* 2003, Vol.33(2), (257) 268; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 527; U.S. DEPARTMENT OF JUSTICE, *FBI: A brief history*, <https://www.fbi.gov/history/brief-history> (consultation 12 November 2020).

¹⁶⁵ J.C. CARLSON, "The Act Requirement and the Foundations of the Entrapment Defense", *Virginia Law Review* 1987, Vol.73(6), (1011) 1012; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 11-12; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 52; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 166.

¹⁶⁶ D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 210; O.S. BURN, "Abscam Ethics: Moral Issues And Deception In Law Enforcement edited by Gerald M. Caplan", *Journal of Criminal Justice* 1984, Vol.12(1), (93) 93; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 53; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 11-13; C. FIJNAUT, "De exfiltratie van verdachte en veroordeelde criminelen", *Justitiële verkenningen* 2012, Vol.38(3), (68) 73; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 246; G.T. MARX, "The New Police Undercover Work", *Journal of*

With the war on drugs, the arrest rate for drug cases where undercover operations were employed, increased from 44 to 339 per 100,000 population between 1966 and 1974.¹⁶⁷ Besides drug cases, undercover operations were also used in cases concerning prostitution, selling and/or buying of stolen goods, pornography, burglary, street crime, organized crime and corruption.¹⁶⁸ In the 1970s however, the ABSCAM case caused a national scandal.¹⁶⁹ The case originally started as an investigation into stolen art and securities with the main aim of recovering stolen art, but given its unlimited geographical, personal and criminal scope, it turned into a political corruption case.¹⁷⁰ ABSCAM was an undercover company set up by the FBI, where undercover agents pretending to be wealthy sheiks were trying to invest their so-called oil money in valuable (stolen) art.¹⁷¹ This was successful and soon the undercover company developed into an investment company that started operating on a larger scale and also tried to arrange asylum in the United States for these so-called sheiks.¹⁷² When they met with Angelo Errichetti, a state senator with influence in state politics, he offered them the grant

Contemporary Ethnography 1980, Vol.8(4), (399) 400; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 165; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-241.

¹⁶⁷ G.T. MARX, "The New Police Undercover Work", *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 400.

¹⁶⁸ G.T. MARX, "The New Police Undercover Work", *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 401-410; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 166-168.

¹⁶⁹ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 747; B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 153-154; O.S. BURN, "Abscam Ethics: Moral Issues And Deception In Law Enforcement edited by Gerald M. Caplan", *Journal of Criminal Justice* 1984, Vol.12(1), (93) 93; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 64; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 224; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1565-1566; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 188; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 53; S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 29; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 9-10 and 131-132; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 511; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 245.

¹⁷⁰ C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 224.

¹⁷¹ M. RAY, *ABSCAM United States history*, <https://www.britannica.com/topic/Abscam> (consultation 19 November 2020); U.S. DEPARTMENT OF JUSTICE, *ABSCAM*, <https://www.fbi.gov/history/famous-cases/abscam> (consultation 19 November 2020).

¹⁷² G. DWORKIN, "The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime", *Law and Philosophy* 1985, Vol.4(1), (17) 35; M. RAY, *ABSCAM United States history*, <https://www.britannica.com/topic/Abscam> (consultation 19 November 2020); U.S. DEPARTMENT OF JUSTICE, *ABSCAM*, <https://www.fbi.gov/history/famous-cases/abscam> (consultation 19 November 2020).

and approval of a casino gaming license in return for \$400,000.¹⁷³ He also provided them with a list of other politicians who according to him could be susceptible to bribes.¹⁷⁴ As a consequence, the undercover sheiks tried to bribe different members of Congress, even though no concrete suspicion against these members existed, except for the suggestion made by Angelo Errichetti.¹⁷⁵ The sheiks, played by FBI undercover agent Anthony Amoroso and informant Melvin Weinberg, were trying to purchase political influence of the Congressmen for their so-called immigration and investment problems.¹⁷⁶ When they obtained help from some of the members of Congress, they offered various gifts in return which were used afterwards as proof of bribery.¹⁷⁷ Even though this investigation technique could be considered as entrapment (*Part III, Chapter 4, §3, b*)), the Court of Appeals for the Second Circuit upheld the convictions of numerous politicians in this case.¹⁷⁸ In the aftermath of this scandal, some members of Congress wanted to adopt “The Undercover Operations Act”, but they did not succeed.¹⁷⁹ This Act would have “amended the Federal criminal code to authorize the Attorney General to allow law

¹⁷³ *Ibid.*

¹⁷⁴ *Ibid.*

¹⁷⁵ United States v. Kelly, 539 F.Supp. 363 (D.D.C. 1982); B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 747; O.S. BURN, “Abscam Ethics: Moral Issues And Deception In Law Enforcement edited by Gerald M. Caplan”, *Journal of Criminal Justice* 1984, Vol.12(1), (93) 93; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 224; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1565-1576 and 1584; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 188; E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 53; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 29; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 9-10 and 131-132; M. RAY, *ABSCAM United States history*, <https://www.britannica.com/topic/Abscam> (consultation 19 November 2020); J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 511; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 245.

¹⁷⁶ United States v. Kelly, 539 F.Supp. 363 (D.D.C. 1982); J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1061; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 224; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1571-1575; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 188; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 29.

¹⁷⁷ United States v. Kelly, 539 F.Supp. 363 (D.D.C. 1982); C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 224; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1571-1575; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 188.

¹⁷⁸ United States v. Myers, 527 F.Supp. 1206 (E.D.N.Y. 1981); M. RAY, *ABSCAM United States history*, <https://www.britannica.com/topic/Abscam> (consultation 19 November 2020).

¹⁷⁹ E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 54; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 511.

enforcement components of the Department of Justice to conduct undercover operations”. It would have “required the Attorney General to issue, maintain and enforce guidelines governing undercover operations, which” should have “included: (1) the procedures to be followed to initiate, extend or terminate undercover operations; (2) the standards to be employed in such operations; and (3) the functions, powers and composition of the Undercover Operations Review Committee”. Further, it would have “prescribed limitations on undercover operations, created standards for establishing the targets of investigations and shifted the tort liability for negligent acts committed by government agents during the course of an undercover operation from the agent to the Federal government”. Finally, this Act would have “required the Attorney General to report annually to the Judiciary Committees of the House and of the Senate on all undercover operations and established a statutory entrapment defense”.¹⁸⁰ As a reaction to and alternative for the failure to enact this Act, the Department of Justice formulated some guidelines for situations in which FBI undercover operations are allowed (*Part III, Chapter 2, §2*).¹⁸¹

c) Pre-9/11 undercover operations compared

The pre-9/11 historical overview of police infiltration in Belgium and the United States shows many similarities. In both countries, it was first employed in the political sphere in order to fight against state espionage. The use of informants and spies led however to the unpopularity of this investigation technique and reluctance by the public to its use. A few decades later, the expansion of organized crime and drug trafficking required a new response and law enforcement decided to re-introduce the investigation technique of police infiltration. This technique became rapidly very popular and widely used in criminal investigations. Due to its popularity and the fact that it was only modestly regulated, the risk for scandals increased. In Belgium as well as in the United States scandals occurred, and this led to a more strictly regulated framework for the use of the investigation technique of police infiltration, which included conditions that need to be fulfilled prior and during the investigation, and, privacy concerns that need to be taken into account.

¹⁸⁰ Undercover Operations Act: Hearing Before the S. Subcomm. on Criminal Law of the S. Comm. on the Judiciary, 98th Cong. 8 (1984), <https://www.congress.gov/bill/98th-congress/senate-bill/804> (consultation 13 December 2020).

¹⁸¹ E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 54.

§2. Post-9/11 undercover operations

a) Post-9/11 undercover operations in Belgium and Europe

After the terrorist attacks in New York on September 11, 2001, antiterrorism legislation was enacted with unprecedented speed.¹⁸² Until that time, it was in many European countries not possible for law enforcement to conduct undercover operations against suspected terrorists, since only the intelligence agencies had this authority.¹⁸³ After the attacks of 9/11, law enforcement was granted the authority to infiltrate and prosecute extremist organizations founded on religious beliefs or that planned terrorist attacks abroad.¹⁸⁴ In some cases, this authority was even expanded to the possibility of accessing personal data maintained by banks, airlines or telecommunication companies.¹⁸⁵ The main concern about this expansion of authority is that a risk profile without concrete evidence of wrongdoing became a sufficient ground for conducting an undercover operation and an individual ground of suspicion was no longer required.¹⁸⁶

b) Post-9/11 undercover operations in the United States

Unlike in Europe, US law enforcement has always had the right to use undercover operations against suspected terrorists.¹⁸⁷ The Patriot Act allowed information sharing between intelligence agencies and law enforcement, which was up until then kept largely separate for national security investigations.¹⁸⁸ After 2001, this was further extended by allowing FBI agents

¹⁸² J. AUVRET-FINCK, *L'Union européenne et la lutte contre le terrorisme*, Brussels, Larcier, 2010, 8; W. BLOSS, "Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects", *Surveillance & Society* 2007, Vol.4(3), (208) 210; R. BORKOWSKI, "Kontrteryoryzm i antyteryoryzm (aspekty teoretyczne i praktyczne)", *Bezpieczeństwo. Teoria i Praktyka* 2016, Vol.XXIV(3), (39) 44; T. TURAN, "War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties", *Uluslararası Hukuk ve Politika* 2006, Vol.7, (111) 111-112; S. WERNERT, "L'Union européenne et la lutte contre le terrorisme", *Politique étrangère* 2018, Vol.2, (133) 135; D. ZIMMERMANN, "The European Union and Post-9/11 Counterterrorism: A Reappraisal", *Studies in Conflict & Terrorism* 2006, Vol.29(2), (123) 126-127.

¹⁸³ J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 503 and 521; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 264.

¹⁸⁴ J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 263-265.

¹⁸⁵ *Ibid.*

¹⁸⁶ J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 263.

¹⁸⁷ *Ibid.*

¹⁸⁸ Sealed Case, 310 F.3d 717 (F.I.S.C. 2002); P. ROSENZWEIG, "Civil Liberty and the Response to Terrorism", *Duquesne Law Review* 2004, Vol.42(4), (663) 686-690.

to direct a confidential human source to attend public events to collect intelligence on potential threats or terrorist activities.¹⁸⁹ However, to direct a confidential human source to collect this information, the FBI has to have predication (i.e. information or an allegation of activity that (might) constitute a federal crime or threat to national security).¹⁹⁰ This confidential human source can be anyone whom the FBI may direct to attend, observe and provide information about an individual or organization at a public event that is under suspicion.¹⁹¹ These confidential human sources can surveil churches and mosques if there is an individual or organization under suspicion, regardless of their religious beliefs, since the latter is qualified as a sensitive investigative matter.¹⁹² A sensitive investigative matter involves according to the

¹⁸⁹ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 16 Undisclosed participation*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,16/1-16/18>; P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 702-703; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 527 and 536; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 264; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

¹⁹⁰ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 6.5 Predication*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,6/3>.

¹⁹¹ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 16 Undisclosed participation*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,16/1>; *Socialist Workers Party v. Attorney General*, 419 U.S. 1314 (1974).

¹⁹² U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 5.7 Sensitive Investigative Matters in Assessments and Sensitive Potential CHS or Sensitive Characteristic Designations in Type 5 Assessments*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,5/33>; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 16 Undisclosed participation*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,16/1-16/18>; *Socialist Workers Party v. Attorney General*, 419 U.S. 1314 (1974); P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 703; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 533-536; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 264; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 11 and 47; M.A. WASSERMAN, “First

FBI's internal Domestic Investigations and Operations Guide (DIOG) "the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which (...) should be brought to the attention of the FBI Head Quarters and other Department Of Justice officials".¹⁹³ In these 'sensitive investigative' situations a higher level of approval and more oversight are required, since the FBI wants to make sure not to infringe people's civil rights protected by the Bill of Rights.¹⁹⁴

c) Post-9/11 undercover operations compared

The evolution of the investigation technique of police infiltration in Belgium and in the United States shows also after 9/11 many similarities. First of all, the threshold to initiate an undercover operation was lowered in both countries, making it easier to conduct undercover operations in suspected terrorism investigations. In Belgium and Europe, law enforcement acquired the authority to conduct undercover operations in suspected cases of terrorism. In the United States, the FBI already had this authority, but it was expanded in order to facilitate its use. This expansion has however reduced the rights of (potential) suspects in both countries, given that there are less restrictions to access personal data in suspected cases of terrorism and religious beliefs, even though more strictly regulated with more oversight, may be one of the factors, though not the only one, to initiate an undercover operation.

Amendment limitations on police surveillance: The case of the Muslim surveillance program", *New York University Law Review* 2015, Vol.90(5), (1786) 1787-1793.

¹⁹³ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 5.7 Sensitive Investigative Matters in Assessments and Sensitive Potential CHS or Sensitive Characteristic Designations in Type 5 Assessments*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 5/33; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 10 Sensitive Investigative matter and Sensitive Operations Review Committee*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 10/1.

¹⁹⁴ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 16 Undisclosed participation*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operation%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 16/1-16/18.

Chapter 2: Legal framework on police infiltration

§1. Belgian legal framework on police infiltration

The enactment of official legislation regulating police infiltration only happened in Belgium in 2003.¹⁹⁵ In the meantime, case law served as the first regulation of this investigation technique.¹⁹⁶ In 1984, the Court of Appeal in Brussels was confronted with a pseudo-buy of drugs case.¹⁹⁷ In its decision it stated the conditions for lawful police infiltration, which have consequently been used by law enforcement and courts, and which were confirmed in the official legislation enacted in 2003, namely:

- The suspect may not be entrapped, the undercover agent may not ‘implant’ the intention of committing a crime into the suspect’s mind;
- This investigation technique may only be used for serious crime (proportionality requirement);
- The undercover agent may not commit crimes, except in the case of an emergency;
- The undercover agent’s superiors should supervise and conscientiously control the agent’s actions.¹⁹⁸

Up until 1990, there was no formal regulation of undercover operations in Belgium.¹⁹⁹ The first document regulating police infiltration was a confidential and secret guideline of April 24, 1990

¹⁹⁵ Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 May 2003; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 361; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/11; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134; F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen””, *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, “Cassatie zet nieuwe BOM-bakens uit”, *Juristenkrant* 2008, Vol.180, (5) 5; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61.

¹⁹⁶ Brussels 19 November 1984, *Pas.* 1985, II, 37, *RW* 1984-85, 2563; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 114-115; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137.

¹⁹⁷ *Ibid.*

¹⁹⁸ *Ibid.*

¹⁹⁹ MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 4; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 55 and 109; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 112-119; F. HUTSEBAUT

and remained for a long time the only regulatory basis, which was followed and adapted by the secret guideline of March 5, 1992.²⁰⁰ The guidelines defined police infiltration as “situations where a police officer using a cover identity contacts a group of persons who participate in serious criminal activities or who – on the basis of objective data – are supposed (to be about) to commit serious crimes, and tries to enter into extended interaction with its members”.²⁰¹ They contained the requirements of proportionality (serious crime and/or organized by a gang), subsidiarity (the evidence necessary cannot be collected by other investigative methods), prior authorization by a superior for minor crimes being committed by the undercover agent and respect for human rights and a fair trial.²⁰² These guidelines were however not in conformity with art. 8 of the European Convention on Human Rights (ECHR), which requires a formal source of law as legal basis for interference with the right to privacy, and needed therefore an official legal replacement which only happened in 2003.²⁰³ Until then, the guidelines remained to serve as a regulatory basis. In addition to this, the Belgian courts ruled in the 1990s that if provocation occurred during an undercover operation, the prosecution had to quash the case.²⁰⁴

and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 7.

²⁰⁰ Ministeriële Omzendbrief van 24 april 1990 betreffende de bijzondere opsporingstechnieken om de zware of georganiseerde criminaliteit te bestrijden, *Parl.doc.* nr. 1-447/4 A; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 4; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 55-56 and 110; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 112-119 and 134; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 152; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 7.

²⁰¹ Tweede tussentijds verslag van de parlementaire commissie van onderzoek naar de georganiseerde criminaliteit in België over De impact van de bestrijding van de georganiseerde criminaliteit, onder meer door het gebruik van bijzondere opsporingsmethoden, op de organisatie van de politiediensten en het openbaar ministerie, *Parl.doc.* nr. 1-326/8, 13; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 121; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 152.

²⁰² Ministeriële Omzendbrief van 24 april 1990 betreffende de bijzondere opsporingstechnieken om de zware of georganiseerde criminaliteit te bestrijden, *Parl.doc.* nr. 1-447/4 A; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 119.

²⁰³ S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 117 and 132; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

²⁰⁴ Art. 30 wet van 17 april 1878 houdende de Voorafgaande Titel van het Wetboek van Strafvordering (V.T.Sv.), *BS* 25 April 1878; Bergen 5 May 1992, *JLMB* 1993, 12, *Rev.dr.pén.* 1992, 890; Brussels 7 September 1994, *JLMB* 1994, 1135, *Journ. proc.* 1994, Vol.268, 25, *Pas.* 1993, II, 112, *Rev.dr.pén.* 1995, 419; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 125; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 12; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137.

The first official legal framework for Special Investigation Methods (in Dutch: Bijzondere OpsporingsMethoden; BOM) was introduced by the law of January 6, 2003.²⁰⁵ Special Investigation Methods (SIMs) are considered to consist of the investigation techniques of systemic police observation, police informants and police and civilian infiltration.²⁰⁶ These SIMs were introduced in the Belgian Code of Criminal Procedure (in Dutch: Wetboek van Strafvordering; Sv.).²⁰⁷ Police infiltration is defined in art. 47octies Sv. as “a police officer (the infiltrator) who is, under a fictitious identity, in long-lasting contact with one or more persons of whom there are serious indications that they are or could be committing criminal offenses, within a criminal organization (punishable with a prison sentence of at least three years) or for which ordering a wiretap is permitted”.²⁰⁸ Police infiltration is mostly used as a proactive SIM

²⁰⁵ Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 May 2003; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 361; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/11; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134; F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen””, *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, “Cassatie zet nieuwe BOM-bakens uit”, *Juristenkrant* 2008, Vol.180, (5) 5; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61.

²⁰⁶ Art. 47ter, §1 Wetboek van Strafvordering (Sv.), *BS* 27 November 1808; MvT bij het wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/001, 7-8; Arbitragehof 21 December 2004, nr. 202/2004, A.A. 2004, Vol.5, 2283, *BS* 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106; Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 361; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/01; CRIMINIS WOORDENLIJST, *Bijzondere opsporingsmethoden*, <https://joachimmeese.be/criminis/woordenlijst/bijzondere-opsporingsmethoden/> (consultation 10 October 2020); J. DELMULLE, “Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.”, *T.Strafr.* 2005, Vol.3, (230) 230-231; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 8; JURECA, *Bijzondere opsporingsmethoden (BOM)*, <https://www.jureca.be/verklaring/bijzondere-opsporingsmethoden-bom> (consultation 10 October 2020); B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 64 and 205; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61.

²⁰⁷ H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 363; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147-1150.

²⁰⁸ Art. 47octies Sv., *BS* 27 November 1808; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 217 and 224; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 261; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1149-1150; B. TILLEMANN, E.

in the early planning stages of a criminal offense, whereas other, reactive, investigation methods tend to be used only after the criminal offense has already occurred.²⁰⁹ The Crown prosecutor or the investigating judge has to issue a warrant authorizing undercover operations prior to their initiation.²¹⁰ In case law enforcement wants to make use of these SIMs, they have to take four principles into account; subsidiarity, proportionality, the prohibition of provocation, and the prohibition to commit criminal offenses (*Part III, Chapter 4*).²¹¹

According to BERKMOES, SIMs can be characterized by their possibility to infringe fundamental rights and freedoms, secrecy, their possibility to infringe the regular way of evidence gathering and their possibility to endanger the right to a fair trial.²¹² In order to safely conduct an investigation where SIMs are being used, it is necessary to modify the right to

DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 205; P. VANWALLEGHEM, “Infiltratie mag ook om verdachte te arresteren”, *De Juristenkrant* 2014, Vol.4, (2) 2; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264.

²⁰⁹ H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/26 and 216/35; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 3 and 88-89; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 8-9; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 129; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 163; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 9; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1135-1136; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242; G. PATAKI, “Conducting Reactive and Proactive Internet Investigations” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (253) 253-256; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1114-1119; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2865-2866; S. SINGLETON, “Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques”, *Ohio Northern University Law Review* 2004, Vol.30(3), (417) 417; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390.

²¹⁰ Art. 47octies Sv., BS 27 November 1808; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

²¹¹ Art. 30 V.T.Sv., BS 25 April 1878; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 30-33; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/02 and 216/58 and 216/71; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 8-12; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137-1138.

²¹² MvT bij het wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/001, 8; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/20.

confront and cross-examine the counterparty, which is part of the right to a fair trial.²¹³ When SIMs are being employed, two investigation files are being created, one public and one confidential.²¹⁴ The confidential file, which consists of the techniques that were used and the

²¹³ ECtHR 16 February 2000, nr. 27052/95, Jasper/United Kingdom, *Juristenkrant* 2000, Vol.5, 4, *RW* 2002-03, Vol.6, 233; ECtHR 23 May 2017, nr. 67496/10, 52936/12, Van Wesenbeeck/Belgium, *JLMB* 2017, Vol.23, 1079, *RW* 2017-18, Vol.38, 1514; Arbitragehof 21 December 2004, nr. 202/2004, A.A. 2004, Vol.5, 2283, *BS* 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106; GwH 19 July 2007, nr. 105/2007, *BS* 13 August 2007, 42941, *JLMB* 2008, Vol.14, 598, *NJW* 2007, Vol.168, 695, *RABG* 2008, Vol.1, 3, *Rev.dr.pén.* 2007, Vol.12, 1118, *RW* 2007-08, Vol.2, 85, *RW* 2007-08, Vol.43, 1811, *TBP* 2008, Vol.5, 286, *TGR-TWVR* 2008, Vol.1, 55, *T.Strafr.* 2007, Vol.4, 254; GwH 30 September 2009 (preliminary question), nr. 150/2009, *BS* 29 December 2009, 82208; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 10 February 2015, *Arr.Cass.* 2015, Vol.2, 244, *Pas.* 2015, Vol.2, 310, *T.Strafr.* 2015, Vol.3, 139; Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170; H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 29; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 378-380; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10 and 216/39-216/45; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 260; CRIMINIS WOORDENLIJST, *Bijzondere opsporingsmethoden*, <https://joachimmeese.be/criminis/woordenlijst/bijzondere-opsporingsmethoden/> (consultation 10 October 2020); J. DELMULLE, “Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.”, *T.Strafr.* 2005, Vol.3, (230) 230-233; S. GUENTER and F. SCHUERMANS, “Enkele recente Antigooon-evoluties en de toepassing ervan op een onregelmatige observatie en/of infiltratie”, *T.Strafr.* 2013, Vol.5, (329) 334; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 11; JURECA, *Bijzondere opsporingsmethoden (BOM)*, <https://www.jureca.be/verklaring/bijzondere-opsporingsmethoden-bom> (consultation 10 October 2020); F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen’”, *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, “Cassatie zet nieuwe BOM-bakens uit”, *Juristenkrant* 2008, Vol.180, (5) 5; A. THIENPONT, “Nieuwe BOM-wet legt bom onder fundamentele rechten en vrijheden”, *Juristenkrant* 2006, Vol.1, (2) 2; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 63.

²¹⁴ Art. 47septies and 47novies Sv., *BS* 27 November 1808; art. 235ter-235quater Sv., *BS* 19 December 1808; ECtHR 16 February 2000, nr. 27052/95, Jasper/United Kingdom, *Juristenkrant* 2000, Vol.5, 4, *RW* 2002-03, Vol.6, 233; Arbitragehof 21 December 2004, nr. 202/2004, A.A. 2004, Vol.5, 2283, *BS* 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106; GwH 19 July 2007, nr. 105/2007, *BS* 13 August 2007, 42941, *JLMB* 2008, Vol.14, 598, *NJW* 2007, Vol.168, 695, *RABG* 2008, Vol.1, 3, *Rev.dr.pén.* 2007, Vol.12, 1118, *RW* 2007-08, Vol.2, 85, *RW* 2007-08, Vol.43, 1811, *TBP* 2008, Vol.5, 286, *TGR-TWVR* 2008, Vol.1, 55, *T.Strafr.* 2007, Vol.4, 254; GwH 30 September 2009 (preliminary question), nr. 150/2009, *BS* 29 December 2009, 82208; GwH 3 December 2009, nr. 196/2009, *A.GrwH* 2009, Vol.5, 2693, *BS* 4 January 2010, 2, *RW* 2009-10, Vol.19, 813, *RW* 2010-11, Vol.10, 420; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; Cass. 31 October 2006, *Vigiles* 2007, Vol.3, 93; Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 10 February 2015, *Arr.Cass.* 2015, Vol.2, 244, *Pas.* 2015, Vol.2, 310, *T.Strafr.* 2015, Vol.3, 139; Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170; H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 29; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 378-379; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01)

identity of the undercover agents, cannot be accessed by the parties in a case or by the judge, but only by the Indictment Chamber.²¹⁵ The parties can submit their questions and concerns to

216/01-216/07 and 216/21; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 260; CRIMINIS WOORDENLIJST, *Bijzondere opsporingsmethoden*, <https://joachimmeese.be/criminis/woordenlijst/bijzondere-opsporingsmethoden/> (consultation 10 October 2020); J. DELMULLE, “Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.”, *T.Strafr.* 2005, Vol.3, (230) 230-233; S. GUENTER and F. SCHUERMANS, “Enkele recente Antigoon-evoluties en de toepassing ervan op een onregelmatige observatie en/of infiltratie”, *T.Strafr.* 2013, Vol.5, (329) 334; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 10; JURECA, *Bijzondere opsporingsmethoden (BOM)*, <https://www.jureca.be/verklaring/bijzondere-opsporingsmethoden-bom> (consultation 10 October 2020); J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137-1143; F. SCHUERMANS and H. BERKMOES, “De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden”, *T.Strafr.* 2006, Vol.2, (65) 68-69; F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen””, *Juristenkrant* 2008, Vol.165, (8) 8; A. THIENPONT, “Nieuwe BOM-wet legt bom onder fundamentele rechten en vrijheden”, *Juristenkrant* 2006, Vol.1, (2) 2; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61-62; P. VANWALLEGHEM, “Infiltratie mag ook om verdachte te arresteren”, *De Juristenkrant* 2014, Vol.4, (2) 2.

²¹⁵ Art. 189ter Sv., *BS* 29 November 1808; art. 235ter-235quater Sv., *BS* 19 December 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomcommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 74; ECtHR 16 February 2000, nr. 27052/95, Jasper/United Kingdom, *Juristenkrant* 2000, Vol.5, 4, *RW* 2002-03, Vol.6, 233; Arbitragehof 21 December 2004, nr. 202/2004, A.A. 2004, Vol.5, 2283, *BS* 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106; GwH 19 July 2007, nr. 105/2007, *BS* 13 August 2007, 42941, *JLMB* 2008, Vol.14, 598, *NJW* 2007, Vol.168, 695, *RABG* 2008, Vol.1, 3, *Rev.dr.pén.* 2007, Vol.12, 1118, *RW* 2007-08, Vol.2, 85, *RW* 2007-08, Vol.43, 1811, *TBP* 2008, Vol.5, 286, *TGR-TWVR* 2008, Vol.1, 55, *T.Strafr.* 2007, Vol.4, 254; GwH 31 July 2008 (preliminary question), nr. 111/2008, A.*GrwH* 2008, Vol.3, 1809, *BS* 15 September 2008, 47853, *Juristenkrant* 2008, Vol.174, 3, *Rev.dr.pén.* 2009, Vol.1, 65, *RW* 2008-09, Vol.1, 44, *RW* 2008-09, Vol.9, 360; GwH 30 September 2009 (preliminary question), nr. 150/2009, *BS* 29 December 2009, 82208; GwH 3 December 2009, nr. 196/2009, A.*GrwH* 2009, Vol.5, 2693, *BS* 4 January 2010, 2, *RW* 2009-10, Vol.19, 813, *RW* 2010-11, Vol.10, 420; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; Cass. 31 October 2006, *Arr.Cass.* 2006, Vol.10, 2198, *Pas.* 2006, Vol.11, 2235, *Rev.dr.pén.* 2007, Vol.6, 616; Cass. 31 October 2006, *Vigiles* 2007, Vol.3, 93; Cass. 31 October 2006, *NC* 2007, Vol.1, 61; Cass. 14 October 2008, *Arr.Cass.* 2008, Vol.10, 2226, *Juristenkrant* 2008, Vol.180, 5, *JT* 2008, Vol.6333, 755, *NC* 2008, Vol.6, 458, *Pas.* 2008, Vol.10, 2215, *Rev.dr.pén.* 2009, Vol.1, 92, *TBP* 2009, Vol.8, 492-493; Cass. 16 February 2010, *Arr.Cass.* 2010, Vol.2, 460, *NC* 2010, Vol.2, 127, *Pas.* 2010, Vol.2, 483, *P&B* 2010, Vol.6, 212, *T.Strafr.* 2011, Vol.3, 195; Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145; Cass. 23 November 2010, *Arr.Cass.* 2010, Vol.11, 2823, *Pas.* 2010, Vol.11, 3011, *T.Strafr.* 2011, Vol.3, 198; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 10 February 2015, *Arr.Cass.* 2015, Vol.2, 244, *Pas.* 2015, Vol.2, 310, *T.Strafr.* 2015, Vol.3, 139; Cass. 25 March 2015, *Arr.Cass.* 2015, Vol.3, 830, *NC* 2017, Vol.5, 490, *Pas.* 2015, Vol.3, 811, *Rev.dr.pén.* 2015, Vol.9-10, 979; Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170; KI Ghent 6 December 2004, *RABG* 2005, Vol.13, 1215, *T.Strafr.* 2005, Vol.3, 227; H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 30-33; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 378-379; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/04-216/07 and 216/17 and 216/35-216/54; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 260; CRIMINIS WOORDENLIJST, *Bijzondere opsporingsmethoden*, <https://joachimmeese.be/criminis/woordenlijst/bijzondere-opsporingsmethoden/> (consultation 10 October 2020); J. DELMULLE, “Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en

the Indictment Chamber, which will review them together with the confidential file.²¹⁶ During this review, the Indictment Chamber will only check the SIM's regularity and whether it complies with its conditions.²¹⁷ In this way, the Belgian legislator found a compromise between

onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.", *T.Strafr.* 2005, Vol.3, (230) 230-234; S. GUENTER and F. SCHUERMANS, "Enkele recente Antigoon-evoluties en de toepassing ervan op een onregelmatige observatie en/of infiltratie", *T.Strafr.* 2013, Vol.5, (329) 334; JURECA, *Bijzondere opsporingsmethoden (BOM)*, <https://www.jureca.be/verklaring/bijzondere-opsporingsmethoden-bom> (consultation 10 October 2020); F. SCHUERMANS and H. BERKMOES, "De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden", *T.Strafr.* 2006, Vol.2, (65) 68-69; F. SCHUERMANS, "Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen'", *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, "Cassatie zet nieuwe BOM-bakens uit", *Juristenkrant* 2008, Vol.180, (5) 5; F. SCHUERMANS, "De wettigheidscontrole van de observatie en infiltratie", *T.Strafr.* 2015, Vol.1, (27) 27; A. THIENPONT, "Nieuwe BOM-wet legt bom onder fundamentele rechten en vrijheden", *Juristenkrant* 2006, Vol.1, (2) 2; J. VAN GAEVER, "Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden", *T.Strafr.* 2007, Vol.1, (61) 61-64.

²¹⁶ Art. 189ter Sv., *BS* 29 November 1808; art. 235ter-235quater Sv., *BS* 19 December 1808; Arbitragehof 21 December 2004, nr. 202/2004, *A.A.* 2004, Vol.5, 2283, *BS* 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106; GwH 31 July 2008 (preliminary question), nr. 111/2008, *A.GrwH* 2008, Vol.3, 1809, *BS* 15 September 2008, 47853, *Juristenkrant* 2008, Vol.174, 3, *Rev.dr.pén.* 2009, Vol.1, 65, *RW* 2008-09, Vol.1, 44, *RW* 2008-09, Vol.9, 360; GwH 3 December 2009, nr. 196/2009, *A.GrwH* 2009, Vol.5, 2693, *BS* 4 January 2010, 2, *RW* 2009-10, Vol.19, 813, *RW* 2010-11, Vol.10, 420; Cass. 31 October 2006, *Arr.Cass.* 2006, Vol.10, 2198, *Pas.* 2006, Vol.11, 2235, *Rev.dr.pén.* 2007, Vol.6, 616; Cass. 16 February 2010, *Arr.Cass.* 2010, Vol.2, 460, *NC* 2010, Vol.2, 127, *Pas.* 2010, Vol.2, 483, *P&B* 2010, Vol.6, 212, *T.Strafr.* 2011, Vol.3, 195; Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 10 February 2015, *Arr.Cass.* 2015, Vol.2, 244, *Pas.* 2015, Vol.2, 310, *T.Strafr.* 2015, Vol.3, 139; Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 378-379; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/04-216/07 and 216/17 and 216/40-216/54; J. DELMULLE, "Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.", *T.Strafr.* 2005, Vol.3, (230) 230-234; S. GUENTER and F. SCHUERMANS, "Enkele recente Antigoon-evoluties en de toepassing ervan op een onregelmatige observatie en/of infiltratie", *T.Strafr.* 2013, Vol.5, (329) 334; F. SCHUERMANS and H. BERKMOES, "De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden", *T.Strafr.* 2006, Vol.2, (65) 68-69; F. SCHUERMANS, "Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen'", *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, "Cassatie zet nieuwe BOM-bakens uit", *Juristenkrant* 2008, Vol.180, (5) 5; J. VAN GAEVER, "Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden", *T.Strafr.* 2007, Vol.1, (61) 61-63.

²¹⁷ Art. 235ter-235quater Sv., *BS* 19 December 1808; Cass. 16 February 2010, *Arr.Cass.* 2010, Vol.2, 460, *NC* 2010, Vol.2, 127, *Pas.* 2010, Vol.2, 483, *P&B* 2010, Vol.6, 212, *T.Strafr.* 2011, Vol.3, 195; Cass. 14 September 2010, *Arr.Cass.* 2010, Vol.9, 2186, *Pas.* 2010, Vol.9, 2263, *RW* 2011-12, Vol.38, 1670, *TGR-TWVR* 2011, Vol.2, 136, *T.Strafr.* 2011, Vol.3, 196; Cass. 23 November 2010, *Arr.Cass.* 2010, Vol.11, 2823, *Pas.* 2010, Vol.11, 3011, *T.Strafr.* 2011, Vol.3, 198; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/04-216/07 and 216/42-216/47 and 216/54; F. SCHUERMANS and H. BERKMOES, "De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden", *T.Strafr.* 2006, Vol.2, (65) 68-70; F. SCHUERMANS, "De wettigheidscontrole van de observatie en infiltratie", *T.Strafr.* 2015, Vol.1, (27) 27.

the right of the suspect to cross-examine the counterparty and guaranteeing the safety of undercover agents and methods.

§2. US legal framework on police infiltration

For the US legal framework on undercover operations, three levels of regulation will be discussed; firstly, a nationwide level applicable to all law enforcement departments in the United States; secondly, the FBI level; and thirdly, the local level for local law enforcement departments. Given that the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations and the FBI's internal Domestic Investigations and Operations Guide (DIOG) fulfill in the United States more or less the same role for the FBI as the Belgian Code of Criminal Procedure (Sv.) in regulating police infiltration, this comparative law research will mainly focus on the FBI level.

Police infiltration is in the United States still largely unregulated by constitutional criminal procedure and there is no general statute regulating the conditions that are applicable for undercover operations.²¹⁸ However, in the Bill of Rights there are several protections to limit government intrusion and these have to be respected at all times (Part V). Within each (FBI, local,...) procedural framework, it is as a consequence prohibited for law enforcement to violate someone's constitutional rights. Police infiltration can be used for all sorts of crime and is not limited to organized or serious crime.²¹⁹ This investigation technique is often employed to obtain information about groups which are closed to the general public or whose members' identity is not common knowledge.²²⁰ Undercover agents use disguise and deception to become accepted members of these groups in order to learn more about their criminal activities, such as drug trafficking or organized crime.²²¹ The main regulation consists of the entrapment defense (*Part III, Chapter 4, §3, b*)), but this does not take into account the various ways of influencing

²¹⁸ O.S. BURN, "Abscam Ethics: Moral Issues And Deception In Law Enforcement edited by Gerald M. Caplan", *Journal of Criminal Justice* 1984, Vol.12(1), (93) 93; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2865-2867.

²¹⁹ J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 563.

²²⁰ X, "Police infiltration of dissident groups", *The Journal of Criminal Law, Criminology, and Police Science* 1970, Vol.61(2), (181) 181.

²²¹ B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 154; X, "Police infiltration of dissident groups", *The Journal of Criminal Law, Criminology, and Police Science* 1970, Vol.61(2), (181) 181.

that may occur during undercover operations.²²² In the United States, there is no general applicable standard, there is no general requirement for a warrant based on probable cause or reasonable suspicion, in order to initiate an undercover operation and every level has its own regulations.²²³

The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations contain on the federal level some instructions for internal use only.²²⁴ One of the requirements to initiate an FBI undercover operation is the prior approval by the Special Agent in Charge of the FBI office, which must confirm that this investigation technique appears to be effective and will be conducted in a minimally intrusive way.²²⁵ In sensitive circumstances (which are listed exhaustively in the Guidelines), it is additionally required that an Undercover Review Committee approves the proposed undercover operation.²²⁶ The Guidelines define undercover

²²² W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 106; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2865-2868.

²²³ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 162; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 250; S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 33; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 544; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 194; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1121; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 513 and 563; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867.

²²⁴ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>; ATTORNEY GENERAL, *The Attorney General's Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 31; B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756; D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 224-230; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1586; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 176-179; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 511.

²²⁵ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 3-4; D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 229; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 176-179.

²²⁶ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 6-9; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 176-179; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 512.

activities as “any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, or local law enforcement organization working with the FBI”, and an undercover operation as “an investigation involving a series of related undercover activities over a period of time by an undercover employee. For purposes of these Guidelines, a ‘series of related undercover activities’ generally consists of more than three separate contacts by an undercover employee with the individual(s) under investigation. (...) A contact is ‘substantive’ if it is a communication with another person, whether by oral, written, wire, or electronic means, which includes information of investigative interest. Mere incidental contact, e.g. a conversation that establishes an agreed time and location for another meeting, is not a substantive contact within the meaning of these Guidelines”.²²⁷ An undercover employee is further explained as being “any employee of the FBI, or employee of a Federal, state, or local law enforcement agency working under the direction and control of the FBI in a particular investigation, whose relationship with the FBI is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity”.²²⁸ Moreover, it is specifically stated in the FBI’s internal DIOG that FBI employees have to ensure that the constitutional rights of the public will be respected.²²⁹ These guidelines are specific to the FBI and overseen by the Department of Justice on a national level.²³⁰ They do not create any rights and cannot be relied on as a legal basis.²³¹ A procedural violation will as a consequence only constitute a breach of agency policy.²³²

²²⁷ J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 1; OFFICE OF THE ATTORNEY GENERAL, *Undercover and sensitive operations unit, attorney general’s guidelines on FBI undercover operation*, 1992, <https://www.justice.gov/archives/ag/undercover-and-sensitive-operations-unit-attorney-generals-guidelines-fbi-undercover-operations>.

²²⁸ *Ibid.*

²²⁹ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 4 Privacy and Civil Liberties, and Least Intrusive Methods*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 4/1-4/19.

²³⁰ B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756; D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 229-230; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 178-179; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 511.

²³¹ B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756; D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 229-230; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 178-179.

²³² D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 229-230; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of

There are three hierarchical types of investigation according to the FBI's internal DIOG; an assessment (to gather information)²³³, a preliminary investigation (to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security based on any allegation or information indicative of possible criminal activity)²³⁴ and a full investigation (to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security based on an articulable factual basis of possible criminal or national threat activity)²³⁵. These types of investigation are in hierarchical order, meaning that the investigation methods allowed during an assessment are also allowed during a preliminary and full investigation. An undercover operation can only be initiated during a full investigation.²³⁶

Most undercover work in criminal investigations takes place on a local level, therefore the FBI guidelines discussed above are not applicable and rarely used in undercover operations set up by local police departments, which have each their own guidelines regarding undercover operations.²³⁷ These guidelines are however most often only focused on procedural aspects (such as how to recruit undercover agents, the equipment to be used, safety precautions etc.) and only some focus also on so-called 'authorizational' aspects which specify the circumstances in which undercover operations can be employed.²³⁸

Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1586; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 178-179.

²³³ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 5 Assessments*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 5/1-5/38.

²³⁴ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 6 Preliminary Investigations*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 6/1-6/11.

²³⁵ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 7 Full Investigations*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 7/1-7/11.

²³⁶ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 7.9 Authorized Investigative Methods in Full Investigations, U) Undercover operations*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 7/7-7/8.

²³⁷ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 816-817.

²³⁸ *Ibid.*

§3. Legal framework on police infiltration compared

The legal frameworks of Belgium and the United States show some differences. First of all, the investigation technique of police infiltration is in Belgium regulated in legally binding criminal procedural law that is generally applicable to law enforcement. This is not the case in the United States, where there is no general legal framework set up by constitutional criminal procedure, but different frameworks apply to different law enforcement departments. The Attorney General's Guidelines on FBI Undercover Operations and the FBI's internal DIOG form the most important legal framework and are applied by the FBI, mainly in national security investigations. These FBI guidelines are however instructions for internal use only and unless a constitutional right will also be violated, a suspect will not be able to address a violation of these FBI guidelines in his defense. Local law enforcement departments in the United States have at their turn their own guidelines, which they will most often apply during criminal investigations. Secondly, this investigation method may in Belgium only be used in case of serious criminal offenses for which a minimum threshold is set, whereas in the United States a division has to be made between national security investigations (higher threshold) and criminal investigations (lower threshold) (*Part III, Chapter 4, §2*). Thirdly, it is in Belgium only possible to initiate an undercover operation based on prior authorization by the Crown prosecutor or the investigating judge. In the United States on the contrary, there is no general requirement for obtaining prior authorization, but the Attorney General's Guidelines mention that prior approval by the Special Agent in Charge of the FBI office is required for FBI undercover investigations. Fourthly, the Belgian system where two investigation files, a public and a confidential one, are being created, could also be interesting for the United States. This way the suspect's right to a fair trial would only slightly be modified, since he would still have access to the public file containing all non-sensitive information. Only the identity of the undercover agent and the techniques used during the undercover operation would be in the confidential file, which could only be accessed by a particular judge. The suspect could ask this judge to check the regularity of the investigation technique and whether all conditions were fulfilled, without endangering sensitive information.

Besides these differences, the legal frameworks of these countries also show some similarities. In both the Belgian and the FBI definition of this investigation technique, the use of disguise and a fictitious identity is a characterizing element. The contact between the undercover agent and the suspect should moreover be of a long-lasting nature and not merely incidental, with

often an intelligence gathering aim. Finally, the four principles of subsidiarity, proportionality, the prohibition of provocation, and the prohibition to commit criminal offenses stated by Belgian law can also be retrieved in US law and US legislative documents, such as the FBI guidelines. These four principles will be discussed more in detail in Chapter 4 of this Part.

Chapter 3: Legal framework on police infiltration in the digital age

§1. Belgian legal framework on police infiltration in the digital age

The definition of offline police infiltration received its own online version in art. 46*sexies* Sv. and was introduced by the law of December 25, 2016.²³⁹ Online police infiltration is defined as “a police officer who maintains contact, if necessary under a fictitious identity, with one or more persons of whom there are serious indications that they are committing or might commit criminal offenses that are punishable with a prison sentence of minimum one year, and only when this is required by the investigation and no other means appear to be sufficient in order to reveal the truth”.²⁴⁰ According to this article, the Crown prosecutor or investigating judge may issue a warrant to authorize police officers to conduct an online undercover operation.²⁴¹ This

²³⁹ Art. 46*sexies* Sv., BS 27 November 1808; art. 7 wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, BS 17 January 2017; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 9 and 36-45; GwH 6 December 2018, nr. 174/2018, BS 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 362; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/19; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 259-261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390-392 and 400.

²⁴⁰ Art. 46*sexies* Sv., BS 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 36-37; GwH 6 December 2018, nr. 174/2018, BS 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 362; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/58-216/59; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 259-260; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 400-401.

²⁴¹ Art. 46*sexies* Sv., BS 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 37; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 362; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 400-401.

provides law enforcement with the possibility to infiltrate for example social media or to create fake profiles while making use of fake identities.²⁴² They may gain access to initially non-publicly available information on private groups on Facebook, they can try to become ‘friends’ with a suspect in order to gain access to private information posted on his Facebook page or they might start a conversation with the suspect using a false identity.²⁴³ In addition, law enforcement can also contact social media providers and ask for access to a suspect’s private chat messages.²⁴⁴

Even though there are many similarities between off- and online police infiltration, there are also some very important differences. Firstly, the use of a false identity or participation in criminal offenses is not always necessary for online undercover operations to succeed.²⁴⁵ Sometimes, it is sufficient for law enforcement to adopt a nickname in order to gain access to public chatting channels without joining the conversation or to receive an automatic invitation link without providing any personal information in order to login to a webpage.²⁴⁶ These

²⁴² KB van 17 oktober 2018 tot uitvoering van artikel 46*sexies*, §1, tweede lid van het Wetboek van Strafvordering, BS 19 November 2018; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 37; L. BOVÉ, *Politie mag infiltreren op internet*, <https://www.tijd.be/politiek-economie/belgie/federaal/politie-mag-infiltreren-op-internet/10037561.html> (consultation 19 November 2020); C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 217 and 224; DATANEWS, *Politie mag valse identiteit gebruiken om te infiltreren op internet*, https://datanews.knack.be/ict/politie-mag-valse-identiteit-gebruiken-om-te-infiltreren-op-internet/article-normal-1181521.html?cookie_check=1605805119 (consultation 19 November 2020); J. JANSEN, *Belgische politie krijgt recht om te infiltreren op internet*, <https://tweakers.net/nieuws/141799/belgische-politie-krijgt-recht-om-te-infiltreren-op-internet.html> (consultation 19 November 2020); J.-J. OERLEMANS, “Facebookvrienden worden met de verdachte”, *Justitiële verkenningen* 2018, Vol.44(5), (83) 83 and 95; F. PETITJEAN, *Politie mag infiltreren via het internet*, <https://www.computable.be/artikel/nieuws/overheid/6427352/5440850/politie-mag-infiltreren-via-het-internet.html> (consultation 19 November 2020); SECURITY MANAGEMENT, *Belgische politie mag online undercover gaan*, https://www.securitymanagement.nl/belgische-politie-mag-online-undercover-gaan/?vakmedianet-approve-cookies=1&_ga=2.160358325.923604566.1605804501-1241609121.1605804501 (consultation 19 November 2020); M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 260-264.

²⁴³ *Ibid.*

²⁴⁴ M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 260.

²⁴⁵ W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 401.

²⁴⁶ Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; Antwerp 10 November 2016, *Limb.Rechtsl.* 2018, Vol.2, 132; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 64; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 215-224; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon:*

situations are however not considered to be police infiltration, but online police observation in a publicly accessible place (*Part IV, Chapter 2, §2, a*).²⁴⁷ The amount of times that this occurs will be decisive in categorizing the observation as short-term (modest legal framework) or systemic (strict legal framework) (*Part I, Chapter 1, §2*). The main distinctive criterion between online police infiltration and online police observation is therefore whether personal information is being shared or not. Situations where an undercover agent has to share personal information do not necessarily entail the use of a false identity. Personal information like gender, age, nationality, religious orientation, sexual orientation etc. can be authentic and sufficient in order to infiltrate the internet without requiring to set up a complete false identity. Secondly, an online undercover police officer will also face less (physical) danger, since he does not have to actively interact with the suspect in real life.²⁴⁸ It is also easier to register all the contacts between the suspect and the undercover agent when they occur in cyberspace than when they occur in real life, where microphones, cameras and other recording devices have to be used.²⁴⁹

Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk 2012, Vol.33(3), (258) 264-265; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 391.

²⁴⁷ Art. 26 Wet op het Politieambt (WPA), *BS* 22 December 1992; Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; Antwerp 10 November 2016, *Limb.Rechtsl.* 2018, Vol.2, 132; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 64; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 215-224; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264-265; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 391.

²⁴⁸ MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 36; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 260-261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 401.

²⁴⁹ Art. 46*sexies*, §4 Sv., *BS* 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 9 and 36 and 44; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 260-261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 401.

Given that the Special Investigation Methods (SIMs) are exhaustively listed in art. 47ter Sv., there is discussion about whether online police infiltration can be considered a SIM.²⁵⁰ Art. 47ter Sv. mentions only police infiltration and not its online counterpart, and therefore strictly legally speaking online police infiltration cannot be considered a SIM.²⁵¹ VAN DEN WYNGAERT *et al.* suggest however another criterion in order to decide whether an investigation technique can be considered a SIM, based on the existence of a confidential file.²⁵² In contrast to real life police infiltration, it will not always be necessary to create a second confidential file in order to protect the identity of an online undercover agent.²⁵³ Given that online police infiltration is (physically) less dangerous than its offline counterpart and the adoption of a fictitious identity is not always required, it will not always be necessary to restrict the suspect's right to a fair trial by creating a confidential file which can only be reviewed by the Indictment Chamber (*Part III, Chapter 2, §1*).²⁵⁴ A confidential file will only be created if permission will be granted to the online undercover agent to commit criminal offenses.²⁵⁵ Strictly legally speaking, it however has to be concluded that online police infiltration is not a SIM.²⁵⁶

²⁵⁰ Art. 47ter, §1 Sv., BS 27 November 1808; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/20.

²⁵¹ *Ibid.*

²⁵² H. BERKMOES, *Ibid.*

²⁵³ MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 41 and 74; GwH 6 December 2018, nr. 174/2018, BS 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; C. CONINGS, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr.* 2019, Vol.5, (257) 260-261; S. ROYER, "Wet 25 december 2016 digitaal spuurwerk op twee punten vernietigd (noot onder GwH 6 december 2018)", *NJW* 2019, Vol.398, (212) 212; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 402.

²⁵⁴ MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 41 and 74; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 362; S. ROYER, "Wet 25 december 2016 digitaal spuurwerk op twee punten vernietigd (noot onder GwH 6 december 2018)", *NJW* 2019, Vol.398, (212) 212; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 402.

²⁵⁵ Art. 46sexies, §3, zevende lid Sv., BS 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 41 and 74; GwH 6 December 2018, nr. 174/2018, BS 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 362; C. CONINGS, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr.* 2019, Vol.5, (257) 260-261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 402.

²⁵⁶ Art. 47ter, §1 Sv., BS 27 November 1808; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 362; H. BERKMOES, "Bijzondere opsporingsmethoden

§2. US legal framework on police infiltration in the digital age

In the previous chapter it has already been explained that there is no general regulation of the investigation technique of police infiltration applicable to all law enforcement departments nationwide in the United States, and this research will therefore mainly focus on the FBI level.

The Attorney General's Guidelines, titled the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations, contain some provisions on online undercover operations and set certain requirements forth with which the FBI has to comply.²⁵⁷ For offline police infiltration a "series of related undercover activities generally consisting of more than three separate contacts by an undercover employee with the individual(s) under investigation" are required.²⁵⁸ A Note following this definition explains that "in the context of online communications, (...), multiple transmissions or e-mail messages can constitute one contact, much like a series of verbal exchanges can comprise a single conversation. Factors to be considered in determining whether multiple online transmissions constitute a single contact or multiple contacts include; the time between transmissions, the number of transmissions, the number of interruptions, topical transitions, and the media by which the communications are exchanged".²⁵⁹ Moreover, "a Special Agent in Charge of the FBI office or his or her designee may authorize, in writing, continued online undercover contact (...) if it is essential to continue online contact with a subject in order to either maintain credibility or avoid permanent loss of contact with a subject during the period of time in which an application for an online undercover operation is being prepared and submitted for approval".²⁶⁰ This is in contrast to its offline

(observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/19.

²⁵⁷ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>; D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 224-229; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1586; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 176-179; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 511.

²⁵⁸ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 1; OFFICE OF THE ATTORNEY GENERAL, *Undercover and sensitive operations unit, attorney general's guidelines on FBI undercover operation*, 1992, <https://www.justice.gov/archives/ag/undercover-and-sensitive-operations-unit-attorney-general-s-guidelines-fbi-undercover-operations>.

²⁵⁹ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 1.

²⁶⁰ *Ibid.*, 15.

counterpart where an undercover operation can only be initiated after approval by the Special Agent in Charge. The FBI needs predication within the framework of one of the three types of investigation to conduct online undercover operations (*Part III, Chapter 2, §2*).²⁶¹ As explained before, an undercover operation can only be conducted within a full investigation. It can however happen that during an assessment or a preliminary investigation online contact or communication is initiated with someone who can later turn out to be a suspect. This type of contact will therefore not always immediately be categorized as an online undercover operation.²⁶² An additional request ‘to continue online undercover contact during the time in which an application for an online undercover operation is being prepared and submitted for approval’ will in those cases be necessary. “A full report of all online activity occurring during this period must be submitted to the approving authority as soon as practicable. If approved, the undercover employee maintaining online contact during this period must: (a) maintain an accurate recording of all online communication; (b) avoid otherwise illegal activity; (c) maintain as limited an online profile as possible consistent with the need to accomplish the objectives stated above; (d) avoid physical contact with subjects; (e) take all necessary and reasonable actions during the interim period to protect potential victims and prevent serious criminal activity if online contact reveals a significant and imminent threat to third party individuals, commercial establishments, or government entities; and (f) cease undercover activities if (...) a determination is made to disapprove the undercover operation”.²⁶³

Where in person undercover agents physically infiltrate criminal organizations in order to obtain evidence or gain information, this can be done with much more ease from behind their computer through online infiltration on for example social media.²⁶⁴ It is in general not prohibited by US law to create fake profiles based on fake identities in order to interact with suspects, but a predicated reason within the framework of one of the three types of investigation

²⁶¹ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 6.5 Predication*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 6/3.

²⁶² R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 551.

²⁶³ J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 15-16.

²⁶⁴ T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 233.

(Part III, Chapter 2, §2) will be required.²⁶⁵ In *United States v. Gatson*, the District Court of New Jersey ruled that law enforcement can create fake Instagram accounts in order to investigate suspects without the need for a search warrant.²⁶⁶ If the suspect voluntarily accepts the friend request, the files found on his profile can be used as evidence against him.²⁶⁷ Social media policies prohibit however the use of fake accounts.²⁶⁸ Facebook's company policy emphasizes for example that not only its users, but also law enforcement has to comply with their rules, including their 'real name policy'.²⁶⁹ In a letter to the US Drug Enforcement Administration (DEA) regarding their online undercover operations, Facebook "asked to cease all activities that involve the impersonation of others" and stated that "the DEA's deceptive actions violate the terms and policies that govern the use of the Facebook service and undermine trust in the Facebook community".²⁷⁰ Facebook sued the DEA for this practice after an undercover operation where the DEA created a fake profile using photos and information of a suspect, which also sued the DEA for damages resulting from this operation.²⁷¹ As a reaction,

²⁶⁵ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 6.5 Predication*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 6/3; *United States v. Gatson*, Criminal No. 13-705 (D.N.J. Dec. 15, 2014); J. CROOK, *Police Can Create Fake Instagram Accounts to Investigate Suspects*, <https://techcrunch.com/2014/12/24/police-can-create-fake-instagram-accounts-to-investigate-suspects/> (consultation 6 November 2020); R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 541-542 and 551-552.

²⁶⁶ *United States v. Gatson*, Criminal No. 13-705 (D.N.J. Dec. 15, 2014); J. CROOK, *Police Can Create Fake Instagram Accounts to Investigate Suspects*, <https://techcrunch.com/2014/12/24/police-can-create-fake-instagram-accounts-to-investigate-suspects/> (consultation 6 November 2020).

²⁶⁷ *Ibid.*

²⁶⁸ S. HORWITZ, *Justice Dept. will review practice of creating fake Facebook profiles*, https://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html (consultation 6 November 2020); R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 542 and 551-552.

²⁶⁹ FACEBOOK, *Servicevoorwaarden*, <https://www.facebook.com/legal/terms> (consultation 27 October 2020); FACEBOOK, *Welke namen zijn toegestaan op Facebook?*, https://www.facebook.com/help/112146705538576?helpref=faq_%20content (consultation 27 October 2020); S. HORWITZ, *Justice Dept. will review practice of creating fake Facebook profiles*, https://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html (consultation 6 November 2020); R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 551-552; J. SULLIVAN, *Facebook letter to DEA*, <https://www.documentcloud.org/documents/1336541facebook-letter-to-dea.html> (consultation 27 October 2020); D. TWENEY, *Facebook is going after the DEA for creating fake profiles*, <https://www.businessinsider.com/facebook-is-going-after-the-dea-for-creating-fake-profiles-2014-10?IR=T> (consultation 19 November 2020).

²⁷⁰ J. SULLIVAN, *Facebook letter to DEA*, <https://www.documentcloud.org/documents/1336541facebook-letter-to-dea.html> (consultation 27 October 2020).

²⁷¹ E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 247-248; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1008; J. LINSHI, *Federal Drug Agency sued for creating fake Facebook profile*, <https://time.com/3479424/dea-fake-facebook-profile/> (consultation 19 November 2020); NBC NEWS, *DEA agent sued over fake Facebook page in drug case*, <https://>

the Department of Justice settled the case with the suspect paying her damages and decided to review its policy on creating fake profiles on Facebook.²⁷²

§3. Legal framework on police infiltration in the digital age compared

The legal frameworks on online police infiltration are in both countries regulated similarly to their offline counterparts. In Belgium, it is regulated by criminal procedural law, whereas in the United States no general regulation applicable to all law enforcement departments nationwide exists. The FBI and the local departments have therefore developed their own internal guidelines on this matter.

In Belgium, this investigation method requires an approving warrant issued by the Crown prosecutor or the investigating judge prior to its initiation. This is not required for the FBI in the United States and law enforcement agents will be able to continue communicating with a suspect until approval will be granted. This will however always take place within the framework of one of the three types of investigation which can only be initiated after prior approval based on predication. Given that (online) undercover operations can only be initiated during a full investigation, a delayed approval for this investigation technique is possible. The Belgian regulation seems to better protect the suspect's rights, given that an approving warrant prior to the initiation of an (online) undercover operation is required.

www.nbcnews.com/news/us-news/dea-agent-sued-over-fake-facebook-page-drug-case-n220461 (consultation 19 November 2020); THE GUARDIAN, *Justice Department settles case after DEA set up fake Facebook page in woman's name*, <https://www.theguardian.com/us-news/2015/jan/20/justice-department-woman-settlement-fake-facebook-page-dea> (consultation 19 November 2020); D. TWENEY, *Facebook is going after the DEA for creating fake profiles*, <https://www.businessinsider.com/facebook-is-going-after-the-dea-for-creating-fake-profiles-2014-10?IR=T> (consultation 19 November 2020);

²⁷² *Arquiett v. United States*, No. 13-CV-0752, *Stipulation for Voluntary Dismissal, Compromise Settlement, and Release of Claims*, http://online.wsj.com/public/resources/documents/2015_0120_Arquiettsettlement.pdf; S. HORWITZ, *Justice Dept. will review practice of creating fake Facebook profiles*, https://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html (consultation 6 November 2020); E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 247-248; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1008; J. LINSHI, *Federal Drug Agency sued for creating fake Facebook profile*, <https://time.com/3479424/dea-fake-facebook-profile/> (consultation 19 November 2020); THE GUARDIAN, *Justice Department settles case after DEA set up fake Facebook page in woman's name*, <https://www.theguardian.com/us-news/2015/jan/20/justice-department-woman-settlement-fake-facebook-page-dea> (consultation 19 November 2020).

The Belgian and FBI legal frameworks on online police infiltration have also some characteristics in common. Both systems require to maintain accurate and detailed transcripts of all the online communication between the undercover agent and the suspect. The requirement of the ‘long-lasting contact between the suspect and the undercover agent’ is being translated into the online world as a conversation consisting of multiple messages sent back and forth between the undercover agent and the suspect. The Belgian and FBI legal frameworks also state that the use of fake identities should be avoided for as long as possible and that anonymous accounts should be used instead, if possible. The social media’s real name policy is of course not country-specific and applies therefore in Belgium as well as in the United States. Online police infiltration gives undercover agents the opportunity to avoid physical contact with the suspects in real life and is therefore an important asset for both countries.

Chapter 4: The four principles compared

In case law enforcement in Belgium wants to make use of the Special Investigation Methods, and more specifically of police infiltration (including its online counterpart), they have to take four principles into account; subsidiarity, proportionality, the prohibition of provocation, and the prohibition to commit criminal offenses.²⁷³ In this chapter each of these Belgian principles will be discussed and compared to their US counterparts in order to find similarities or differences between both legal systems.

§1. Subsidiarity

a) Subsidiarity in Belgium

The investigation techniques of offline as well as online police infiltration can only be used “when this is required by the investigation and no other means appear to be sufficient in order to reveal the truth”.²⁷⁴ The subsidiarity principle in Belgium therefore requires that other investigative methods must seem to be insufficient in order to obtain the necessary information and only then these investigation techniques can be used. The investigation technique of police infiltration has been strictly regulated in the European Union (EU) given its risk of provoking

²⁷³ Art. 30 V.T.Sv., *BS* 25 April 1878; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 30-33; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/02 and 216/58 and 216/71; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 8-12; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137-1138.

²⁷⁴ Art. 46*sexies*, §1 and 47*octies*, §2 Sv., *BS* 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 36-37; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 362; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/58-216/59; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 259-260; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 20 and 149; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 400-401.

the person of interest.²⁷⁵ It is considered to be a much bigger invasion on the suspect's privacy and private life than for example wiretapping or police surveillance, and is therefore much less used.²⁷⁶ Undercover operations are considered to be an *ultimum remedium* that can only be employed when no other investigation techniques are sufficiently effective in order to obtain the evidence or information needed.²⁷⁷ According to ROSS, "in Europe, undercover investigations should always be considered as a tactic of last resort".²⁷⁸

b) Subsidiarity in the United States

In order to correctly discuss how the subsidiarity principle is applied in the United States, a distinction has to be made between national security investigations on the one hand, and criminal investigations on the other hand. National security investigations are executed by the FBI and are strictly regulated in the Attorney General's Guidelines and the FBI's internal DIOG.²⁷⁹ These are rarely used, well-thought and well-planned, long-term deep cover

²⁷⁵ D.J. KORF *et al.*, "Drugs en drugshandel in Nederland en België", *Tijdschrift voor Criminologie* 2006, Vol.48(2), (115) 122; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 62; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 496 and 537; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-240.

²⁷⁶ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 146; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 58-59; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 235; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-241.

²⁷⁷ C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 20 and 149; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

²⁷⁸ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 146; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 58-59; E.A. NADELMANN, *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 235; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 494 and 508; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

²⁷⁹ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,5/1-7/11>.

operations, for which only a few agents are certified. Undercover operations can only occur during a full investigation, which requires “an articulable factual basis of possible criminal or national threat activity” (*Part III, Chapter 2, §2*).²⁸⁰

Criminal investigations can be executed by all law enforcement departments and have headquarters’ oversight. In the pre-9/11 historical overview, it was already mentioned that in these investigations, undercover operations are very popular and largely employed for all types of crime (*Part III, Chapter 1, §1, b*).²⁸¹ They are one of the most effective investigation techniques in order to obtain quick results in criminal investigations.²⁸² Police infiltration is therefore sometimes overused as a tactic in order to obtain evidence in an easy way by provoking the target (also called ‘the shortcut problem’).²⁸³ These types of undercover operations can therefore not only have intended, but also many unintended consequences.²⁸⁴ Sometimes, law enforcement may offer irresistible temptations or encouragement to people who under normal circumstances would not have committed a crime (*Part III, Chapter 4, §3, b*).²⁸⁵

From a Fourth Amendment’s perspective, undercover operations are less privacy invasive than wiretapping or electronic surveillance (*Part V, Chapter 1, §2*).²⁸⁶ The FBI can approve an

²⁸⁰ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 7 Full Investigations*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%202/2002/view,7/1-7/11>.

²⁸¹ D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 210; O.S. BURN, “Abscam Ethics: Moral Issues And Deception In Law Enforcement edited by Gerald M. Caplan”, *Journal of Criminal Justice* 1984, Vol.12(1), (93) 93; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 53; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 11-13; C. FIJNAUT, “De exfiltratie van verdachte en veroordeelde criminelen”, *Justitiële verkenningen* 2012, Vol.38(3), (68) 73; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 246; G.T. MARX, “The New Police Undercover Work”, *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 400-410; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-241.

²⁸² J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120.

²⁸³ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 87; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1123.

²⁸⁴ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 140; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246.

²⁸⁵ G.T. MARX, “The New Police Undercover Work”, *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 411-412.

²⁸⁶ *Lopez v. United States*, 373 U.S. 427 (1963); E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 58-59; G.T. MARX, *Undercover: police*

undercover operation internally, whereas a wiretap requires a court authorized order. The US Supreme Court considers police infiltration to be less intrusive than electronic surveillance, and as a consequence requires no judicial authorization for it.²⁸⁷ ROSS summarizes this as “Before you subpoena documents; before you call witnesses to the grand jury; before you consider conventional sources of evidence; make sure to exhaust all undercover options first. This should become your mantra”.²⁸⁸

c) Subsidiarity compared

For national security investigations, the Belgian and FBI regulations on undercover operations show many similarities. They are strictly regulated and can only be used in rare cases under strict conditions. For criminal investigations, a difference can be noted between the Belgian and US legal systems. ROSS’ statements show a reversed use of the subsidiarity principle. In Belgium (and Europe), it is an investigation technique that may only be used as a last resort, whereas in the United States, it is sometimes overused as a tactic in order to obtain quick results and evidence in a fast and easy way. In Belgium, undercover operations are considered to entail a serious invasion on someone’s privacy and can therefore only be initiated based on a warrant, whereas from a US Fourth Amendment’s privacy perspective, undercover operations are less privacy invasive than wiretapping or electronic surveillance. There is no warrant requirement for the initiation of an undercover operation in the United States, whereas this is always required

surveillance in America, Berkeley, University of California press, 1988, 55; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

²⁸⁷ *Lopez v. United States*, 373 U.S. 427 (1963); *Lewis v. United States*, 385 U.S. 206 (1966); *Hoffa v. United States*, 385 U.S. 293 (1966); *United States v. White*, 401 U.S. 745 (1971); *Illinois v. Perkins*, 496 U.S. 292 (1990); C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 54; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 106; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 162; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 32-33; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 544; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1121; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 513 and 563; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867.

²⁸⁸ E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 58-59; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 494.

for a wiretap or electronic surveillance. Undercover operations in criminal investigations are therefore much less used in Belgium (and Europe) than in the United States.²⁸⁹

§2. Proportionality

a) Proportionality in Belgium

The Belgian courts have from the beginning made clear that police infiltration may only be used for serious crimes, with a main focus on organized crime.²⁹⁰ This was consequently confirmed in the confidential and secret guidelines, which were reconfirmed by the official legal framework regulating the Special Investigation Methods.²⁹¹ Offline police infiltration may only be employed if “there are serious indications that the persons of interest are or could be committing criminal offenses within a criminal organization or for which ordering a wiretap is permitted”.²⁹² The threshold for online police infiltration is somewhat lower and requires

²⁸⁹ E.W. KRUISBERGEN and D. DE JONG, “Undercoveroperaties: een noodzakelijk kwaad?”, *Justitiële verkenningen* 2012, Vol.38(3), (50) 58-59; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-241; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

²⁹⁰ Brussels 19 November 1984, *Pas.* 1985, II, 37, *RW* 1984-85, 2563; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 114-115; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 20 and 149; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137.

²⁹¹ Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 May 2003; Ministeriële Omzendbrief van 24 april 1990 betreffende de bijzondere opsporingstechnieken om de zware of georganiseerde criminaliteit te bestrijden, *Parl.doc.* nr. 1-447/4 A; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 4; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 361; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/11; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 55-56 and 110; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 112-119 and 134; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 7; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134; F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen””, *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, “Cassatie zet nieuwe BOM-bakens uit”, *Juristenkrant* 2008, Vol.180, (5) 5; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61.

²⁹² Art. 47octies Sv., *BS* 27 November 1808; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht*,

“serious indications that the persons of interest are committing or might commit criminal offenses that are punishable with a prison sentence of minimum one year”.²⁹³ An online undercover police officer faces less (physical) danger since he does not have to actively interact with the suspects in real life, and this is considered as a justifying ground for lowering the threshold.²⁹⁴ Long-term online interaction between a suspect and an undercover agent can however have an impact on the suspect’s privacy rights, but this is considered to be mitigated by the requirement that all communication has to be registered in order to ensure transparency.²⁹⁵ During real life police infiltration, it is almost impossible to register all contacts and communication between the suspect and the undercover agent, since it could endanger the agent’s credibility and safety.²⁹⁶ In both cases, offline as well as online, police infiltration can only be employed for serious crimes (punishable with a prison sentence of at least one year) and not for minor offenses.

criminologie en forensisch welzijnswerk 2012, Vol.33(3), (205) 217-224; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 261; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1149-1150; B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 205; P. VANWALLEGHEM, “Infiltratie mag ook om verdachte te arresteren”, *De Juristenkrant* 2014, Vol.4, (2) 2; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264.

²⁹³ Art. 46sexies Sv., *BS* 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St. Kamer* 2015-16, nr. 54-1966/001, 36-37; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 362; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/58-216/59; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 259-260; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 400-401.

²⁹⁴ MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St. Kamer* 2015-16, nr. 54-1966/001, 36; GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; C. CONINGS, “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, (257) 260-261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 401.

²⁹⁵ MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St. Kamer* 2015-16, nr. 54-1966/001, 36.

²⁹⁶ *Ibid.*

b) Proportionality in the United States

In order to correctly discuss how the proportionality principle is applied in the United States, a distinction has to be made again between national security investigations and criminal investigations. In national security investigations, an FBI undercover operation will only be initiated during a full investigation in order to “detect, obtain information about, or prevent or protect against federal crimes or threats to the national security based on an articulable factual basis of possible criminal or national threat activity” (*Part III, Chapter 2, §2*).²⁹⁷ In criminal investigations, it can on the contrary be used for all types of crime and is not limited to organized or serious crime.²⁹⁸ During the war on drugs, it was mainly used in drug and drug trafficking cases, but it is also employed in cases concerning prostitution, pornography, selling and/or buying of stolen goods, burglary and street crime.²⁹⁹

c) Proportionality compared

For national security investigations, the Belgian and FBI regulations of undercover operations show again many similarities, limiting their use to serious crime. For criminal investigations, the proportionality principle is again used in a reversed way. Where in Belgium police infiltration can only be employed in cases concerning serious crime, it has an almost universal use in the United States. The privacy implications of this investigation technique probably play a role in this decision. In Belgium (and Europe), undercover operations are considered to have a serious impact on someone’s privacy rights, whereas from a US Fourth Amendment’s privacy perspective, police infiltration is less privacy invasive than some other investigation techniques. The possibility of registering the interaction between a suspect and an undercover agent during online undercover operations is in Belgium considered to be a mitigating factor for the infringement of the privacy rights of the suspect, since it guarantees transparency in their communications. The more interactions can be registered, the more the privacy rights are

²⁹⁷ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 7 Full Investigations*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,7/1-7/11>.

²⁹⁸ J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 563.

²⁹⁹ G. DWORKIN, “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), (17) 18; G.T. MARX, “The New Police Undercover Work”, *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 400-410; G.T. MARX, “Who really gets stung? Some issues raised by the New Police Undercover Work”, *Crime & Delinquency* 1982, Vol.28(2), (165) 166-168.

considered to be protected, and therefore the threshold for allowing to initiate this online investigation technique can be lowered. Investigation methods have to be proportionate to the crimes being investigated and therefore it is understandable that the more privacy intrusive an investigation technique is considered to be, the more serious the crimes being investigated have to be and vice versa.³⁰⁰

§3. The prohibition of provocation

During undercover operations both the suspect and the undercover agent (also called agent provocateur) influence each other, and as the name says can sometimes even ‘provoke’ each other, having an impact on their mutual behavior.³⁰¹ This offers law enforcement the opportunity to not only investigate, but also create the events to a certain extent.³⁰² It is not

³⁰⁰ ATTORNEY GENERAL, *The Attorney General’s Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 13.

³⁰¹ ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/60-216/61; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 130-132; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1112-1115 and 1144-1148; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 497 and 537; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240 and 249-252 and 260; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2869-2870.

³⁰² ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/60-216/61; G. DWORKIN, “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), (17) 24; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1568-1569; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 163-164; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; I. LEIGH, “Undercover: Police Surveillance in America By G.T. Marx: Reviewed”, *British Journal of Criminology* 1991, Vol.31(1), (100) 101; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 65-67 and 130-132; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 244-245; R. ROIPHE, “The Serpent Beguiled Me: A History of the Entrapment Defense”, *Seton Hall Law Review* 2003, Vol.33(2), (257) 257; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1112-1114 and 1148; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 497 and 511-519 and 537; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239 and 249 and 260; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-

always clear when a certain form of undercover participation can be seen as provocation by the government and in which circumstances this can be allowed.³⁰³ Both Belgium and the United States have therefore created some guidelines and criteria in order to assess whether the suspect was provoked by the government.

a) The prohibition of provocation in Belgium

According to Belgian law, a case must be quashed by the court if the defendant can prove that he would not have committed the crime without being deceived and provoked by an (undercover) government official.³⁰⁴ The sole deception and creation of opportunity where the defendant is free to choose whether or not to engage in the criminal activity is not considered to be provocation.³⁰⁵ Provocation is according to art. 30 V.T.Sv. (Voorafgaande Titel van het Wetboek van Strafvordering, Chapter preceding the Belgian Code of Criminal Procedure) and the case law of the court of cassation characterized by; its occurrence prior to the crime, by a police officer or a civilian working for the police, and its direct influence on the commission of

2870; D.D. TAWIL, "Ready-Induce-Sting: Arguing for the Government's Burden of Proving Readiness in Entrapment Cases", *Michigan Law Review* 2000, Vol.98(7), (2371) 2372.

³⁰³ ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; ECtHR 24 April 2014, nr. 6228/09, 19678/07, 52340/08, 7451/09, 19123/09, Lagutin a.o./Russia, *T.Strafr.* 2014, Vol.3, 199; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 379-380; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 34; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62-63; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240.

³⁰⁴ Art. 30 V.T.Sv., *BS* 25 April 1878; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/60-216/62; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003, Vol.11, (1134) 1137-1138; F. SCHUERMANS and H. BERKMOES, "De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden", *T.Strafr.* 2006, Vol.2, (65) 67; F. SCHUERMANS, "De wettigheidscontrole van de observatie en infiltratie", *T.Strafr.* 2015, Vol.1, (27) 27.

³⁰⁵ Art. 30 V.T.Sv., *BS* 25 April 1878; Cass. 3 April 2001, *Arr.Cass.* 2001, Vol.4, 595, *Pas.* 2001, Vol.4, 589, *T.Strafr.* 2001, 338; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26; Cass. 6 September 2016 (R.E.J.P.); Antwerp 6 January 1993, *Turnh. Rechtsl.* 1993, 28, *Turnh. Rechtsl.* 1993, 68; Brussels 7 September 1994, *JLMB* 1994, 1135, *Journ. proc.* 1994, Vol.268, 25, *Pas.* 1993, II, 112, *Rev.dr.pén.* 1995, 419; Antwerp 21 May 1997, *Limb.Rechtsl.* 1997, 223; Corr. Brussels 12 April 1994, *Rev.dr.pén.* 1995, 423; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003, Vol.11, (1134) 1137-1138; F. SCHUERMANS and H. BERKMOES, "De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden", *T.Strafr.* 2006, Vol.2, (65) 67; F. SCHUERMANS, "De wettigheidscontrole van de observatie en infiltratie", *T.Strafr.* 2015, Vol.1, (27) 27.

the crime.³⁰⁶ An example of a case where provocation was employed, was a drug delivery case where the undercover agents requested the delivery of large amounts of drugs by the suspect, even though he had only been delivering small amounts before and he had never had the intention to deliver larger amounts.³⁰⁷ The sole aim of this provocation was to convict the suspect to a higher sentence.³⁰⁸

b) The prohibition of provocation in the United States

The use of undercover agents in some undercover operations has proven to be sometimes problematic and the suspect can use the defense of entrapment when the government was unduly providing the conditions to induce that person in criminal activity.³⁰⁹ The Fifth and

³⁰⁶ Art. 30 V.T.Sv., BS 25 April 1878; Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/63-216/64; F. SCHUERMANS and H. BERKMOES, “De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden”, *T.Strafr.* 2006, Vol.2, (65) 67; F. SCHUERMANS, “De wettigheidscontrole van de observatie en infiltratie”, *T.Strafr.* 2015, Vol.1, (27) 27.

³⁰⁷ Art. 30 V.T.Sv., BS 25 April 1878; Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26; F. SCHUERMANS, “De wettigheidscontrole van de observatie en infiltratie”, *T.Strafr.* 2015, Vol.1, (27) 27.

³⁰⁸ *Ibid.*

³⁰⁹ J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 16; *Sorrells v. United States*, 287 U.S. 435 (1932); *Sherman v. United States*, 356 U.S. 369 (1958); *United States of America v. Michael Leja and John M. Cody*, 563 F.2d 244 (6th Cir. 1977); *United States of America v. James B. Borum*, 584 F.2d 424 (D.C. Cir. 1978); *United States v. Jannotti*, 501 F.Supp. 1182 (E.D. Pa. 1980); B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756-757; B.W. BELL, “Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy”, *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 160; A. CARLON, “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), (1081) 1085-1090; J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1013 and 1051-1052; D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 265-266; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 158; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; G.T. MARX, “The New Police Undercover Work”, *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 416; R. ROIPHE, “The Serpent Beguiled Me: A History of the Entrapment Defense”, *Seton Hall Law Review* 2003, Vol.33(2), (257) 289-290; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1112 and 1144-1145; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 512 and 539 and 556; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 242 and 266-267; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; L.M. SEIDMAN, “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, (111) 111; D.D. TAWIL, “Ready-Induce-Sting: Arguing for the Government’s Burden of Proving Readiness in Entrapment Cases”, *Michigan Law Review* 2000, Vol.98(7), (2371) 2384; G. YAFFE, “The government beguiled

Fourteenth Amendment contain Due Process Clauses which consider the use of deception by law enforcement in some cases as “outrageous government conduct”.³¹⁰ A suspect can only rely on this defense in situations where no actual harm was caused (e.g. to a victim).³¹¹ If this defense will be accepted by the court, the suspect will be completely acquitted.³¹² If not, the use of deception and provocation will not be considered at all, not even as a mitigating ground.³¹³ Therefore, this defense is also called an ‘all or nothing type of defense’ or ‘affirmative defense’.³¹⁴ Historically, this defense has rarely been accepted, since oversight is provided by the Department of Justice during FBI undercover operations.³¹⁵ The Attorney General’s office

me: The entrapment defense and the problem of private entrapment”, *Journal of Ethics & Social Philosophy* 2005, Vol.1(1), (1) 2.

³¹⁰ Fifth Amendment to the United States Constitution, 15 December 1791; Fourteenth Amendment to the United States Constitution, 9 July 1868; *Brown v. Mississippi*, 297 U.S. 278 (1936); *Rochin v. California*, 342 U.S. 165 (1952); *United States v. Jannotti*, 501 F.Supp. 1182 (E.D. Pa. 1980); *United States v. Wylie*, 625 F.2d 1371 (9th Cir. 1980); *United States v. Fekri*, 650 F.2d 1044 (9th Cir. 1981); *State v. Hohensee*, 650 S.W.2d 268 (Mo. Ct. App. 1982); *Vaden v. State*, 768 P.2d 1102 (Alaska 1989); J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1014-1016 and 1051-1052 and 1072; D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 261-262 and 278; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 158; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1144-1147; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 512 and 539 and 556; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 242; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867; L.M. SEIDMAN, “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, (111) 116; C.E. SMITH, “The Bill of Rights after September 11th: Principles or Pragmatism”, *Duquesne Law Review* 2004, Vol.42(2), (259) 267-268.

³¹¹ J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1104; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 556.

³¹² A. CARLON, “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), (1081) 1085-1087; J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1017 and 1085 and 1104; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 556; L.M. SEIDMAN, “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, (111) 131; G. YAFFE, “The government beguiled me: The entrapment defense and the problem of private entrapment”, *Journal of Ethics & Social Philosophy* 2005, Vol.1(1), (1) 2.

³¹³ *Ibid.*

³¹⁴ A. CARLON, “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), (1081) 1085-1087; J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1017 and 1085 and 1104; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 556; L.M. SEIDMAN, “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, (111) 131; U.S. DEPARTMENT OF JUSTICE, 645. *Entrapment-Elements*, <https://www.justice.gov/archives/jm/criminal-resource-manual-645-entrapment-elements> (consultation 1 May 2021); G. YAFFE, “The government beguiled me: The entrapment defense and the problem of private entrapment”, *Journal of Ethics & Social Philosophy* 2005, Vol.1(1), (1) 2.

³¹⁵ J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations>

works with FBI undercover agents and provides guidance to ensure that there is no excessive government involvement or provocation.³¹⁶ This is applicable to law enforcement agents and confidential human sources alike.³¹⁷ The sole deception and creation of opportunity where the defendant is free to choose whether or not to engage in the criminal activity will also here not be considered as provocation.³¹⁸

Suspects that are ‘predisposed to engage in criminal conduct’ may however not rely on this defense.³¹⁹ Someone is considered to be predisposed when it is likely that he would have

.pdf, 17-18; *United States v. Russell*, 411 U.S. 423 (1973); *Hampton v. United States*, 425 U.S. 484 (1976); *United States v. Prairie*, 572 F.2d 1316 (9th Cir. 1978); *United States v. Wylie*, 625 F.2d 1371 (9th Cir. 1980); *United States v. Fekri*, 650 F.2d 1044 (9th Cir. 1981); *State v. Hohensee*, 650 S.W.2d 268 (Mo. Ct. App. 1982); *Vaden v. State*, 768 P.2d 1102 (Alaska 1989).

³¹⁶ J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 17-18.

³¹⁷ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 16.1 Undisclosed participation: Overview*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 16/1.

³¹⁸ U.S. DEPARTMENT OF JUSTICE, 645. *Entrapment-Elements*, <https://www.justice.gov/archives/jm/criminal-resource-manual-645-entrapment-elements> (consultation 1 May 2021).

³¹⁹ *Sorrells v. United States*, 287 U.S. 435 (1932); *Sherman v. United States*, 356 U.S. 369 (1958); *State v. Hohensee*, 650 S.W.2d 268 (Mo. Ct. App. 1982); *Vaden v. State*, 768 P.2d 1102 (Alaska 1989); B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756-757; A. CARLON, “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), (1081) 1087-1090 and 1126-1127; J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1014-1016 and 1036-1044 and 1072-1073; G. DWORKIN, “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), (17) 22; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 239-240; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1566-1570 and 1580; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; G.T. MARX, “The New Police Undercover Work”, *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 416-417; G.T. MARX, “Who really gets stung? Some issues raised by the New Police Undercover Work”, *Crime & Delinquency* 1982, Vol.28(2), (165) 169-172; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 245; R. ROIPHE, “The Serpent Beguiled Me: A History of the Entrapment Defense”, *Seton Hall Law Review* 2003, Vol.33(2), (257) 257-258 and 289-290; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1144-1147; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 539 and 556; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 242-249; L.M. SEIDMAN, “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, (111) 119; J. SHERMAN, “A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations”, *Journal of constitutional law* 2009, Vol.11(5), (1475) 1480; D.D. TAWIL, “Ready-Induce-Sting: Arguing for the Government’s Burden of Proving Readiness in Entrapment Cases”, *Michigan Law Review* 2000, Vol.98(7), (2371) 2377; U.S. DEPARTMENT OF JUSTICE, 645. *Entrapment-Elements*, <https://www.justice.gov/archives/jm/criminal-resource-manual-645-entrapment-elements> (consultation 1 May 2021); G. YAFFE, “The government beguiled me: The entrapment defense and the problem of private entrapment”, *Journal of Ethics & Social Philosophy* 2005, Vol.1(1), (1) 7.

committed the offense without being deceived by a government official (subjective test).³²⁰ In the Fusko case, the Circuit Court formulated five criteria in order to determine predisposition: “1) the character or reputation of the defendant; 2) whether the suggestion of the criminal activity was originally made by the government; 3) whether the defendant had engaged in criminal activity for a profit; 4) whether the defendant evidenced reluctance to commit the offense, overcome by government persuasion, and; 5) the nature of the inducement or persuasion offered by the government”.³²¹

This predisposition analysis entails however the risk that law enforcement may assume that virtually every type of deception is allowed once predisposition has been proven.³²² Some scholars question these criteria and have therefore suggested alternative means to prove predisposition.³²³ DWORKIN argues that the government should prove that it had probable cause to believe that the suspect was predisposed to commit the particular criminal offense.³²⁴ DRIPPS agrees with his statement and suggests that there should be proof of a certain involvement in criminal activities before allowing to initiate an undercover operation, lowering DWORKIN’s criterion of ‘probable cause’ to ‘reasonable suspicion’.³²⁵ The main aim of using

³²⁰ *Ibid.*

³²¹ United States of America v. Marian Fusko, 869 F.2d 1048 (7th Cir. 1989); U.S. v. Skarie, 971 F.2d 317 (9th Cir. 1992); United States v. Nettles, 400 F.Supp.2d 1084 (N.D. III. 2005); A. CARLON, “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), (1081) 1088; J. SHERMAN, “A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations”, *Journal of constitutional law* 2009, Vol.11(5), (1475) 1504-1505; D.D. TAWIL, “Ready-Induce-Sting: Arguing for the Government’s Burden of Proving Readiness in Entrapment Cases”, *Michigan Law Review* 2000, Vol.98(7), (2371) 2374.

³²² A. CARLON, “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), (1081) 1089; J.C. CARLSON, “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), (1011) 1039; T. FORAN, “Covert Operations on the Internet” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (233) 239-240; G.T. MARX, “Who really gets stung? Some issues raised by the New Police Undercover Work”, *Crime & Delinquency* 1982, Vol.28(2), (165) 170; G. YAFFE, “The government beguiled me: The entrapment defense and the problem of private entrapment”, *Journal of Ethics & Social Philosophy* 2005, Vol.1(1), (1) 7.

³²³ D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 261 and 277; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1113; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 244.

³²⁴ D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 237-238; G. DWORKIN, “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), (17) 17 and 33; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 244.

³²⁵ D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 261 and 281-282; B.L. GERSHMAN, “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, (1565) 1588-1589; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 244.

police infiltration should according to him be the prevention of criminal activity and bringing suspects to trial.³²⁶ The probable cause criterion might in some (endangered national security) cases be too strict.³²⁷ DRIPPS' theory is based on the Due Process Clause of the Fourteenth Amendment which prohibits deprivation of life, liberty, or property without due process of law.³²⁸

Ongoing offenders are suspects that will commit criminal offenses anyway, with or without deception by government officials.³²⁹ Targets of opportunity are people that would not have committed the criminal offenses without the specific circumstances provided by the government.³³⁰ Sometimes, law enforcement uses specific inducements to seduce or convince a potential suspect to commit a crime, such as sex or money (objective test).³³¹ In other cases,

³²⁶ D.A. DRIPPS, "At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense", *University of Illinois Law Review* 1993, Vol.2, (261) 261.

³²⁷ D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 237-238.

³²⁸ Fourteenth Amendment to the United States Constitution, 9 July 1868; D.A. DRIPPS, "At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense", *University of Illinois Law Review* 1993, Vol.2, (261) 261 and 276-283; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1588-1589; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 244.

³²⁹ A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1090-1096; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 172; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 245.

³³⁰ *Sherman v. United States*, 356 U.S. 369 (1958); A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1090-1096 and 1127; J.C. CARLSON, "The Act Requirement and the Foundations of the Entrapment Defense", *Virginia Law Review* 1987, Vol.73(6), (1011) 1016-1017 and 1026-1032 and 1044-1052 and 1072; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 249-250; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 172; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1149; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 245; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2868.

³³¹ *United States v. Jannotti*, 501 F.Supp. 1182 (E.D. Pa. 1980); A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1090-1093 and 1109; J.C. CARLSON, "The Act Requirement and the Foundations of the Entrapment Defense", *Virginia Law Review* 1987, Vol.73(6), (1011) 1016-1017 and 1026-1032 and 1044-1052; G. DWORKIN, "The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime", *Law and Philosophy* 1985, Vol.4(1), (17) 22-23; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1578-1579; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 250; G.T. MARX, "The New Police Undercover Work", *Journal of Contemporary Ethnography* 1980, Vol.8(4), (399) 416-417; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 130-132; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 512; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 245; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and

they might use a person's moment of temporary vulnerability in order to deceive him, such as someone's bankruptcy or through repeating the offer several times when the suspect turned it down at first hand.³³² In these circumstances, the court will more likely accept the defense of entrapment by conducting the objective test.³³³

The subjective and objective tests are sometimes considered to be each other's opposite. However, some courts apply them together and scrutinize not only the defendant's predisposition (subjective test), but also the level of inducement offered by law enforcement

D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2868; L.M. SEIDMAN, "The Supreme Court, Entrapment, and Our Criminal Justice Dilemma", *Supreme Court Review* 1981, (111) 119; J. SHERMAN, "A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations", *Journal of constitutional law* 2009, Vol.11(5), (1475) 1480; D.D. TAWIL, "Ready-Induce-Sting: Arguing for the Government's Burden of Proving Readiness in Entrapment Cases", *Michigan Law Review* 2000, Vol.98(7), (2371) 2378.

³³² Sorrells v. United States, 287 U.S. 435 (1932); Sherman v. United States, 356 U.S. 369 (1958); United States v. Kelly, 539 F.Supp. 363 (D.D.C. 1982); Jacobson v. United States, 503 U.S. 540 (1992); A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1090-1095 and 1109-1110 and 1128-1129; J.C. CARLSON, "The Act Requirement and the Foundations of the Entrapment Defense", *Virginia Law Review* 1987, Vol.73(6), (1011) 1016-1017 and 1026-1032 and 1044-1052; D.A. DRIPPS, "At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense", *University of Illinois Law Review* 1993, Vol.2, (261) 276; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 224-225; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1577-1583; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 170-171; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 130-132; R. ROIPHE, "The Serpent Beguiled Me: A History of the Entrapment Defense", *Seton Hall Law Review* 2003, Vol.33(2), (257) 289-290 and 299-300; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 245; L.M. SEIDMAN, "The Supreme Court, Entrapment, and Our Criminal Justice Dilemma", *Supreme Court Review* 1981, (111) 121-122; J. SHERMAN, "A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations", *Journal of constitutional law* 2009, Vol.11(5), (1475) 1479-1481.

³³³ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756-757; A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1085-1093; J.C. CARLSON, "The Act Requirement and the Foundations of the Entrapment Defense", *Virginia Law Review* 1987, Vol.73(6), (1011) 1013-1017 and 1026-1032 and 1044-1052 and 1072; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 249; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1127; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 512; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 245; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2868; J. SHERMAN, "A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations", *Journal of constitutional law* 2009, Vol.11(5), (1475) 1480; D.D. TAWIL, "Ready-Induce-Sting: Arguing for the Government's Burden of Proving Readiness in Entrapment Cases", *Michigan Law Review* 2000, Vol.98(7), (2371) 2378; U.S. DEPARTMENT OF JUSTICE, *645. Entrapment-Elements*, <https://www.justice.gov/archives/jm/criminal-resource-manual-645-entrapment-elements> (consultation 1 May 2021).

(objective test).³³⁴ Even when courts tend to prefer one test, they still somehow take the elements of the other test into account.³³⁵

c) The prohibition of provocation compared

The prohibition of provocation is an important principle in the Belgian and US legal systems. Both systems recognize the importance of the mutual influence that a suspect and an undercover agent may have on each other's behavior. The establishment of provocation can therefore as well in Belgium as in the United States, for the latter under the defense of entrapment, be invoked by the suspect in order to quash the case. In both countries the suspect's predisposition will be examined in order to decide whether the government only deceived the suspect by creating an opportunity leaving him free to choose whether or not to commit the criminal offense, or, whether provocation indeed occurred. For establishing the latter, it is required that the crime was suggested by the government prior to its commitment and that the government's persuasion influenced the decision of the suspect. Solely deception and creation of opportunity do not count as provocation. Belgian and US courts will therefore often use the subjective (predisposition) and objective (government inducement) test in a combined way in order to establish whether provocation by the government has occurred. These tests are in Belgium however not as explicitly mentioned as in US law, but implicitly these criteria can also be derived from the Belgian regulation of the prohibition of provocation. In Belgium and in the United States, provocation by law enforcement officials as well as by private individuals commissioned by the government, can be invoked by the suspect in order to establish that provocation by the government has occurred, and as a consequence he can request that the case will be quashed.

³³⁴ United States v. Daniel A. Gendron, 18 F.3d 955 (1st Cir. 1994); A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1093-1095; J.C. CARLSON, "The Act Requirement and the Foundations of the Entrapment Defense", *Virginia Law Review* 1987, Vol.73(6), (1011) 1014 and 1030-1031 and 1045-1046 and 1074 and 1093; R. ROIPHE, "The Serpent Beguiled Me: A History of the Entrapment Defense", *Seton Hall Law Review* 2003, Vol.33(2), (257) 292.

³³⁵ A. CARLON, "Entrapment, Punishment, and the Sadistic State", *Virginia Law Review* 2007, Vol.93(4), (1081) 1093-1095; L.M. SEIDMAN, "The Supreme Court, Entrapment, and Our Criminal Justice Dilemma", *Supreme Court Review* 1981, (111) 117.

§4. The prohibition to commit criminal offenses

During undercover operations, it will sometimes be necessary that police infiltrators commit certain criminal offenses in order to convince the suspects or persons of interest to trust and rely on them.³³⁶ The principle of the prohibition to commit criminal offenses is therefore not that strict for the investigation technique of police infiltration.³³⁷ The European as well as the United States' legal systems have in response created certain categories of 'acceptable participation', and in those situations the agents will not be prosecuted for their actions.³³⁸ However, if an undercover agent engages in unauthorized criminal offenses, he can be held liable and this may sometimes also constitute an exoneration ground for the suspect.³³⁹ The

³³⁶ MvT bij het wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/001, 25; State v. Rowan, 288 N.E.2d 829 (Ohio Ct. App. 1972); H. BERKMOES, "De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden", *Orde van de dag* 2003, Vol.4, (25) 34; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/73-216/74; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 34; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62-63; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 165-167; E.W. KRUISBERGEN and D. DE JONG, "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), (50) 50; K.J. MITCHELL, J. WOLAK and D. FINKELHOR, "Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?", *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), (241) 242-243; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 499 and 538; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240 and 252; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 401.

³³⁷ H. BERKMOES, "De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden", *Orde van de dag* 2003, Vol.4, (25) 30-33; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/02 and 216/71; F. HUTSEBAUT and K. VAN CAUWENBERGHE, "De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?", *Orde van de dag* 2003, Vol.4, (7) 12; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003, Vol.11, (1134) 1138-1140; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 401 and 410-411.

³³⁸ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 34; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62-63; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1123-1124; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240 and 250 and 266.

³³⁹ J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 539; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 250 and 266.

level of exoneration for the suspect might differ from mitigating grounds to even a complete dismissal of criminal charges.³⁴⁰

a) The prohibition to commit criminal offenses in Belgium

When an undercover agent participates in criminal activities, he can in some situations be liable for the crimes he committed.³⁴¹ In some European countries, this may in the most extreme cases lead to a complete dismissal of criminal charges for the suspect before the trial even starts.³⁴² In other European countries, it will not go as far as to dismiss the whole case against the suspect, but the criminal liability of the undercover agent might be taken into account by the court as a mitigating factor and may result in a reduction of the suspect's punishment.³⁴³ Most European countries have therefore enumerated a list of situations and immunities that can be invoked by undercover agents.³⁴⁴ Belgium has however decided not to make such an enumerating list.³⁴⁵ It feared that this would offer criminal organizations the possibility to test new members by

³⁴⁰ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 61; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1127; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 539 and 555-556; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 250 and 261.

³⁴¹ H. BERKMOES, "De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden", *Orde van de dag* 2003, Vol.4, (25) 30-34; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/02; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 257; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

³⁴² J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 539; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240-241 and 257-260; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2870.

³⁴³ J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 555-556; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 241 and 257-260; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2870.

³⁴⁴ J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

³⁴⁵ MvT bij het wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/001, 27-28; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 41-43; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/75; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003, Vol.11, (1134) 1140-1141.

DIOG, “specific approval for Otherwise Illegal Activity must be obtained in the context of these undercover activities or operations in addition to general approval of the scenario or the operation. Otherwise Illegal Activity by an FBI employee in an undercover operation relating to activity in violation of federal criminal law (...) must be approved in conformity with the Attorney General’s Guidelines on FBI Undercover Operations”.³⁵⁰ Therefore, undercover agents are immune to prosecution as long as their (criminal) actions are situated within the scope of their official undercover role and approval has been obtained.³⁵¹ These (criminal) actions can consist of providing an opportunity for the suspect to engage in criminal activity or engaging in criminal activities in order to maintain the agent’s false identity and gain the suspect’s confidence.³⁵² The crimes committed by the undercover agent have to be limited in scope, reasonably necessary and may moreover never exceed the severity of the crime being investigated.³⁵³ Police infiltrators are therefore allowed to engage in conduct that would under normal circumstances constitute a violation of federal, state or local law, as long as it is based on prior authorization.³⁵⁴ However, Otherwise Illegal Activity appears to occur rather limited,

20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%20001%20of%2002/view, 16/1 and 17/1-17/2; State v. Rowan, 288 N.E.2d 829 (Ohio Ct. App. 1972); United States v. Parisi, 674 F.2d 126 (1st Cir. 1982); Vaden v. State, 768 P.2d 1102 (Alaska 1989); E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 157; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 571.

³⁵⁰ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 17 Otherwise Illegal Activity (OIA)*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%20001%20of%2002/view, 17/1-17/2>.

³⁵¹ State v. Rowan, 288 N.E.2d 829 (Ohio Ct. App. 1972); E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 158 and 169.

³⁵² J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf, 13>; ATTORNEY GENERAL, *The Attorney General’s Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf, 33-34>; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 165.

³⁵³ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 17.2 Otherwise Illegal Activity (OIA): Purpose and Scope*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%20001%20of%2002/view, 17/1>.

³⁵⁴ J. ASHCROFT, *The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf, 13>; ATTORNEY GENERAL, *The Attorney General’s Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf, 33-34>; State v. Rowan, 288 N.E.2d 829 (Ohio Ct. App. 1972); E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 157-158 and 177-178; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 571.

since a higher level of approval and oversight is needed in order to engage in it.³⁵⁵ In unauthorized cases, the jury will have to decide whether or not the undercover agent exceeded his legal authority.³⁵⁶

In addition, the Attorney General's Guidelines do not allow FBI undercover agents to participate in violent acts, unless authorized and only "1) in situations where it is necessary to obtain not reasonably available information or evidence; 2) when it is necessary to establish or maintain the credibility of an undercover agent's cover identity, or; 3) in order to prevent death or serious bodily injury".³⁵⁷

c) The prohibition to commit criminal offenses compared

Belgium and the United States allow undercover agents to commit criminal offenses and grant them immunity until a certain extent. Both countries consider this allowed in situations of self-defense, when it is necessary to ensure other people's safety and when it is necessary for closing an investigation or obtaining necessary evidence. In the United States, FBI undercover agents may under these circumstances even participate in violent acts. Belgian criminal procedural law and the Attorney General's Guidelines specify some requirements which have to be fulfilled in order to legally commit criminal offenses. First of all, prior authorization has to be acquired by an FBI undercover agent who intends to commit a criminal offense during his undercover operation. In Belgium, this is regulated by the condition that before every undercover operation, the Crown prosecutor or the investigating judge has to make a list of enumerated criminal offenses that are allowed to be committed by the police infiltrator in that particular case. Belgium did not opt for a general list enumerating criminal offenses that are allowed during undercover operations, but takes a specific approach by enumerating the accepted criminal

³⁵⁵ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 14; ATTORNEY GENERAL, *The Attorney General's Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 34; *State v. Rowan*, 288 N.E.2d 829 (Ohio Ct. App. 1972); *United States v. Parisi*, 674 F.2d 126 (1st Cir. 1982); *Vaden v. State*, 768 P.2d 1102 (Alaska 1989).

³⁵⁶ C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 62-63; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 539; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 240-241.

³⁵⁷ J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 12-17; ATTORNEY GENERAL, *The Attorney General's Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 34; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 178.

offenses in each case. In the United States, prior authorization suffices for an undercover agent to commit the criminal offense he requested. Sometimes, it will however not be possible to obtain this prior authorization and therefore both countries allow undercover agents to notify their supervisor as soon as possible after the commitment of a crime in these special circumstances.³⁵⁸ This will mainly happen when the undercover agent has to participate in an unexpected criminal offense in order to safeguard his cover, without having the time to (safely) contact his supervisor to ask for prior permission.³⁵⁹ In any case, all crimes committed by undercover agents have to be proportionate to the crime under investigation. This is required by both Belgian and US law. If these conditions will be fulfilled, immunity will most likely be granted to the police infiltrator for the crimes he committed.

Within these similarities also some differences can be identified. The specific situations in which immunity will be granted, and more specifically the enumerating list of cases in which the prohibition to commit criminal offenses can be neglected by law enforcement, are in Belgium more strict than in the United States. The FBI legal framework is therefore less sympathetic for suspects than the Belgian legal system. In Belgium, the list of enumerated allowed criminal offenses creates a more strict framework for law enforcement to comply with and can therefore be considered to be more sympathetic for the suspects. Belgian police infiltrators will after all be restricted in their actions.

³⁵⁸ Art. 46*sexies*, §3 and 47*quinquies*, §2 Sv., BS 27 November 1808; ATTORNEY GENERAL, *The Attorney General's Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 34.

³⁵⁹ *Ibid.*

Part IV: Systemic police observation and surveillance

The second investigation technique that will be discussed in this research is systemic police observation. Given its common characteristics with the investigation technique of police infiltration, namely consistency and a certain period of time to be able to recognize patterns in someone's life, these two investigation techniques are interesting to compare. They show even more similarities in their online versions and especially then it will not always be clear where the line has to be drawn between police infiltration and systemic police observation. In the introduction and methodology, it has already been explained that for the investigation technique of police observation only systemic police observation will be analyzed, leaving short-term police observation out of the topics discussed in this research.

Chapter 1: Legal framework on systemic police observation

§1. Belgian legal framework on systemic police observation

The investigation technique of systemic police observation or surveillance is in Belgium, as police infiltration, part of the Special Investigation Methods (SIMs).³⁶⁰ Its legal history is

³⁶⁰ Art. 47ter, §1 Sv., BS 27 November 1808; MvT bij het wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/001, 7-8; Arbitragehof 21 December 2004, nr. 202/2004, A.A. 2004, Vol.5, 2283, BS 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106; Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170; H. BERKMOES, "Actualia BOM en enige andere opsporings- en onderzoekshandelingen", *NC* 2019, Vol.5, (361) 361; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/01; CRIMINIS WOORDENLIJST, *Bijzondere opsporingsmethoden*, <https://joachimmeese.be/criminis/woordenlijst/bijzondere-opsporingsmethoden/> (consultation 10 October 2020); J. DELMULLE, "Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.", *T.Strafr.* 2005, Vol.3, (230) 230-231; F. HUTSEBAUT and K. VAN CAUWENBERGHE, "De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?", *Orde van de dag* 2003, Vol.4, (7) 8; JURECA, *Bijzondere opsporingsmethoden (BOM)*, <https://www.jureca.be/verklaring/bijzondere-opsporingsmethoden-bom> (consultation 10 October 2020); B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 64 and 205; J.

therefore similar to that of the investigation technique of police infiltration (*Part III, Chapter 2, §1*). Up until 1990, there was no formal regulation of police surveillance.³⁶¹ In 1990, it was regulated in the same non-legislative secret guideline (circulaire) of April 24, 1990 as police infiltration, followed by the secret guideline of March 5, 1992, which required a reasonable suspicion in order to initiate a long-term police surveillance operation.³⁶² The Crown prosecutor or the investigating judge had to be notified of the surveillance and a written report had to be delivered to them afterwards.³⁶³

The first official legal framework for systemic police observation was introduced by the law of January 6, 2003 on the Special Investigation Methods (*Part III, Chapter 2, §1*) and received its own regulation in the Belgian Code of Criminal Procedure with article 47*sexies*.³⁶⁴ The four principles discussed in the previous part (subsidiarity, proportionality, the prohibition of

VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61.

³⁶¹ M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 55 and 109; S. FIELD and C. PELSNER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 112-119; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 7.

³⁶² Ministeriële Omzendbrief van 24 april 1990 betreffende de bijzondere opsporingstechnieken om de zware of georganiseerde criminaliteit te bestrijden, *Parl.doc.* nr. 1-447/4 A; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/09; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 30; S. FIELD and C. PELSNER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 121; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 7; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134; F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen’”, *Juristenkrant* 2008, Vol.165, (8) 8; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61-64.

³⁶³ H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/35; M. DEN BOER, *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 30; S. FIELD and C. PELSNER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 121.

³⁶⁴ Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 May 2003; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 361-363; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/11; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134 and 1147-1150; F. SCHUERMANS, “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen’”, *Juristenkrant* 2008, Vol.165, (8) 8; F. SCHUERMANS, “Cassatie zet nieuwe BOM-bakens uit”, *Juristenkrant* 2008, Vol.180, (5) 5; J. VAN GAEVER, “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, (61) 61.

provocation, and the prohibition to commit criminal offenses) have also to be taken into account when the investigation technique of systemic police observation is employed.³⁶⁵

Systemic police observation is defined in art. 47*sexies* Sv. as “the systemic observation by a police officer of one or more persons, their presence or behavior, or of certain matters, places or events”.³⁶⁶ If these conditions are fulfilled, the strict SIM rules will be applicable.³⁶⁷ The Crown prosecutor can issue a warrant for this type of observation in a criminal investigation (in Dutch: opsporingsonderzoek).³⁶⁸ A warrant is in any case required and has to be in writing, unless in urgent cases where authorization can be granted orally.³⁶⁹ In those cases, it however has to be confirmed in writing as soon as possible.³⁷⁰ Moreover, the conditions of necessity for the investigation on the one hand and the non-availability of other sufficient means in order to obtain the evidence required on the other hand (subsidiarity principle) have to be fulfilled.³⁷¹ Lastly, §2 of art. 47*sexies* Sv. states that systemic observations during which technical resources

³⁶⁵ Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; H. BERKMOES, “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, (25) 30-31; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/58; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 8-12; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137-1138.

³⁶⁶ Art. 47*sexies* Sv., *BS* 27 November 1808; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 363; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 217-223; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147; B. TILLEMANN, E. DIRIX and P. VAN ORSHOVEN, *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 280; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262.

³⁶⁷ H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 363; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 217-223; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147-1148; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262.

³⁶⁸ Art. 47*sexies*, §2 Sv., *BS* 27 November 1808; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147-1148; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262.

³⁶⁹ Art. 47*sexies*, §3 and §5 Sv., *BS* 27 November 1808.

³⁷⁰ Art. 47*sexies*, §5 Sv., *BS* 27 November 1808.

³⁷¹ Art. 47*sexies*, §2 Sv., *BS* 27 November 1808; Cass. 9 October 2013, *Arr.Cass.* 2013, Vol.10, 2061, *Pas.* 2013, Vol.10, 1903; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147-1148; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262.

are used, also called electronic surveillance, may only occur if there are serious indications that the criminal offenses under investigation may result in a prison sentence of at least one year (proportionality principle).³⁷² Paragraph 1 of this article provides some indicators of situations which can be considered as systemic police observation, like: “1) an observation of more than five consecutive days or of more than five non-consecutive days spread over a period of one month; 2) an observation during which technical resources are used (electronic surveillance); 3) an observation with an international dimension, or; 4) an observation carried out by the special forces of the federal police”.³⁷³

Wiretapping and monitoring someone else’s communication without the required authorization is under Belgian law a criminal offense.³⁷⁴ Art. 259*bis* and 314*bis* Sw. (Strafwetboek; Belgian Criminal Code) penalize these acts.³⁷⁵ These articles apply also to police officers who do not possess the authorization required in order to gather and process this type of information.³⁷⁶

³⁷² Art. 47*sexies*, §2 Sv., BS 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St. Kamer* 2015-16, nr. 54-1966/001, 45; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 224; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 11-12; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147-1148; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262.

³⁷³ Art. 47*sexies*, §1 Sv., BS 27 November 1808; H. BERKMOES, “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, (361) 363-364; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 223; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 332; F. HUTSEBAUT and K. VAN CAUWENBERGHE, “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, (7) 11-12; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1147; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262.

³⁷⁴ M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

³⁷⁵ Art. 259*bis* and 314*bis* Strafwetboek (Sw.), BS 9 June 1867; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

³⁷⁶ M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

§2. US legal framework on systemic police observation

Police surveillance might in the United States come within the scope of ‘search’ protected by the Fourth Amendment (*Part V, Chapter 1, §2*) and in those cases this can only occur based on a warrant.³⁷⁷ However, not all surveillance operations are defined as ‘searches’ and require therefore not always a warrant. If the FBI has a predicated reason³⁷⁸ in an assessment (*Part III, Chapter 2, §2*) and no use of technical resources is made, it is allowed to physically surveil a person for an unlimited amount of time without a warrant.³⁷⁹ The idea behind this regulation is that since it is such a human and energy intensive investigation technique, the FBI will be forced to limit itself to conducting this only in very rare cases based on an well-founded suspicion and during a limited amount of time. The main criterion in order to determine whether police surveillance constitutes a ‘search’ within the meaning of the Fourth Amendment is whether the person concerned could have a ‘reasonable expectation of privacy’.³⁸⁰ If surveillance only occurs occasionally and in public places, a warrant will not be required since there will be no

³⁷⁷ Fourth Amendment to the United States Constitution, 15 December 1791; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 272; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 538-540.

³⁷⁸ i.e. information or an allegation of activity that (might) constitute a federal crime or threat to national security; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 6.5 Predication*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 6/3.

³⁷⁹ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 18.5.8 Investigative Method: Physical Surveillance (not requiring a court order)*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 18/50-18/54.

³⁸⁰ Fourth Amendment to the United States Constitution, 15 December 1791; *United States v. Knotts*, 460 U.S. 276 (1983); *United States v. Karo*, 468 U.S. 705 (1984); *Osburn v. Nevada*, 118 Nev. 323 (Nev. 2002); *United States v. Smith*, 387 Fed.Appx. 918 (11th Cir. 2010); *United States v. Marquez*, 605 F.3d 604 (8th Cir. 2010); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 732; W. BLOSS, “Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects”, *Surveillance & Society* 2007, Vol.4(3), (208) 212; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 262-263; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 538-545; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; M. RADLER, “Privacy is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance”, *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1228; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1810-1811.

intrusion with someone's Fourth Amendment rights.³⁸¹ The use of technical resources, such as the placement of a wiretap, bug or GPS monitoring, constitutes however a 'search' within the meaning of this Amendment if it is used to follow and localize someone at all places, also non-public ones like someone's home.³⁸² This was decided in the Karo case, where the placement of an electronic beeper device to monitor and follow a can of ether was considered to be a 'search'.³⁸³ The discussion about whether or not the placement of a GPS monitoring system on a car that drives on public streets consists of a 'search' was finally decided in *United States v. Jones*.³⁸⁴ In this case, the court stated that since a car is someone's private property, and the placement of a GPS device on that car consists of an intrusion of that person's privacy, this

³⁸¹ Fourth Amendment to the United States Constitution, 15 December 1791; *United States v. Knotts*, 460 U.S. 276 (1983); *Osborn v. Nevada*, 118 Nev. 323 (Nev. 2002); *United States v. Smith*, 387 Fed.Appx. 918 (11th Cir. 2010); *United States v. Marquez*, 605 F.3d 604 (8th Cir. 2010); J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 739-743; H. FUSON, "Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State", *The University of Memphis law review* 2020, Vol.50(1), (231) 262-263; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 538-540; E.W. MARSHALL *et al.*, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; M. RADLER, "Privacy is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1228; M.A. WASSERMAN, "First Amendment limitations on police surveillance: The case of the Muslim surveillance program", *New York University Law Review* 2015, Vol.90(5), (1786) 1810-1811.

³⁸² *Osborn v. United States*, 385 U.S. 323 (1966); *Katz v. United States*, 389 U.S. 347 (1967); *United States v. White*, 401 U.S. 745 (1971); *United States v. Karo*, 468 U.S. 705 (1984); J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 733-743; H. FUSON, "Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State", *The University of Memphis law review* 2020, Vol.50(1), (231) 262-263 and 272; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 538-540; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1010; E.W. MARSHALL *et al.*, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 55 and 194; J.E. ROSS, "Valuing inside knowledge: Police infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 512.

³⁸³ *United States v. Karo*, 468 U.S. 705 (1984).

³⁸⁴ *United States v. Jones*, 132 S.Ct. 945 (2012); J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 739-743; H. FUSON, "Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State", *The University of Memphis law review* 2020, Vol.50(1), (231) 262-263; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 544-545; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1010; E.W. MARSHALL *et al.*, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; M. RADLER, "Privacy is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1211.

consists of a ‘search’ within the meaning of the Fourth Amendment and is therefore protected.³⁸⁵

The duration of the surveillance, with the exception of physical in person surveillance conducted by the FBI explained above, also plays an important role in determining whether or not a warrant is required.³⁸⁶ In *United States v. Maynard*, the court stated that “a whole is different from the sum of its individual parts (the mosaic theory)” and “the whole of one’s movements over the course of a month is not constructively exposed to the public because ... the whole reveals far more than the individual movements it comprises”.³⁸⁷ The court therefore decided that the suspect “had a subjective expectation of privacy in his travels over the time when he was monitored because the district court has found that even outside of the home, the Fourth Amendment secures for each individual a private enclave, a zone bounded by the individual’s won reasonable expectation of privacy”.³⁸⁸ Monitoring devices are therefore allowed to use for surveillance purposes, but a distinction will be made between their short-term (no warrant required) and long-term (warrant required) use.³⁸⁹ Since the use of technical resources such as a GPS monitoring system or wiretap will always require a warrant, this will mostly be decisive for obtaining information such as cell phone location data. Cell-site location information (CSLI) is generated each time a phone connects to a cell site.³⁹⁰ Modern devices like smartphones are designed to connect to cell sites multiple times, even if they are not being

³⁸⁵ Fourth Amendment to the United States Constitution, 15 December 1791; *United States v. Jones*, 132 S.Ct. 945 (2012); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 739-743; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 544-545; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1010; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; M. RADLER, “Privacy is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance”, *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1211.

³⁸⁶ *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 742-743; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 542-547; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-754; M. RADLER, “Privacy is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance”, *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1213-1214 and 1229-1236.

³⁸⁷ *Ibid.*

³⁸⁸ *Ibid.*

³⁸⁹ T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 545-547; M. RADLER, “Privacy is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance”, *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1213-1214 and 1229-1236.

³⁹⁰ *Carpenter v. United States*, No. 16–402, 585 U.S. (2018).

used by their owners.³⁹¹ In the Carpenter case, the Supreme Court decided that government's access to historical cell phone records that provide a comprehensive chronicle of the user's past movements consists of a 'search' and is therefore protected by the Fourth Amendment.³⁹² What the exact demarcation is between short-term and long-term has however not been clarified by the court.³⁹³ The main criterion in order to decide whether the time of surveillance might trigger the requirement of a warrant is whether the surveilled person could have a reasonable expectation of privacy for that period of time.³⁹⁴ Based on the discussions in this case law, the demarcation period seems to be situated somewhere around seven consecutive days.

The Carpenter case shows a nice combination of the Karo and Jones cases on the one hand and the Maynard case on the other hand. The Karo and Jones cases assessed the use of new technical resources by law enforcement during surveillance operations. In the Carpenter case, the use of CSLI was assessed as a new technical resource. The Maynard case dealt with the period during which law enforcement may surveil a person of interest without obtaining a warrant. Given the combination of the extensive period of time (127 days) on the one hand and the detailed location information provided by CSLI on the other hand, this situation was indeed well-decided to be a 'search' under the Fourth Amendment and requires as a consequence a warrant.

Before electronic surveillance of a suspect can be requested, the U.S. Department of Justice Electronic Surveillance Title III Affidavits require "a detailed discussion of the other investigative procedures", including police infiltration, "that have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ. It need not be shown that no other investigative avenues are available, only that they have been tried and proven inadequate or have been considered and rejected for reasons described".³⁹⁵ It must also be shown that there is probable cause for requesting this measure.³⁹⁶

³⁹¹ *Ibid.*

³⁹² *Ibid.*

³⁹³ T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 547; M. RADLER, "Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1213-1214 and 1236.

³⁹⁴ *Ibid.*

³⁹⁵ 18 United States Code (U.S.C.) §2518 (1)(c); U.S. DEPARTMENT OF JUSTICE, 29. *Electronic Surveillance—Title III Affidavits*, 2018, <https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits>; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 55; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120.

³⁹⁶ 18 U.S.C. §2518 (1)(d); U.S. DEPARTMENT OF JUSTICE, 29. *Electronic Surveillance—Title III Affidavits*, 2018, <https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits>; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 512.

§3. Legal framework on systemic police observation compared

The legal framework on systemic police observation is in Belgium as well as in the United States regulated by law. A distinction is made between regular in person surveillance and electronic surveillance. The use of technical resources during surveillance operations is in both countries considered to be more privacy invasive and therefore additional requirements are set forth. In the United States, this is categorized as a ‘search’ which is protected by the Fourth Amendment’s right to privacy and requires a warrant. In Belgium, art. 47*sexies*, §2 Sv. provides a proportionality requirement for this type of surveillance. Both countries require prior authorization in case law enforcement wants to wiretap someone else’s communication and there are sanctions if this requirement will not be fulfilled. Authorization will in Belgium as well as in the United States only be granted if probable cause will be established in order to justify the employment of this investigation technique. The Belgian Criminal Code states that these sanctions also apply to police officers that have gathered and processed information resulting from a surveillance operation without the necessary authorization. In the United States, it is also prohibited for law enforcement to unduly violate a person of interest’s constitutional privacy rights.

A difference between both countries can be identified for long-term in person surveillance. The FBI is allowed to surveil a suspect for an unlimited amount of time based on a predicated reason without a warrant. In Belgium, systemic police observation of “more than five consecutive days or of more than five non-consecutive days spread over a period of one month” requires a warrant. The logic behind this exception in the United States is that firstly a predicated reason is required and secondly in person surveillance is very human and energy intensive. The FBI will based on its experience only be able to conduct this type of surveillance for a limited amount of time and will only initiate this in well-founded situations. This contradicts however the ‘reasonable expectation of privacy’ which emerges after a period of approximately seven days. The Belgian legal system provides therefore a better protection for potential suspects in these situations and is as a consequence preferable.

The idea of the US reasonable expectation of privacy can be found in the Belgian regulation as well. The main reason why in Belgium for systemic police observation a duration of five consecutive days or of more than five non-consecutive days spread over a period of one month is required, is in order to be able to recognize patterns in someone’s life. This is often also the

aim of the use of technical resources during a long-term surveillance operation. When these characteristics can be established, the observation will most likely aim at gaining insight in someone's private life. This goes further than a single observation in public, which as such does not reveal much about a person's private life. Traces of the idea of the US reasonable expectation of privacy can therefore also be found in the Belgian regulation of systemic police observation.

In the previous part, the subsidiarity and proportionality principles were discussed for the investigation technique of police infiltration (*Part III, Chapter 4, §1 and §2*). These principles are for systemic police observation also used in a reversed way, however, in the exact opposite way as for police infiltration. Systemic police observation is in the United States considered to be more Fourth Amendment's privacy invasive than police infiltration and can therefore only occur based on a warrant. In Belgium on the contrary, police infiltration is considered to be more privacy invasive than systemic police observation.

Chapter 2: Legal framework on systemic police observation in the digital age

§1. General legal framework on systemic police observation in the digital age

Due to the technological development, surveillance equipment has become smaller, easier to hide and has the capability of delivering much higher audio and/or visual quality.³⁹⁷ Surveillance can secretly take place from a remote distance with remote-controlled and self-activated devices which make it easier to observe and record a suspect's behavior, in real life as well as on social media.³⁹⁸ In this paragraph, the general legal framework on police surveillance operations in the digital age will be discussed.

a) Belgian general legal framework on systemic police observation in the digital age

One of the main issues of Belgian criminal and criminal procedural law is that it is largely outdated and still mainly focused on crimes committed in the real world.³⁹⁹ As a consequence,

³⁹⁷ United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 744; D.A. DRIPPS, "At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense", *University of Illinois Law Review* 1993, Vol.2, (261) 274; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1010; G.T. MARX, "Who really gets stung? Some issues raised by the New Police Undercover Work", *Crime & Delinquency* 1982, Vol.28(2), (165) 168 and 192-193; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 55-56 and 211-214; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 370; M. RADLER, "Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1218.

³⁹⁸ United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 744; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 95; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 538-539; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1010; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 55-56 and 211-214; G.T. MARX, "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues* 2003, Vol.59(2), (369) 370; M. RADLER, "Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance", *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1218.

³⁹⁹ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 62-63; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 205-213 and 227; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 333; E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 12.

law enforcement has to be creative and adapt the real world legislation to virtual world situations.⁴⁰⁰ One of the principles for doing this is offline = online.⁴⁰¹ Where possible, the police will try to find similarities and apply the existing legislation to similar situations off- and online.⁴⁰² In contrast to the investigation technique of police infiltration, systemic police observation did not receive its own online version in the Belgian Code of Criminal Procedure (Sv.).⁴⁰³ There are only general provisions that allow the police to perform tasks of observation, which can be found in art. 47sexies Sv. (*Part IV, Chapter 1, §1*) and art. 26 WPA (*Part IV, Chapter 2, §2, a*).⁴⁰⁴

In case law enforcement decides to check someone's Facebook page and gather information from it, it will depend on the type of information (publicly available or not) and the amount of times that this occurs whether this can be considered as accessing publicly available

⁴⁰⁰ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 62-63; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 205-213 and 227; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 333; E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 12; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 390.

⁴⁰¹ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 62-63; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 213 and 228; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 333; E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 12; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 390.

⁴⁰² *Ibid.*

⁴⁰³ Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, "Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche", *Juristenkrant* 2017, Vol.351, (3) 3; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261.

⁴⁰⁴ Art. 47sexies Sv., *BS* 27 November 1808; art. 26 WPA, *BS* 22 December 1992; Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 218; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, "Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche", *Juristenkrant* 2017, Vol.351, (3) 3; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 391 and 403.

information, systemic police observation or police infiltration.⁴⁰⁵ Gathering information through the consequent observation of a person's Facebook page or public tweets can for example according to art. 47*sexies*, §1 Sv. be categorized under "an observation of more than five consecutive days or of more than five non-consecutive days spread over a period of one month" or under "an observation during which technical resources are used", and will therefore constitute of systemic police observation which is subject to the more strict SIM rules (*Part IV, Chapter 1, §1*).⁴⁰⁶ If the publicly accessible information on someone's Facebook page will only be accessed and gathered occasionally, this will be considered as the regular police authority to check whether law and order is being maintained (*Part IV, Chapter 2, §2, a*).⁴⁰⁷ If the gathered information will consist of non-publicly accessible information, a warrant will be required (*Part IV, Chapter 2, §3, a*).⁴⁰⁸

Sometimes, it is sufficient for law enforcement to adopt a nickname in order to access public chatting channels without joining the conversation or to receive an automatic invitation link without providing any personal information in order to login to a webpage. These situations are considered to be online observation in a publicly accessible place.⁴⁰⁹ Law enforcement can

⁴⁰⁵ C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 332; E. DE PAUW, "Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?", *Orde van de dag* 2010, Vol.3, (5) 13; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 999; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 260.

⁴⁰⁶ Art. 47*sexies*, §1 Sv., *BS* 27 November 1808; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 223-224; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 333; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 262-270.

⁴⁰⁷ Art. 26 WPA, *BS* 22 December 1992; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 403.

⁴⁰⁸ L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 65; H. BERKMOES, "Identificatie van (gebruikers van) elektronische communicatie" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, (3/01) 3/01 and 3/37-3/42; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

⁴⁰⁹ Art. 26 WPA, *BS* 22 December 1992; Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; Antwerp 10 November 2016, *Limb.Rechtsl.* 2018, Vol.2, 132; L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 64; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 215-224; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, "Cassatie vult wettelijke leemte op over

surveil the internet (including the darknet) using a nickname as long as it is not provocative, not credible and when only formal (not personal) access conditions are required.⁴¹⁰ The main distinctive criterion between online police infiltration and online systemic police observation is therefore whether personal information has to be provided or not (*Part III, Chapter 3, §1*).

b) US general legal framework on systemic police observation in the digital age

In the United States, law enforcement may also monitor publicly available information on social media, such as people's social interactions and political involvement.⁴¹¹ However, certain sensitive investigative matters cannot be used as the only basis for justifying an FBI investigation, such as religious or domestic political involvement or the news media (*Part III, Chapter 1, §2, b*).⁴¹² A predicated reason will be required on top of this.⁴¹³ Law enforcement may passively observe real time publicly accessible electronic communications under the same circumstances as when they would attend a public meeting.⁴¹⁴ This social media monitoring

politiezone internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264-265; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 391.

⁴¹⁰ Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; Antwerp 10 November 2016, *Limb.Rechtsl.* 2018, Vol.2, 132; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politiezone internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3.

⁴¹¹ E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 322; A. DIAZ, *New York City Police Department Surveillance Technology*, New York, New York University School of Law, 2019, 4; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 525; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 999.

⁴¹² U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 10 Sensitive Investigative matter and Sensitive Operations Review Committee*, 2016, [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view, 10/1](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,10/1).

⁴¹³ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 6.5 Predication & 10.1.3 Factors to Consider When Opening or Approving an Investigative Activity Involving a SIM & 10.1.4 Opening Documentation, Approval, Notice, Change in SIM Status, and Sensitive Potential CHS or Sensitive Characteristic Designations in Type 5 Assessments*, 2016, [https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view, 6/3 and 10/3-10/10](https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,6/3and10/3-10/10).

⁴¹⁴ THE ONLINE INVESTIGATIONS WORKING GROUP, *Online investigative principles for federal law enforcement agents*, 1999, <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>, ix; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 18.5.1 Investigative Method: Public Information (“Publicly Available Information”)*, 2016, <https://vault.fbi.gov/FBI%20Domestic>

can occur in three different forms: 1) online following or watching an identified individual, group of individuals, or affiliation; 2) making use of an informant in order to obtain information, this can be a friend of the target (civilian or law enforcement official) or an undercover agent, or; 3) making use of analytical software in order to generate data about individuals, groups, associations, or locations.⁴¹⁵ In this chapter, the first form, namely the online following or watching of a person of interest, will be discussed. The second form, where an informant is used in order to obtain information, has been discussed in Part III, Chapter 3, §2. The third form consisting of the use of analytical software will not be addressed in this research.

c) General legal framework on systemic police observation in the digital age compared

The general legal framework on online systemic police observation is similar in Belgium and in the United States. The online version of this investigation technique is in both countries largely unregulated and therefore the principle of offline = online is being applied. The general provisions that allow (systemic) police observation in public spaces in the real world are used in and translated to the virtual world. Information that is publicly available in the virtual world can as a consequence be accessed and monitored under the same conditions as someone's behavior or movements in public places in the real world.

§2. Online publicly accessible information: legal framework

In today's society, social media is playing a central role in the social relations, political involvement and economic transactions of individuals.⁴¹⁶ Some people post this personal

%20Investigations%20and%20Operations%20Guide%20%28DI0G%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DI0G%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DI0G%29%202016%20Version%20Part%2001%20of%2002/view, 18/6.

⁴¹⁵ E. DE BONO, "Investigating Social Networking Sites" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 322; A. DIAZ, *New York City Police Department Surveillance Technology*, New York, New York University School of Law, 2019, 4; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 246; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 526; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 999-1000.

⁴¹⁶ E. DE BONO, "Investigating Social Networking Sites" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 315 and 325;

information on social media in a public way, making it available to anyone who accesses their webpage. In this paragraph, the legal framework on this type of online publicly accessible information will be discussed.

a) Belgian legal framework on online publicly accessible information

Belgian law enforcement can observe publicly accessible information, such as public tweets, Facebook status updates or YouTube videos, in accordance with the legal framework for gathering information from publicly accessible platforms.⁴¹⁷ Art. 26 WPA (Wet op het Politieambt; Belgian law on law enforcement) discusses only offline publicly accessible information, and since a specific online version of this article is still lacking, it is being used by analogy in the virtual world (*Part IV, Chapter 2, §1, a*).⁴¹⁸ According to this article, “law enforcement can enter publicly accessible places in order to check whether law and order is being maintained and whether the local laws and regulations are being respected”.⁴¹⁹ However, if a person’s Facebook page or public tweets will be observed for more than five consecutive days or for more than five non-consecutive days spread over a period of one month, a warrant will be required based on art. 47*sexies*, §1 and §3 Sv. (*Part. IV, Chapter 2, §1, a*). There is a difference between accessing publicly available information and storing this information in a systemic way.⁴²⁰ For the latter, a reasonable suspicion of involvement in a criminal offense should be present.⁴²¹ This is in accordance with the Belgian privacy law which requires legality,

E. DE PAUW, “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, (5) 5-6; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 525.

⁴¹⁷ M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 403.

⁴¹⁸ Art. 26 WPA, *BS* 22 December 1992; Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 65; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 331-332; F. SCHUERMANS, “Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, (3) 3; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390-391 and 403.

⁴¹⁹ Art. 26 WPA, *BS* 22 December 1992.

⁴²⁰ M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261-262.

⁴²¹ *Ibid.*

correctness, accuracy and purpose limitation.⁴²² Moreover, it is only possible to use the collected data for the purposes for which they were initially gathered.⁴²³

b) US legal framework on online publicly accessible information

When a person has a public account on Facebook, Instagram or Twitter, it is possible for anyone, including law enforcement, who types that person's name into a search engine to view the information posted on that account.⁴²⁴ This type of 'online' police surveillance, where law enforcement monitors suspects on social media without the use of undercover agents, can also in the United States be considered very analogous to its 'offline' version.⁴²⁵ Police officers may therefore obtain information from publicly accessible online sources under the same conditions as from other sources that are generally open to the public.⁴²⁶ One can sometimes find very detailed information on someone's online profile about his life and (daily) activities.⁴²⁷ Law enforcement is also allowed to use widely available software tools for obtaining publicly available identifying information about a user or a host computer under the same circumstances as they are permitted to look up similar identifying information, like a telephone number, by non-electronic means.⁴²⁸ This publicly available information is not protected by the Fourth Amendment's right to privacy nor by the Katz ruling (*Part V, Chapter 1, §2*) on the evolution

⁴²² Art. 28 wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 September 2018; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261.

⁴²³ M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 261.

⁴²⁴ E. DE BONO, "Investigating Social Networking Sites" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 322; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 526.

⁴²⁵ R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 533.

⁴²⁶ THE ONLINE INVESTIGATIONS WORKING GROUP, *Online investigative principles for federal law enforcement agents*, 1999, <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>, viii; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 18.5.1 Investigative Method: Public Information ("Publicly Available Information")*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,18/6>.

⁴²⁷ R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 527.

⁴²⁸ THE ONLINE INVESTIGATIONS WORKING GROUP, *Online investigative principles for federal law enforcement agents*, 1999, <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>, viii.

of the concept of privacy, since it falls under the third party doctrine (*Part IV, Chapter 2, §3, b*)).⁴²⁹

The New York City Police Department has for example a specialized Intelligence Division whose main task is to monitor and anticipate large-scale events and criminal activity, and to assist other units during criminal investigations.⁴³⁰ They may analyze how and with whom members of youth gangs interact on social media.⁴³¹ Even hitting the ‘like’ button or sharing a specific comment can attract the attention of law enforcement.⁴³² In contrast to regular offline police surveillance, police officers do not have to be in close proximity to a suspect.⁴³³ They can ‘follow’ and monitor a suspect on social media in a largely undetected way.⁴³⁴

c) Legal framework on online publicly accessible information compared

There is no specific legal framework on online publicly accessible information in Belgium as well as in the United States. Therefore, also in this case the main rule of offline = online is applied, and the existing offline regulation is interpreted in an online way. Law enforcement is allowed to enter publicly accessible places in order to check whether the law is being respected, and this can also be applied and translated to online publicly accessible places like online available information on social media.

The example of the monitoring authority of the New York City Police Department shows however a difference with the Belgian approach. Online publicly accessible information on for example social media is in the United States not protected by the Fourth Amendment’s right to privacy. The US legal system reasons that once someone makes information publicly available, he renounces his right to privacy for that information (*Part V, Chapter 1, §2*). In Belgium, the consistent monitoring of this type of online publicly accessible information can be qualified as systemic police observation (*Part IV, Chapter 2, §1, a*) and law enforcement will have to obtain

⁴²⁹ Fourth Amendment to the United States Constitution, 15 December 1791; P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 703.

⁴³⁰ R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 527.

⁴³¹ A. DIAZ, *New York City Police Department Surveillance Technology*, New York, New York University School of Law, 2019, 4; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 527.

⁴³² R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 529.

⁴³³ R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 534.

⁴³⁴ *Ibid.*

a warrant if they want to proceed with this type of monitoring. Moreover, if this information will be systemically stored by Belgian law enforcement, a reasonable suspicion of involvement in a criminal offense will have to be proven. Online publicly accessible information that is being monitored in a systemic way can therefore be considered more protected in Belgium than in the United States.

§3. Online non-publicly accessible information: legal framework

a) Belgian legal framework on online non-publicly accessible information

The gathering and processing of non-publicly accessible information is a more sensitive issue and can therefore only occur based on a warrant issued by the Crown prosecutor or the investigating judge.⁴³⁵ This authority can be found in art. 46*bis* Sv., which states that the Crown prosecutor can request this information directly from social media providers and operators.⁴³⁶ However, in these situations only data for identifying the people involved can be requested, but not the content of their communication.⁴³⁷ In case the police would also like to track down and localize the content of their communication or place a wiretap (including for internet communication), they will first have to obtain a warrant from the investigating judge based on

⁴³⁵ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 65; H. BERKMOES, “Identificatie van (gebruikers van) elektronische communicatie” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, (3/01) 3/01 and 3/37-3/42; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

⁴³⁶ Art. 46*bis* Sv., BS 27 November 1808; MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001, 10 and 32-34; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 65; H. BERKMOES, “Identificatie van (gebruikers van) elektronische communicatie” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, (3/01) 3/01 and 3/33-3/42; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 208-209; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 118-120; M. VERMEULEN and P. DE HERT, “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

⁴³⁷ *Ibid.*

art. 88*bis* and 90*ter* Sv.⁴³⁸ The investigating judge also has the possibility to issue a warrant for a more broad network search based on art. 88*ter* Sv.⁴³⁹

A network search makes it possible to obtain information from another network than the one which is located in the place that is being searched, like a search of the suspect's activities on Facebook or Skype, even though these companies store their data in the United States.⁴⁴⁰ The Belgian legislation is very progressive in allowing this, but some countries may see this as an infringement of their sovereignty and therefore refuse to cooperate.⁴⁴¹ The social media

⁴³⁸ Art. 88*bis* and 90*ter* Sv., BS 27 November 1808; Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26; L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 65; H. BERKMOES, "Identificatie van (gebruikers van) elektronische communicatie" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, (3/01) 3/33-3/39 and 3/48; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 209; C. CONINGS and S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 120-124; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263.

⁴³⁹ Art. 88*ter* Sv., BS 27 November 1808; GwH 6 December 2018, nr. 174/2018, BS 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; L. BEIRENS, "De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace", *Orde van de dag* 2010, Vol.3, (51) 65; H. BERKMOES, "Identificatie van (gebruikers van) elektronische communicatie" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, (3/01) 3/33-3/39; C. CONINGS and S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 105-114 and 125; C. CONINGS, "Wetgever maakt digitaal spoorwerk makkelijker", *Juristenkrant* 2017, Vol.19, (3) 3; C. CONINGS, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr.* 2019, Vol.5, (257) 257-258; S. ROYER, "Wet 25 december 2016 digitaal spoorwerk op twee punten vernietigd (noot onder GwH 6 december 2018)", *NJW* 2019, Vol.398, (212) 212; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 263; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 394.

⁴⁴⁰ Corr. Antwerp 27 October 2016, *Computerr.* 2017, Vol.1, 35, *Juristenkrant* 2016, Vol.337, 4, *NJW* 2016, Vol.353, 921, *NC* 2017, Vol.1, 89, *TRNI* 2017, Vol.1, 91; C. CONINGS and S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" in *Topics bewijs- en procesrecht*, Morsel, Intersentia, 2017, (99) 105-106; C. CONINGS, "Wetgever maakt digitaal spoorwerk makkelijker", *Juristenkrant* 2017, Vol.19, (3) 3; C. CONINGS, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr.* 2019, Vol.5, (257) 258; S. ROYER, "Medewerkingsplicht van een telecommunicatiedienst", *NJW* 2016, Vol.353, (928) 928-929; S. ROYER, "Wet 25 december 2016 digitaal spoorwerk op twee punten vernietigd (noot onder GwH 6 december 2018)", *NJW* 2019, Vol.398, (212) 212; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 394.

⁴⁴¹ Corr. Antwerp 27 October 2016, *Computerr.* 2017, Vol.1, 35, *Juristenkrant* 2016, Vol.337, 4, *NJW* 2016, Vol.353, 921, *NC* 2017, Vol.1, 89, *TRNI* 2017, Vol.1, 91; S. ROYER, "Medewerkingsplicht van een telecommunicatiedienst", *NJW* 2016, Vol.353, (928) 928-929; M. VERMEULEN and P. DE HERT, "Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (258) 264.

providers have however in both cases a duty of cooperation and can be fined in case they would refuse to cooperate.⁴⁴²

The law of November 28, 2000 changed the Dutch word ‘telephone tapping’ (used for wiretapping) into ‘information tapping’ in art. 90ter Sv. in order to adapt it to the virtual world.⁴⁴³ Since only the wording was changed and not the definition, information tapping was still only allowed for real time communication ‘in transfer’, and therefore continued to cause problems in the virtual world.⁴⁴⁴ Online messages are being sent and received, and could therefore not be wiretapped if the recipient had already read the message, since the message had then already been ‘delivered’ and was not anymore ‘in transfer’.⁴⁴⁵ This article was therefore modernized in 2016, and makes it now possible to access, search and record non-publicly accessible communication or data on computer systems while making use of technical resources.⁴⁴⁶ As a consequence, it is now possible for law enforcement to (secretly) access data on laptops and smartphones in order to search them or monitor a suspect’s conversations on them.⁴⁴⁷

⁴⁴² Corr. Antwerp 27 October 2016, *Computerr.* 2017, Vol.1, 35, *Juristenkrant* 2016, Vol.337, 4, *NJW* 2016, Vol.353, 921, *NC* 2017, Vol.1, 89, *TRNI* 2017, Vol.1, 91; H. BERKMOES, “Identificatie van (gebruikers van) elektronische communicatie” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, (3/01) 3/35 and 3/44-3/45; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 209 and 225-226; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 118-125; S. ROYER, “Medewerkingsplicht van een telecommunicatiedienst”, *NJW* 2016, Vol.353, (928) 928-929.

⁴⁴³ Art. 90ter, §1 Sv., *BS* 27 November 1808; C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 222-223; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 112-114; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333.

⁴⁴⁴ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 222-223; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 112-114.

⁴⁴⁵ C. CONINGS and P. VAN LINTHOUT, “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 222-223.

⁴⁴⁶ Art. 90ter, §1 Sv., *BS* 27 November 1808; art. 17 wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS* 17 January 2017; C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 112-114; C. CONINGS, “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, (331) 333; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 398.

⁴⁴⁷ C. CONINGS and S. ROYER, “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 112.

b) US legal framework on online non-publicly accessible information

Information that is ‘private’ on social media can also in the United States be accessed by law enforcement, but the line between police surveillance and police infiltration becomes more complex in this case.⁴⁴⁸ Online sources with restricted access can be made available to law enforcement, but only based on a warrant permitting entry into private space.⁴⁴⁹ There is a difference between the content of online communication and the sole location of where that communication took place or the people involved in it. The content of online communication can only be accessed by law enforcement based on a warrant, since it is protected by the privacy right of the Fourth Amendment.⁴⁵⁰ The location where that communication took place and the data about the people involved in it are not considered to be private and are therefore not protected by the Fourth Amendment.⁴⁵¹ A subpoena suffices in order to obtain this so-called metadata.⁴⁵² The FBI’s internal DIOG specifies for the FBI that this can moreover only be requested within the context of one of the three investigations (*Part III, Chapter 2, §2*).⁴⁵³ This analysis is made by analogy with the Jackson ruling, where the court stated that the content of a letter is private, but “the outward form and weight of those mailings including the recipient’s name and physical address are not constitutionally protected”.⁴⁵⁴

⁴⁴⁸ R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 541.

⁴⁴⁹ Fourth Amendment to the United States Constitution, 15 December 1791; 18 U.S.C. §2703 (a); THE ONLINE INVESTIGATIONS WORKING GROUP, *Online investigative principles for federal law enforcement agents*, 1999, <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>, ix; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1000.

⁴⁵⁰ *Ibid.*

⁴⁵¹ Fourth Amendment to the United States Constitution, 15 December 1791; *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016).

⁴⁵² 18 U.S.C. §2703 (c)(2); T. BREWSTER, *Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops*, <https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/> (consultation 20 May 2021); OFFICE OF THE INSPECTOR GENERAL, *A Review of the Drug Enforcement Administration’s Use of Administrative Subpoenas to Collect or Exploit Bulk Data*, <https://oig.justice.gov/reports/2019/o1901.pdf>, i-ii (consultation 20 May 2021).

⁴⁵³ U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 18.5.9 Investigative Method: Grand Jury Subpoenas – To Providers of Electronic Communication Services or Remote Computing Services for Subscriber or Customer Information & 18.6.8 Investigative Method: Stored Wire or Electronic Communications and Transactional Records*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view,18/55-18/57> and 18/125-18/137.

⁴⁵⁴ *Ex parte Jackson*, 96 U.S. 727 (1878); *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016).

The police can also ask a Facebook or Twitter friend of the suspect to show or share the information on the suspect's profile with them.⁴⁵⁵ The court acknowledged that when a social media user activates his privacy settings, this shows his intent to preserve that information as private, and this could be protected under the Fourth Amendment.⁴⁵⁶ According to the third party doctrine, this legitimate expectation of privacy ends however when someone shares that information with his (virtual) 'friends', since they are free to use this 'private' information in any way they want, which includes sharing it with government officials.⁴⁵⁷ The use of an informant by the government to gain access to initially private information can therefore not be considered a violation of the Fourth Amendment.⁴⁵⁸ The intention to keep information strictly private is as a consequence still considered as a prerequisite for the rights protected by this

⁴⁵⁵ United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); THE ONLINE INVESTIGATIONS WORKING GROUP, *Online investigative principles for federal law enforcement agents*, 1999, <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>, x-xi; E. DE BONO, "Investigating Social Networking Sites" in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 322; K. HEATHER, *Police embrace social media as crime-fighting tool*, <https://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html> (consultation 18 November 2020); R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 541-547.

⁴⁵⁶ Fourth Amendment to the United States Constitution, 15 December 1791; United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 547; M.A. WASSERMAN, "First Amendment limitations on police surveillance: The case of the Muslim surveillance program", *New York University Law Review* 2015, Vol.90(5), (1786) 1810-1811.

⁴⁵⁷ United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 199; K. HEATHER, *Police embrace social media as crime-fighting tool*, <https://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html> (consultation 18 November 2020); W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 39-40 and 82-87 and 108; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 547; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1009; E.W. MARSHALL *et al.*, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 753; P. ROSENZWEIG, "Civil Liberty and the Response to Terrorism", *Duquesne Law Review* 2004, Vol.42(4), (663) 675-676; M.A. WASSERMAN, "First Amendment limitations on police surveillance: The case of the Muslim surveillance program", *New York University Law Review* 2015, Vol.90(5), (1786) 1810-1811.

⁴⁵⁸ Fourth Amendment to the United States Constitution, 15 December 1791; United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 199; K. HEATHER, *Police embrace social media as crime-fighting tool*, <https://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html> (consultation 18 November 2020); W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 4 and 39-40 and 82-87 and 108 and 116-121; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 547; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1009; E.W. MARSHALL *et al.*, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 753; P. ROSENZWEIG, "Civil Liberty and the Response to Terrorism", *Duquesne Law Review* 2004, Vol.42(4), (663) 675-676.

Amendment.⁴⁵⁹ If law enforcement agents however decide to create a fake profile and try to become themselves ‘friends’ with a suspect in order to gain access to the ‘private’ information on his profile, this will be considered as online police infiltration (*Part III, Chapter 3, §2*).⁴⁶⁰

c) Legal framework on online non-publicly accessible information compared

In both Belgium and the United States, online non-publicly accessible information can only be gathered and processed by law enforcement based on a warrant authorizing entry into private space. In Belgium, this warrant can be issued by the Crown prosecutor if the police only wants to obtain information about the identity of the people involved in the communication. If Belgian law enforcement agents also want to localize or get to know the content of the communication, only the investigating judge will be authorized to issue such a warrant. In the United States, a warrant is only required to obtain the content of the communication, whereas location information and identifying data for the people involved (also called metadata) can be obtained by a subpoena. Communication’s metadata is therefore better protected in Belgium than in the United States.

In both countries, the line between the investigation techniques of systemic police observation and police infiltration becomes less clear in situations where online non-publicly available information is being accessed. Especially when law enforcement decides to make use of an informant who is a state official to obtain this type of information, the investigation technique will rather be considered to be police infiltration than systemic police observation.

⁴⁵⁹ W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 48 and 60-61; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 548; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 753; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1810-1811.

⁴⁶⁰ E. DE BONO, “Investigating Social Networking Sites” in T.G. SHIPLEY and A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, (315) 322; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 541; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 999.

Part V: Privacy, fair trial and freedom of speech

In the previous parts, the investigation methods of (online) police infiltration and (online) systemic police observation were discussed for Belgium and the United States. In this part, these investigation techniques will be balanced with the right to privacy, the right to a fair trial and the freedom of speech. The right to privacy, trial rights, freedom of association and other civil liberties are in the United States protected by the Bill of Rights and can be endangered by undercover and surveillance operations.⁴⁶¹

These rights are in Europe guaranteed by respectively art. 8, 6 and 10 of the European Convention on Human Rights (ECHR).⁴⁶² Given the harmonizing impact of decisions made by the European Court of Human Rights (ECtHR) on many European national Codes of Criminal Procedure, the ECHR and some decisions of the ECtHR will also be discussed in the chapters on the Belgian regulation.⁴⁶³ The right to privacy and freedom of speech are moreover also protected by article 19, 22, 25 and 150 of the Belgian Constitution.⁴⁶⁴ Undercover and surveillance operations may after all come into conflict with the right to privacy, the right to a fair trial and sometimes even with the freedom of speech.⁴⁶⁵

⁴⁶¹ First, Fourth and Fifth Amendment to the United States Constitution, 15 December 1791; Fourteenth Amendment to the United States Constitution, 9 July 1868; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 54-61; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 524; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 147; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-249 and 264.

⁴⁶² Art. 6, 8 and 10 European Convention on Human Rights (ECHR), BS 19 August 1955; ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 152; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

⁴⁶³ J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 262; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2865; K. SCHEPPELE, "Other People's Patriot Acts: Europe's Response to September 11", *Loyola Law Review* 2004, Vol.50(1), (89) 139.

⁴⁶⁴ Art. 19, 22, 25 and 150 Grondwet (Gw.), BS 17 February 1994.

⁴⁶⁵ ECtHR 16 February 2000, nr. 27052/95, Jasper/United Kingdom, *Juristenkrant* 2000, Vol.5, 4, RW 2002-03, Vol.6, 233; ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 11; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 129; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 1; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of

Chapter 1: The right to privacy and (online) police infiltration / systemic observation

§1. Privacy vs. (online) police infiltration / systemic observation in Belgium and Europe

Many European courts accept that undercover operations infringe the right to privacy to a certain extent.⁴⁶⁶ The European Court of Human Rights is in general sceptic about its compatibility with art. 8 ECHR and requires therefore a legal basis for undercover operations, a warrant issued prior to initiating this investigation technique, and continuing oversight by the undercover agent's superiors.⁴⁶⁷ It has also acknowledged that undercover operations can only be used in cases of organized crime and terrorism (proportionality principle) and that no less intrusive investigation methods must seem to be sufficient in order to obtain the information or evidence necessary (subsidiarity principle).⁴⁶⁸

A similar regime is applicable to systemic police observation, for which the ECtHR has set forth the following conditions; a legal basis is required and has to specify "1) the criminal offenses for which a warrant can be issued; 2) the permissible duration of the surveillance, and;

California press, 1988, 147; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 239-241; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; A. THIENPONT, "Nieuwe BOM-wet legt bom onder fundamentele rechten en vrijheden", *Juristenkrant* 2006, Vol.1, (2) 2.

⁴⁶⁶ H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 266; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 390.

⁴⁶⁷ S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 112; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 152; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; K. SCHEPPELE, "Other People's Patriot Acts: Europe's Response to September 11", *Loyola Law Review* 2004, Vol.50(1), (89) 145-146.

⁴⁶⁸ Cass. 9 October 2013, *Arr.Cass.* 2013, Vol.10, 2061, *Pas.* 2013, Vol.10, 1903; H. BERKMOES, "Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)" in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/58-216/59; J. MEESE, "Bijzondere opsporingsmethoden en andere onderzoeksmethoden", *NJW* 2003, Vol.11, (1134) 1149-1150; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; A. THIENPONT, "Nieuwe BOM-wet legt bom onder fundamentele rechten en vrijheden", *Juristenkrant* 2006, Vol.1, (2) 2; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 390.

3) the limits on the purposes for which the results of the surveillance might be used”.⁴⁶⁹ The court has expressed its concern about situations where the suspect is not only occasionally observed, but when all the information of these different observations is put together and provides a full image of the suspect’s life.⁴⁷⁰ In that case, the observation is systemic and when it is moreover collected and stored in a police file, it may come into conflict with the right to privacy.⁴⁷¹ In the Rotaru case, the ECtHR decided that collecting and storing information on the suspect’s studies, political activities and criminal record in a systemic way constituted an interference with art. 8 ECHR.⁴⁷² Mr. Rotaru’s personal information was collected and stored by the Romanian Intelligence Services, but consisted of false information (e.g. that he studied at the Faculty of Sciences instead of the Faculty of Law, and that he was part of the legionnaire movement which was not the case) as a result of mistakenly confusing him with another person holding the same name. This practice of collecting and storing personal information is not per se prohibited as long as it is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society (*see below*). The first condition however does not only require that the measure should have a legal basis, but this legal basis “should also be accessible to the person concerned and foreseeable to its effects” and should therefore be clear and precise. Given the unlimited scope of application and the impreciseness of the law concerned in this case (no time limitations or conditions were provided as to what information could be collected and stored), art. 8 ECHR had been violated since it was not possible to predict or foresee the effects of the regulation concerned.⁴⁷³

The right to private life as guaranteed by art. 8 ECHR is however not absolute.⁴⁷⁴ It can be restricted when the measure is taken by a public authority, pursues a legitimate aim, is in

⁴⁶⁹ ECtHR 24 April 1990, Huvig/France, *Publ.Eur.CourtH.R.* 1990, Serie A, nr. 176-B; K. SCHEPPELE, “Other People’s Patriot Acts: Europe’s Response to September 11”, *Loyola Law Review* 2004, Vol.50(1), (89) 145-146.

⁴⁷⁰ ECtHR 4 May 2000, nr. 28341/95, Rotaru/Romania, *Rev.trim.DH* 2001, 137.

⁴⁷¹ *Ibid.*

⁴⁷² *Ibid.*

⁴⁷³ *Ibid.*

⁴⁷⁴ Art. 8 ECHR, BS 19 August 1955; ECtHR 24 April 1990, Huvig/France, *Publ.Eur.CourtH.R.* 1990, Serie A, nr. 176-B; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 106-107; B.-J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research” in B. AKHGAR and B. BREWSTER, *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Switzerland, Springer International Publishing, 2016, (3) 13-14; K. SCHEPPELE, “Other People’s Patriot Acts: Europe’s Response to September 11”, *Loyola Law Review* 2004, Vol.50(1), (89) 144-146; W. STOL, “Filteren van internet: een politietaak?”, *Orde van de dag* 2010, Vol.3, (43) 44.

accordance with the law (has a legal basis) and is necessary in a democratic society.⁴⁷⁵ This was also confirmed by the ECtHR in the *K.U. vs. Finland* case (*Part I, Chapter 3, §3*). Undercover operations and police surveillance may therefore interfere with the right to privacy as long as their legal framework complies with the requirements provided by paragraph 2 of art. 8 ECHR.

The Belgian regulation of online police infiltration is considered to be a ‘light’ version of the regulation of offline police infiltration, and its conformity with the right to privacy enshrined in art. 8 ECHR has already been acknowledged by the Belgian constitutional court.⁴⁷⁶ It has decided in its judgement of December 6, 2018 that the new investigation method of online police infiltration is in conformity with art. 8 ECHR, read together with art. 22 Gw. (Grondwet; Belgian Constitution) which also guarantees the right to privacy.⁴⁷⁷ In its reasoning, it focused mainly on the difference in physical danger that a real life and an online undercover agent have

⁴⁷⁵ Art. 8, §2 ECHR, *BS* 19 August 1955; ECtHR 21 June 1988, nr. 10730/84, *Berrehab/The Netherlands*, *Publ.Eur.CourtH.R.* 1988, Serie A, nr. 138; ECtHR 24 April 1990, *Huvig/France*, *Publ.Eur.CourtH.R.* 1990, Serie A, nr. 176-B; ECtHR 8 April 2003, nr. 39339/98, *M.M./The Netherlands*, *T.Strafr.* 2003, Vol.6, 288; ECtHR 8 July 2003, nr. 36022/97, *Hatton a.o./United Kingdom, Amén*. 2003, Vol.4, 239, *J.T.dr.eur.* 2003, Vol.101, 213, *MER* 2003, Vol.3, 271, *NJW* 2004, Vol.61, 228, *RW* 2004-05, Vol.12, 476; ECtHR 21 June 2011, nr. 30194/09, *Shimovolos/Russia*, *T.Strafr.* 2011, Vol.5, 360, *TVW* 2011, Vol.3, 263, *Vigiles* 2012, Vol.5, 446; ECtHR 17 April 2012, nr. 20071/07, *Piechowicz/Poland*; ECtHR 1 July 2014, nr. 43835/11, *S.A.S./France*, *Juristenkrant* 2014, Vol.295, 2, *RW* 2015-16, Vol.23, 916, *T.Strafr.* 2014, Vol.5, 328; ECtHR 23 February 2016, nr. 11138/10, *Mozer/Republic of Moldova and Russia*, *RW* 2016-17, Vol.36, 1436; H. BERKMOES, “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2019, (216/01) 216/10; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 106-107; B.-J. KOOPS, “Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research” in B. AKHGAR and B. BREWSTER, *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Switzerland, Springer International Publishing, 2016, (3) 13-14; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1134; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; K. SCHEPPELE, “Other People's Patriot Acts: Europe's Response to September 11”, *Loyola Law Review* 2004, Vol.50(1), (89) 144-146; W. STOL, “Filteren van internet: een politietaak?”, *Orde van de dag* 2010, Vol.3, (43) 44; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390.

⁴⁷⁶ GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; M. CHAWKI *et al.*, *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 106-107; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 402.

⁴⁷⁷ GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; W. YPERMAN, S. ROYER and F. VERBRUGGEN, “Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering”, *NC* 2019, Vol.5, (389) 390 and 402.

to face.⁴⁷⁸ Given that there is less physical danger for an online undercover agent, it justifies the more flexible regulation of online police infiltration compared to its offline counterpart.⁴⁷⁹

For the investigation technique of online systemic police observation, firstly a change in the legislation's wording from 'telephone tapping' into 'information tapping' was introduced and in a later stage also a change in its definition occurred.⁴⁸⁰ The ECtHR has however already made clear that in its opinion this type of information tapping is more capable of violating privacy rights than its telephone tapping predecessor, and that from a privacy rights' perspective it should therefore be more strictly regulated.⁴⁸¹ A smartphone that is being wiretapped contains nowadays much more information (photos, messages, conversations, contact details, documents etc.) than a telephone conversation that was being wiretapped in the past.

§2. Privacy vs. (online) police infiltration / systemic observation in the United States

The Bill of Rights was in the United States in the first place created to 'protect the people from the government'.⁴⁸² The right to privacy is enshrined in the Fourth Amendment and guarantees the right to be free from unreasonable searches and seizures by government officials.⁴⁸³ In the

⁴⁷⁸ GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40; W. YPERMAN, S. ROYER and F. VERBRUGGEN, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, (389) 402-410.

⁴⁷⁹ *Ibid.*

⁴⁸⁰ Art. 90ter, §1 Sv., *BS* 27 November 1808; C. CONINGS and P. VAN LINTHOUT, "Sociale media: Een nieuwe uitdaging voor politie en justitie", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), (205) 222-223; C. CONINGS and S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 112-114; C. CONINGS, "De politie op het darknet", *T.Strafr.* 2017, Vol.5, (331) 333.

⁴⁸¹ ECtHR 12 January 2016, nr. 37138/14, *Szabo and Vissy/Hungary*, *TVW* 2016, Vol.2, 159; C. CONINGS and S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, (99) 105.

⁴⁸² H. FUSON, "Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State", *The University of Memphis law review* 2020, Vol.50(1), (231) 257-258 and 285; E.W. MARSHALL *et al.*, "Police surveillance of cell phone location data: Supreme Court versus public opinion", *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752; C.E. SMITH, "The Bill of Rights after September 11th: Principles or Pragmatism", *Duquesne Law Review* 2004, Vol.42(2), (259) 259.

⁴⁸³ Fourth Amendment to the United States Constitution, 15 December 1791; J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 734; D.A. DRIPPS, "At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense", *University of Illinois Law Review* 1993, Vol.2, (261) 261-263; H. FUSON, "Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State", *The University of Memphis law review* 2020, Vol.50(1), (231) 257-258; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 537; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1009; E.W. MARSHALL *et al.*, "Police surveillance of

eighteenth century when the Bill of Rights was drafted, property and privacy were protecting the same interests.⁴⁸⁴ The concept of privacy was not known at that time, but the idea of protecting one's property then is similar to the idea of protecting one's privacy today.⁴⁸⁵

In *Katz v. United States*, the Fourth Amendment was applied to the technological evolution of the digital age.⁴⁸⁶ The court acknowledged that the authors had drafted the Bill of Rights based on the times they were living in. Individuals wanted to keep their interpersonal communication

cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 751-752; T.L. MEARES, “Law of Community Policing and Public Order Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2823) 2823; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 512 and 562-563; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

⁴⁸⁴ *Katz v. United States*, 389 U.S. 347 (1967); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 734-735; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 257-258; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 12-15; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 537-538; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752.

⁴⁸⁵ *Katz v. United States*, 389 U.S. 347 (1967); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 734-735; W. BLOSS, “Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects”, *Surveillance & Society* 2007, Vol.4(3), (208) 212; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 257-258; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 12-24; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 537-538; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752.

⁴⁸⁶ *Katz v. United States*, 389 U.S. 347 (1967); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 736; B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 755 and 793-794; B.W. BELL, “Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy”, *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 159 and 177; W. BLOSS, “Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects”, *Surveillance & Society* 2007, Vol.4(3), (208) 212; D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 261-263; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 260; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 19-24; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 537-538; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 532; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-753; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 224; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; C.E. SMITH, “The Bill of Rights after September 11th: Principles or Pragmatism”, *Duquesne Law Review* 2004, Vol.42(2), (259) 263-264.

(mainly enshrined in letters) hidden from other people's knowledge. With the evolution of technology, first the telephone and nowadays the internet has taken over that role. Instead of writing letters we nowadays write e-mails, but the purpose of both has by and large remained the same. In both situations, the author wants to deliver a message to the recipient and he does not want other people to know the content of that message.⁴⁸⁷

In *Griswold v. Connecticut*, the Supreme Court interpreted the provisions of the Bill of Rights as including a constitutionally protected right to privacy.⁴⁸⁸ More specifically, it stated that citizens have the right to maintain confidential relationships.⁴⁸⁹ HEFFERNAN argues that when outsiders, like state officials, infiltrate the suspect's life and enter into confidential relationships with him in order to use the obtained information against him, this might violate the suspect's right to privacy.⁴⁹⁰ BELL expresses his concern about this investigation technique as well, since suspects will more likely disclose private information to undercover agents who they consider as friends rather than to regular state officials.⁴⁹¹ This restriction applies however only in case the infiltrator is a state official or a confidential human source, not if it is a conscientious citizen (*Part IV, Chapter 2, §3, b*).⁴⁹²

In the context of social media, it is not always easy to determine whether a suspect can have a 'reasonable expectation of privacy' for information that he voluntarily shares online, and the

⁴⁸⁷ Katz v. United States, 389 U.S. 347 (1967); J. BARD, "Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment", *Boston College Law Review* 2016, Vol.57(2), (731) 736; H. FUSON, "Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State", *The University of Memphis law review* 2020, Vol.50(1), (231) 260; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 19-24; T. HUGHES and C. BURTON, "Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I've Been Watching You Steady", *Am.J.Crim.Just.* 2013, Vol.38, (535) 537-538; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 524.

⁴⁸⁸ *Griswold v. Connecticut*, 381 U.S. 479 (1965); X, "Police infiltration of dissident groups", *The Journal of Criminal Law, Criminology, and Police Science* 1970, Vol.61(2), (181) 189.

⁴⁸⁹ X, "Police infiltration of dissident groups", *The Journal of Criminal Law, Criminology, and Police Science* 1970, Vol.61(2), (181) 189.

⁴⁹⁰ W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 56-57 and 67-68 and 106-111; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 249.

⁴⁹¹ B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 195-198; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 249.

⁴⁹² S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 34; X, "Police infiltration of dissident groups", *The Journal of Criminal Law, Criminology, and Police Science* 1970, Vol.61(2), (181) 190.

courts do in general not consider this data to be private.⁴⁹³ In a pre-digital world, the court had after all decided that “what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection”.⁴⁹⁴ However, the court had also stated that “what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected”.⁴⁹⁵ The Supreme Court reasons that suspects should know that they may be betrayed by their associates, which might happen to be undercover agents, and that therefore there can be no infringement of their reasonable expectation of privacy protected by the Fourth Amendment.⁴⁹⁶

⁴⁹³ United States v. Knotts, 460 U.S. 276 (1983); U.S. v. Kennedy, 81 F.Supp.2d 1103 (D. Kan. 2000); Guest v. Leis, 255 F.3d 325 (6th Cir. 2001); United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); People v. Harris, 949 N.Y.S.2d 590 (City Crim. Ct. 2012); United States v. Gatson, Criminal No. 13-705 (D.N.J. Dec. 15, 2014); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 737; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 273; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 32-37; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 538; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 532-533 and 545-547; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1009; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 752-753; P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 675.

⁴⁹⁴ Fourth Amendment to the United States Constitution, 15 December 1791; Lewis v. United States, 385 U.S. 206 (1966); Katz v. United States, 389 U.S. 347 (1967); California v. Greenwood, 486 U.S. 35 (1988); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 737; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 32-38; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 753; P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 675; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1811.

⁴⁹⁵ Katz v. United States, 389 U.S. 347 (1967); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 736-737; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 260; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 33; E.W. MARSHALL *et al.*, “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), (751) 753.

⁴⁹⁶ Fourth Amendment to the United States Constitution, 15 December 1791; Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971); United States v. Miller, 425 U.S. 435 (1976); Illinois v. Perkins, 496 U.S. 292 (1990); U.S. v. Kennedy, 81 F.Supp.2d 1103 (D. Kan. 2000); Guest v. Leis, 255 F.3d 325 (6th Cir. 2001); United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); United States v. Gatson, Criminal No. 13-705 (D.N.J. Dec. 15, 2014); J. BARD, “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), (731) 737-738; B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 796; B.W. BELL, “Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy”, *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 160 and 198; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 55; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 261;

The investigation method of police surveillance can under US law fall within the category of ‘search’ and might therefore infringe the rights protected by the Fourth Amendment (*Part IV, Chapter 1, §2*), since monitoring a suspect or wiretapping his (telephone) conversations can infringe his reasonable expectation that his conversations are private.⁴⁹⁷ The investigation technique of police infiltration is not considered to be within the category of ‘search’.⁴⁹⁸

Evidence obtained in violation of the Fourth Amendment is subject to the exclusionary rule.⁴⁹⁹ This evidence can as a consequence not be used against the person whose rights have been violated and has to be excluded from the criminal trial.⁵⁰⁰ The defendant may also file a claim for damages against the government officials who violated his privacy rights protected by the Fourth Amendment.⁵⁰¹

W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 86-87 and 106-115; E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 162; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 32-35; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 545-547; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1009; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1121; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867; L.M. SEIDMAN, “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, (111) 139; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1810-1811.

⁴⁹⁷ Fourth Amendment to the United States Constitution, 15 December 1791; D.A. DRIPPS, “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, (261) 263; W.C. HEFFERNAN, “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 2 and 81; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 194; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

⁴⁹⁸ E.E. JOH, “Breaking the law to enforce it: Undercover police participation in crime”, *Stanford Law Review* 2009, Vol.62(1), (155) 160; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 249; J.E. ROSS, “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1120-1121; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 512 and 562-563; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867.

⁴⁹⁹ Fourth Amendment to the United States Constitution, 15 December 1791; B.W. BELL, “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 756.

⁵⁰⁰ *Ibid.*

⁵⁰¹ *Ibid.*

§3. Privacy vs. (online) police infiltration / systemic observation compared

The Belgian and US legal systems are both concerned with the privacy implications that the investigation techniques of (online) police infiltration and (online) systemic police observation may have. The right to privacy has in both systems a legal basis, in Belgium in the Belgian Constitution and in the European Convention on Human Rights, and in the United States in the US Constitution. In case the state, and more specifically law enforcement, wants to interfere with this right, it will have to fulfill some conditions in order to do this lawfully. This right is after all not absolute in the countries discussed and an interference is therefore possible. First of all, a prior warrant authorizing the investigation technique is required in order to infringe this right in a lawful way (with a nuance for undercover operations in the United States; *Part III, Chapter 2, §2*). The infringement of the right to privacy during undercover operations might in the United States occur when the suspect's friendship and trust will be used in order to monitor his conversations and activities, whereas this infringement will in Belgium most likely occur when this investigation technique will be used without a warrant or concrete legal basis. Secondly, there should always be a supervising agent during undercover and surveillance operations to control the legality of the actions of undercover and surveilling agents.

The relation between the investigation technique of systemic police observation and the right to privacy shows some additional similarities between both legal systems. The Belgian as well as the US courts have stated that there is a difference between situations where a suspect is only occasionally observed, and situations where multiple different observations occur and the information of all these observations is put together. In the latter case, it is possible for law enforcement to gain insight into someone's private life and as a consequence there is a more severe invasion on someone's privacy. This should and is therefore more strictly regulated in order to safeguard someone's right to privacy.

Chapter 2: The right to a fair trial and (online) police infiltration / systemic observation

§1. Fair trial vs. (online) police infiltration / systemic observation in Belgium and Europe

The right to a fair trial is in Europe enshrined in art. 6 ECHR, which states that “everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgement shall be pronounced publicly, but the press and public may be excluded (...). Everyone charged with a criminal offense shall be presumed innocent until proved guilty according to law. Everyone charged with a criminal offense has the following minimum rights: (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him; (b) to have adequate time and facilities for the preparation of his defense; (c) to defend himself in person or through legal assistance (...); (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court”.⁵⁰²

One of the constitutive elements of undercover operations is the use of deception which is often employed by infiltrators in order to make their role credible.⁵⁰³ However, this can come into conflict with the obligation to warn defendants of their right to counsel and their right to remain silent.⁵⁰⁴ Undercover operations can therefore sometimes violate the right to a fair trial protected by art. 6 ECHR.

⁵⁰² Art. 6 ECHR, *BS* 19 August 1955.

⁵⁰³ ECtHR 11 February 2014, nr. 16463/08, *Sandu/Moldova*; ECtHR 24 April 2014, nr. 6228/09, 19678/07, 52340/08, 7451/09, 19123/09, *Lagutin a.o./Russia*, *T.Strafr.* 2014, Vol.3, 199; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; E.E. JOH, “Bait, Mask, and Ruse: Technology and Police Deception”, *Harvard Law Review Forum* 2015, Vol.128, (246) 246; J. MEESE, “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, (1134) 1137-1138; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

⁵⁰⁴ ECtHR 11 February 2014, nr. 16463/08, *Sandu/Moldova*; ECtHR 24 April 2014, nr. 6228/09, 19678/07, 52340/08, 7451/09, 19123/09, *Lagutin a.o./Russia*, *T.Strafr.* 2014, Vol.3, 199; GwH 19 July 2007, nr. 105/2007, *BS* 13 August 2007, 42941, *JLMB* 2008, Vol.14, 598, *NJW* 2007, Vol.168, 695, *RABG* 2008, Vol.1, 3, *Rev.dr.pén.* 2007, Vol.12, 1118, *RW* 2007-08, Vol.2, 85, *RW* 2007-08, Vol.43, 1811, *TBP* 2008, Vol.5, 286, *TGR-TWVR* 2008, Vol.1, 55, *T.Strafr.* 2007, Vol.4, 254; Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791; S. FIELD and C. PELSER, *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 11; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 507; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly

Some European countries were convicted for not respecting the right of the defendant to confront and cross-examine undercover agents in a criminal trial, since in some countries it was completely not allowed to call these state officials as witnesses and in other countries it was allowed but only anonymously.⁵⁰⁵ Belgium has found a good balance between the fair trial rights of the defendant and the necessity not to disclose sensitive information of undercover and surveillance investigations with the creation of a confidential file that can only be reviewed by the Indictment Chamber. In this way, law enforcement can safeguard the identity of its undercover agents on the one hand and its surveillance techniques on the other hand, while also enabling the defendant to (indirectly) cross-examine the regularity of these techniques by the Indictment Chamber (*Part III, Chapter 2, §1*).

§2. Fair trial vs. (online) police infiltration / systemic observation in the United States

The right to a fair trial is in the United States mainly enshrined in the Due Process Clauses of the Fifth (federal trials) and the Fourteenth (state trials) Amendment.⁵⁰⁶ The Fifth Amendment guarantees that for federal trials “(n)o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, (...); nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law”.⁵⁰⁷ The Fourteenth Amendment makes a similar statement for state trials requiring that “(no) state (shall) deprive any person of life, liberty, or

Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 256 and 266; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; K. SCHEPPELE, “Other People's Patriot Acts: Europe's Response to September 11”, *Loyola Law Review* 2004, Vol.50(1), (89) 143.

⁵⁰⁵ ECtHR 24 November 1986, Unterpertinger/Austria, *Publ.Eur.CourtH.R.* 1987, Serie A, nr. 110; ECtHR 20 November 1989, Kostovski/The Netherlands, *Rev.trim.DH* 1990, 267, *Publ.Eur.CourtH.R.* 1989, Serie A, nr. 166; ECtHR 19 December 1990, Delta/France, *Rev.trim.DH* 1992, 47, *Publ.Eur.CourtH.R.* 1991, Serie A, nr. 191-A; ECtHR 15 June 1992, Lüdi/Switzerland, *Juristenkrant* 2006, Vol.121, 2, *Rev.trim.DH* 1993, 309, *Publ.Eur.CourtH.R.* 1992, Serie A, nr. 238; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 504-506 and 564; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 261-262; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866.

⁵⁰⁶ Fifth Amendment to the United States Constitution, 15 December 1791; Fourteenth Amendment to the United States Constitution, 9 July 1868; CONGRESS CONSTITUTION ANNOTATED, *Amdt5.4.1 Right to Due Process: Overview*, https://constitution.congress.gov/browse/essay/amdt5_4_1/ (consultation 1 May 2021).

⁵⁰⁷ Fifth Amendment to the United States Constitution, 15 December 1791; CONGRESS CONSTITUTION ANNOTATED, *Amdt5.4.1 Right to Due Process: Overview*, https://constitution.congress.gov/browse/essay/amdt5_4_1/ (consultation 1 May 2021).

property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws”.⁵⁰⁸ Due process protects procedural due process, which includes “notice, opportunity for hearing, confrontation and cross-examination, discovery, basis of decision, and availability of counsel”.⁵⁰⁹

The Fifth Amendment to the US Constitution contains the right not to be compelled to incriminate oneself.⁵¹⁰ The Supreme Court has interpreted this Amendment in the Miranda case, and requires that certain warnings have to be given to people that are interrogated in order to prevent coercive questioning.⁵¹¹ More specifically, the court stated that “any statements that a defendant in custody makes during an interrogation are admissible as evidence at a criminal trial only if law enforcement told the defendant of the right to remain silent and the right to speak with an attorney before the interrogation started, and the rights were either exercised or waived in a knowing, voluntary, and intelligent manner”.⁵¹² By securing this, the suspect can decide whether or not to cooperate and whether or not to remain silent.⁵¹³

In the latter case, it may become difficult for law enforcement to build their case and therefore they will sometimes rely on people that are in close contact with the suspect, like a friend or family member, in order to obtain the information necessary.⁵¹⁴ Since suspects should be aware

⁵⁰⁸ Fourteenth Amendment to the United States Constitution, 9 July 1868; CONGRESS CONSTITUTION ANNOTATED, *Amdt5.4.1 Right to Due Process: Overview*, https://constitution.congress.gov/browse/essay/amdt5_4_1/ (consultation 1 May 2021); CONGRESS CONSTITUTION ANNOTATED, *Constitution of the United States: Fourteenth Amendment*, <https://constitution.congress.gov/constitution/amendment-14/> (consultation 1 May 2021).

⁵⁰⁹ CONGRESS CONSTITUTION ANNOTATED, *Amdt5.4.1 Right to Due Process: Overview*, https://constitution.congress.gov/browse/essay/amdt5_4_1/ (consultation 1 May 2021).

⁵¹⁰ Fifth Amendment to the United States Constitution, 15 December 1791; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 55; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 35; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866; G.C. THOMAS and R.A. LEO, “Law of Police Interrogation” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2835) 2835-2837.

⁵¹¹ *Miranda v. Arizona*, 384 U.S. 436 (1966); C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 55; S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 35; T.L. MEARES, “Law of Community Policing and Public Order Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2823) 2823; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246-247; C.E. SMITH, “The Bill of Rights after September 11th: Principles or Pragmatism”, *Duquesne Law Review* 2004, Vol.42(2), (259) 264-265; G.C. THOMAS and R.A. LEO, “Law of Police Interrogation” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2835) 2835-2837.

⁵¹² *Miranda v. Arizona*, 384 U.S. 436 (1966); M. RADLER, “Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance”, *Geo.Wash.L.Rev.* 2012, Vol.80(4), (1209) 1225.

⁵¹³ S. LEVINSON, “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), (29) 35.

⁵¹⁴ *Ibid.*

that they can be betrayed by their associates, friends or family members, their reasonable expectation of privacy enshrined in the Fourth Amendment read together with the right not to be compelled to incriminate oneself protected by the Fifth Amendment will not be violated (*Part V, Chapter 1, §2*).⁵¹⁵ The police is as a consequence not obliged to apply the Miranda warnings when they interrogate suspects during undercover operations.⁵¹⁶ There are however limitations, since people who possess an evidentiary privilege cannot be compelled, but may consent voluntarily, to disclose certain information.⁵¹⁷ These people have often a confidential relationship with the suspect, such as a husband or wife, an attorney, a doctor or a priest.⁵¹⁸ These relationships are moreover protected by the Fourth Amendment's right to privacy (husband/wife), the right to counsel (attorney) and the First Amendment's freedom of speech and religion (priest).⁵¹⁹ However, this privilege can violate a defendant's right to cross-examine and confrontation in case a privileged person's testimony is necessary for his defense.⁵²⁰

Finally, the Sixth Amendment guarantees that "(i)n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, (...), and to be informed of the nature and cause of the

⁵¹⁵ Fourth and Fifth Amendment to the United States Constitution, 15 December 1791; Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971); United States v. Miller, 425 U.S. 435 (1976); Illinois v. Perkins, 496 U.S. 292 (1990); U.S. v. Kennedy, 81 F.Supp.2d 1103 (D. Kan. 2000); Guest v. Leis, 255 F.3d 325 (6th Cir. 2001); United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012); United States v. Gatson, Criminal No. 13-705 (D.N.J. Dec. 15, 2014); B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 796; B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 160 and 198; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 55; W.C. HEFFERNAN, "Fourth Amendment Privacy Interests", *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), (1) 86-87 and 106-115; E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 162; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 249; S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 32-35; R. LEVINSON-WALDMAN, "Government Access to and Manipulation of Social Media: Legal and Policy Challenges", *Howard Law Journal* 2018, Vol.61(3), (523) 545-547; R. LEVINSON-WALDMAN, "Private Eyes, They're Watching You: Law Enforcement's Monitoring of Social Media", *Oklahoma Law Review* 2019, Vol.71(4), (997) 1009; J.E. ROSS, "Valuing inside knowledge: Police Infiltration as a problem for the law of evidence", *Chicago-Kent Law Review* 2004, Vol.79(3), (1111) 1121; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867; L.M. SEIDMAN, "The Supreme Court, Entrapment, and Our Criminal Justice Dilemma", *Supreme Court Review* 1981, (111) 139.

⁵¹⁶ Illinois v. Perkins, 496 U.S. 292 (1990); E.E. JOH, "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), (155) 162.

⁵¹⁷ L. LETWIN, *Encyclopedia of the American Constitution: Evidentiary privilege*, <https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/evidentiary-privilege> (consultation 1 May 2021).

⁵¹⁸ *Ibid.*

⁵¹⁹ *Ibid.*

⁵²⁰ *Ibid.*

accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense”.⁵²¹

§3. Fair trial vs. (online) police infiltration / systemic observation compared

The majority of the fair trial rights are very similar in Belgium and in the United States. Both countries also agree that undercover operations can endanger some of these rights, more specifically the right not to be compelled to incriminate oneself and the right to cross-examine witnesses. Belgium has solved this issue through the creation of a confidential file, which allows the suspect to obtain the information necessary in order to establish whether the investigation was conducted lawfully, while safeguarding the identity of the undercover agent and the surveillance techniques that require confidentiality. In the United States, the suspect’s rights are guaranteed by the Miranda warnings that will be given to him after he will officially be charged with a criminal offense. The non-mandatory use of the Miranda warnings during undercover operations can however lead to situations where the suspect will make incriminating statements without knowing or being warned that he is speaking with an (undercover) law enforcement official. The evidentiary privilege that certain people can rely on in the United States, can also violate a defendant’s right to cross-examine in case a privileged person’s testimony is necessary for his defense. The confidential file that is used in Belgium could therefore be an asset for the United States as well, since it safeguards the interests of both law enforcement and the defendant. The complete witness statement of an evidentiary privileged person could for example also be included in this confidential file, while only certain parts of his statement necessary for the defendant’s cross-examination rights could be included in the public file. Finally, the fair trial rights can in both countries be found in the hierarchically highest legislation, namely the European Convention on Human Rights and the US Constitution.

⁵²¹ Sixth Amendment to the United States Constitution, 15 December 1791.

Chapter 3: Freedom of speech and (online) police infiltration / systemic observation

§1. Freedom of speech vs. (online) police infiltration / systemic observation in Belgium and Europe

The freedom of speech is embedded in the Belgian Constitution in articles 19 (freedom of religion and expression), 25 (freedom of the printing press) and 150 (exception for racism and xenophobia⁵²²), and in the European Convention on Human Rights in art. 10 ECHR.⁵²³ The ECHR states that the freedom of expression is not absolute and can be restricted in certain situations.⁵²⁴ The second paragraph of art. 10 ECHR states that the conditions and restrictions have to be “prescribed by law (legality), necessary in a democratic society (proportionality), in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary (legitimacy)”.⁵²⁵

Most importantly, the freedom of speech is in Europe restricted by the rights of the other party who is being targeted by the speech.⁵²⁶ One person’s speech can for example constitute of discrimination, libel or defamation of the other person, for which the first person can be held criminally liable. Law enforcement might start an online systemic observation if someone frequently posts discriminatory comments or hate speech. However, hate speech does as such already constitute a criminal offense and online police surveillance will therefore in most cases not be necessary in order to accuse the suspect. An online police surveillance operation will

⁵²² In cases where there are alleged violations of the freedom of expression by the printing press, it was historically considered to be best to let the jury deal with those cases instead of the state. The jury was considered to be more neutral than the state. In cases of racism or xenophobia however, it is the state that will deal with the case and not a jury.

⁵²³ Art. 10, §2 ECHR, *BS* 19 August 1955; art. 19, 25 and 150 Gw., *BS* 17 February 1994; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 16-19.

⁵²⁴ Art. 10 ECHR, *BS* 19 August 1955; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 16; W. STOL, “Filteren van internet: een politietaak?”, *Orde van de dag* 2010, Vol.3, (43) 44.

⁵²⁵ Art. 10 ECHR, *BS* 19 August 1955; K. LEMMENS, “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, (15) 16.

⁵²⁶ L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 56.

most likely only be initiated in the most extreme cases and based on a reasonable suspicion of criminal involvement, in order to obtain more information about the person who posted the hate speech or in order to discover a broader criminal network of which this person might be a member (*Part IV, Chapter 1, §1*). In these situations, the intelligence gathering aim will prevail, since the discriminatory comments or hate speech will temporarily be left unprosecuted and prosecution will only be initiated later, in order to gain more intelligence first.

§2. Freedom of speech vs. (online) police infiltration / systemic observation in the United States

The freedom of speech is in the United States enshrined in the First Amendment, which states that “Congress shall make no law (...) abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble (...)”.⁵²⁷ The First, Fourth and Fourteenth Amendment are often read together, in order to protect minorities and the freedom of religion.⁵²⁸ The Equal Protection Clause of the Fourteenth Amendment prohibits more specifically discrimination by the government based on an individual’s race, national origin or religion.⁵²⁹

⁵²⁷ First Amendment to the United States Constitution, 15 December 1791; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 232 and 252.

⁵²⁸ First and Fourth Amendment to the United States Constitution, 15 December 1791; Fourteenth Amendment to the United States Constitution, 9 July 1868; L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 56; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 54; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 531-534 and 560; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246-247; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 48; T. TURAN, “War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties”, *Uluslararası Hukuk ve Politika* 2006, Vol.7, (111) 118.

⁵²⁹ Fourteenth Amendment to the United States Constitution, 9 July 1868; *Gideon v. Wainwright*, 372 U.S. 335 (1963); *Massiah v. United States*, 377 U.S. 201 (1964); *Brewer v. Williams*, 430 U.S. 387 (1978); *Patterson v. Illinois*, 487 U.S. 285 (1988); *Montejo v. Louisiana*, 556 U.S. 778 (2009); J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 564; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 246-247; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 48; C.E. SMITH, “The Bill of Rights after September 11th: Principles or Pragmatism”, *Duquesne Law Review* 2004, Vol.42(2), (259) 265-266; G.C. THOMAS and R.A. LEO, “Law of Police

Police surveillance might endanger the rights protected by the First and Fourteenth Amendment, when people will fear negative repercussions as a result of exercising their right to freedom of association.⁵³⁰ Muslim American communities have especially since 9/11 experienced a feeling of an unfairly assigned collective responsibility for the occurrence of these events.⁵³¹ Police infiltration might also infringe the rights protected by the First Amendment, when undercover operations will take place in religious or political groups.⁵³² The

Interrogation” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2835) 2835-2839.

⁵³⁰ First Amendment to the United States Constitution, 15 December 1791; Fourteenth Amendment to the United States Constitution, 9 July 1868; Privacy Act 5 U.S.C. §552a (e)(7); NAACP v. Patterson, 357 U.S. 449 (1958); L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 56; D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 210-216 and 239; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 248 and 267-268; A.N. GUIORA, “Transnational Comparative Analysis of Balancing Competing Interests in Counter-Terrorism”, *Temple International & Comparative Law Journal* 2006, Vol.20(2), (363) 369; T. HUGHES and C. BURTON, “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, (535) 547; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 549; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1002; P. ROSENZWEIG, “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), (663) 703; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1787-1797 and 1817-1818.

⁵³¹ A. ARSHAD IMTIAZ, “Off the Record: Police Surveillance, Muslim Youth and an Ethnographer’s Tools of Research”, *Equity & Excellence in education* 2018, Vol.51(3-4), (431) 431; H. FUSON, “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), (231) 248 and 267-268; A.N. GUIORA, “Transnational Comparative Analysis of Balancing Competing Interests in Counter-Terrorism”, *Temple International & Comparative Law Journal* 2006, Vol.20(2), (363) 366-368; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 536 and 550; D. SCHANZER, C. KURZMAN, J. TOLIVER and E. MILLER, *The challenge and promise of using community policing strategies to prevent violent extremism: A call for community partnerships with law enforcement to enhance public safety, Final Report*, <https://www.ncjrs.gov/pdffiles1/nij/grants/249674.pdf> (consultation 14 November 2020); D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 4-10; T. TURAN, “War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties”, *Uluslararası Hukuk ve Politika* 2006, Vol.7, (111) 115 and 124-125; M.A. WASSERMAN, “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), (1786) 1787-1797 and 1822.

⁵³² First Amendment to the United States Constitution, 15 December 1791; D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 207 and 218-223 and 239; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 60-61; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1002; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 100; J.E. ROSS, “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 522-523 and 567; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 247 and 264; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer,

government is allowed to protect itself and its citizens from violence and the destruction of property by operating undercover in suspected terrorist organizations.⁵³³ This might however also harm the right to freedom of association and the right to freedom of religion of many people who are not involved in terrorist activities.⁵³⁴

The Attorney General's Guidelines for Domestic FBI Operations make therefore clear that "the investigation, collection or maintenance of information with the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States is not authorized" and the FBI's internal DIOG also qualifies "activities of (...) a religious or domestic political organization or individual prominent in such an organization, or news media" as a sensitive investigative matter requiring more safeguards (*Part IV, Chapter 2, §1, b*).⁵³⁵ Moreover, the use of deception during undercover operations may make people more suspicious and will probably weaken their social ties which are based on friendship, love and trust.⁵³⁶

2014, (2865) 2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 48.

⁵³³ D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 218-219 and 236-237; A.N. GUIORA, "Transnational Comparative Analysis of Balancing Competing Interests in Counter-Terrorism", *Temple International & Comparative Law Journal* 2006, Vol.20(2), (363) 369.

⁵³⁴ D. BERRY, "The First Amendment and Law Enforcement Infiltration of Political Groups", *Southern California Law Review* 1982, Vol.56(1), (207) 218-219 and 239; C. FIJNAUT, *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 60-61; J.E. ROSS, "The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany", *The American Journal of Comparative Law* 2007, Vol.55, (493) 522-523 and 567; J.E. ROSS, "Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint", *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 264; J.E. ROSS, "Law of Undercover Policing" in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 4-10 and 48.

⁵³⁵ ATTORNEY GENERAL, *The Attorney General's Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 13; U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I, 10 Sensitive Investigative matter and Sensitive Operations Review Committee*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 10/1.

⁵³⁶ B.W. BELL, "Secrets and lies: news media and law enforcement use of deception as investigative tool", *University of Pittsburgh Law Review* 1999, Vol.60(3), (745) 797-798; B.W. BELL, "Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy", *William & Mary Bill of Rights Journal* 2002, Vol.11(1), (151) 196; C. FIJNAUT and G.T. MARX, *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 1; B.L. GERSHMAN, "Abscam, the Judiciary, and the Ethics of Entrapment", *The Yale Law Journal* 1982, Vol.91, (1565) 1585; E.E. JOH, "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, (246) 250; S. LEVINSON, "The Hidden Costs of Infiltration", *The Hastings Center Report* 1982, Vol.12(4), (29) 32; G.T. MARX, *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 96-100 and 148-149; J.E. ROSS, "The

When internet monitoring is among others based on religious, political or other protected categories or activities, the First Amendment may provide a right to privacy extension.⁵³⁷ The US Court of Appeals for the Fourth Circuit has already held that both ‘likes’ and comments on Facebook constitute a form of protected speech by the First Amendment, and also the US Supreme Court has stated that cyberspace is the most important place for the exchange of opinions.⁵³⁸

§3. Freedom of speech vs. (online) police infiltration / systemic observation compared

The freedom of speech is differently regulated in Belgium and in the United States. In the Belgian Constitution, the freedom of expression and religion are mentioned together in art. 19 Gw. In the European Convention on Human Rights, the freedom of speech is embedded in art. 10 ECHR, which states in §2 that this freedom is not absolute and can be restricted in certain cases. The main restriction consists of the rights of the other party that is targeted by the speech, since for him it might constitute of defamation or libel. In the United States, the freedom of speech is an absolute right which gets the highest level of constitutional protection. The US

Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, (493) 497; J.E. ROSS, “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, (239) 248; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 5 and 10.

⁵³⁷ First Amendment to the United States Constitution, 15 December 1791; D. BERRY, “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), (207) 207; M. De S.-O.-L’E. LASSER, “The question of understanding” in P. LEGRAND and R. MUNDAY (eds.), *Comparative legal studies: traditions and transitions*, Cambridge, Cambridge University Press, 2003, (197) 203-204; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 534; J.E. ROSS, “Law of Undercover Policing” in G. BRUINSMA and D. WEISBURD (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, (2865) 2866-2867; D. SHAMAS and N. ARASTU, *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 48.

⁵³⁸ First Amendment to the United States Constitution, 15 December 1791; *Bland v. Roberts*, No. 12-1671 (4th Cir. 2013); *Packingham v. North Carolina*, 137 S.Ct. 1730 (2017); L. BEIRENS, “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, (51) 56; P. GORDON, *What’s in a “Like”?* *Precedent-Setting Case Poses New Risk for Employers*, <https://www.littler.com/publication-press/publication/whats-precedent-setting-case-poses-new-risk-employers> (consultation 21 May 2021); HARVARD LAW REVIEW ASSOCIATION, “First Amendment – Freedom of Speech – Public Forum Doctrine – *Packingham v. North Carolina*”, *Harvard Law Review* 2017, Vol.131(1), (233) 235-236; R. LEVINSON-WALDMAN, “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), (523) 534-535; R. LEVINSON-WALDMAN, “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), (997) 1011.

courts have moreover held that both ‘likes’ and comments on Facebook constitute a form of protected speech by the First Amendment, and cyberspace is the most important place for the exchange of opinions. Surveilling religious or political organizations without other non-religious or non-political indications might violate the freedom of religion and the freedom of association. This last case would also in Belgium be defined as discriminatory government surveillance based on art. 19 of the Belgian Constitution. Even though the freedom of speech is regulated in a different way in Belgium and in the United States, it is in both countries not allowed for law enforcement to initiate undercover or surveillance operations on the sole basis that someone is exercising his constitutionally protected rights, like his freedom of religion or (political) association.

Part VI: Analysis

In this functional comparative law research between Belgium and the United States, the investigation techniques of (online) police infiltration and (online) systemic police observation were analyzed and balanced with the fundamental rights to privacy, a fair trial, and the freedom of speech. The researched investigation techniques are named differently in Belgium (police infiltration and systemic police observation) and in the United States (undercover operations and police surveillance). Given that these concepts describe complex investigation techniques and that it was difficult to find a common term that would fit both systems, the author decided to use the Belgian and US terms as synonyms in this research. The lack of a general nationwide applicable standard for undercover operations in the United States made it difficult to compare this investigation technique. Since every level (FBI, local,...) has its own regulations and the regulations on the FBI level appeared to come closest to the regulation in the Belgian Code of Criminal Procedure, this level was therefore chosen for the comparison.

The investigation techniques of off- and online police infiltration have only recently been granted a legal basis in Belgium, respectively in 2003 and 2016. In the United States, undercover operations have been largely employed and developed since the 1920s and it is therefore considered a leading country. Its approach has served as an example model for the regulation of this investigation technique in many European Codes of Criminal Procedure. Off- and online police infiltration are in Belgium regulated by criminal procedural law⁵³⁹, whereas in the United States there is no general legal framework set up by constitutional criminal procedure, but different frameworks apply to different law enforcement departments. The Attorney General's Guidelines on FBI Undercover Operations and the FBI's internal DIOG provide a legal framework for these investigation techniques on the FBI level, but these guidelines are for internal use only. In case of a violation, the suspect will not be able to rely on them.

A prior warrant authorizing this investigation technique is not required by US law, in contrast to Belgium where an (online) undercover operation can only be initiated based on a prior warrant issued by the Crown prosecutor or the investigating judge. The Attorney General's Guidelines do mention the requirement of prior approval for real life FBI undercover operations that has to be granted by the Special Agent in Charge of the FBI office. For the initiation of an

⁵³⁹ Art. 46*sexies* and 47*octies* Sv., BS 27 November 1808.

online FBI undercover operation, it is possible to request a delayed approval. A suspect will not be able to rely on these guidelines if the FBI undercover operation was initiated without approval. This would according to US supervising Professor David Schanzer however have consequences for the FBI agent who violated the guidelines and he would certainly lose his job, so this hypothetical situation is quite unlikely to occur and the right permissions will therefore almost always be obtained. From the suspect's perspective, the Belgian legal framework provides more safeguards than the US legal system, since a violation can be addressed and relied on by the suspect in court. A legally enforceable framework regulating this investigation method is therefore preferable.

Given that the Attorney General's Guidelines fulfill more or less the same role for the FBI in the United States as the Code of Criminal Procedure in Belgium, it could be interesting for the United States to grant these FBI guidelines a legal status so that they could also be relied on in court by the suspect. In this way, the suspect's rights would also be protected in the United States in case violations of the FBI guidelines would occur. It could however also be argued that from a law enforcement perspective the US legal system is more convenient, since the suspect is not able to rely on procedural mistakes made by FBI state officials. This could be interesting for making sure that suspects of serious criminal offenses do not go unpunished, but these suspects have also a right to a fair trial and their rights should also be protected. It can therefore be concluded that the Attorney General's Guidelines in the United States and the regulation in the Code of Criminal Procedure in Belgium consist of a good legal framework, but the Attorney General's Guidelines should in addition be granted a legally enforceable status in order to protect everyone's fair trial rights.

The Belgian and US definitions of real life as well as online undercover operations show similarities, which is a positive trend. For real life undercover operations, the use of disguise by an undercover agent, the adoption of a fictitious identity, the requirement of a not merely incidental, but a long-lasting contact between the suspect and the police infiltrator and mainly an intelligence gathering aim are characteristics that both definitions have in common. For online undercover operations, both countries require that accurate and detailed transcripts of all the online communication between the undercover agent and the suspect should be registered, that the use of fake identities should be avoided for as long as possible and that anonymous accounts should be used instead, and that the opportunity to avoid physical contact in real life between the suspect and the undercover agent is an important asset to protect the latter's safety. The 'long-lasting contact' requirement will during online undercover operations be fulfilled

when the contact consists of multiple messages that are sent back and forth between the undercover agent and the suspect. These similarities in definitions are very useful in an international context. Off- and online undercover operations are after all often used in investigations with a cross-border dimension where cooperation between different law enforcement units is necessary. Definitions with common elements can facilitate communication and operation in the field between these different agencies.

The four principles specified by Belgian law, namely subsidiarity, proportionality, the prohibition of provocation, and the prohibition to commit criminal offenses have each a substantive counterpart in US law. The first two principles are for criminal investigations used in a reversed way. In Belgium, police infiltration is considered to have serious privacy infringing implications and will therefore only be used as a means of last resort that is preserved for cases concerning serious crime only. In the United States, it is sometimes overused as a tactic in order to obtain quick results and evidence in a fast and easy way for all types of crime. The privacy implications of this investigation technique probably play a role in this decision. From a US Fourth Amendment's privacy perspective, undercover operations are less privacy invasive than wiretapping or electronic surveillance. There is no warrant requirement for the initiation of an undercover operation, whereas this is always required for a wiretap or electronic surveillance. For national security investigations, the Belgian and US regulations of undercover operations show many similarities limiting its use to serious crimes. Both countries recognize that the more privacy intrusive an investigation technique is considered to be, the more serious the crimes being investigated have to be and vice versa. The level of privacy invasion is in Belgium determined based on the actual interaction between a suspect and law enforcement. While interacting undercover, a state official might gain comprehensive insight into someone's private life given that the suspect will most likely trust him and will as a consequence share private information with him. Police infiltration is therefore considered to be more privacy invasive than systemic police observation. It could however also be argued that a suspect is knowingly sharing information with 'his friend' who might turn out to be an undercover agent, which is the logic applied in the United States. When on the contrary a suspect is kept under surveillance, he is not aware that his movements and conversations are being monitored by law enforcement, or in general by a third party. If this logic is followed, it can be understood why in the United States systemic police observation is considered to be more privacy invasive than police infiltration. Systemic police observation comes in the United States within the scope of 'search' protected by the Fourth Amendment and is therefore more strictly regulated. This is

not the case for police infiltration, where the previously explained logic of ‘knowingly sharing private information with third parties’ is being applied for concluding that this investigation technique is less privacy invasive than police surveillance. The suspect is after all aware that he has shared information with a third party, which is not the case if he is (secretly) being monitored and kept under surveillance (*Part IV, Chapter 2, §3, b*). A personal preference of the author for the US approach has developed based on this logic, since a link can be found with everyday situations. In our life we meet many people with whom we interact on a daily basis. Sometimes, it can however happen that these people turn out not to be our friends and have shared our private information with people whom we did not want to share this information with. These situations have a bad impact on our trust, but they do occasionally happen. The risk of employing these techniques by law enforcement on a large scale might however completely diminish our trust in other people and make us suspicious towards relatively everyone. When on the other hand someone is kept under secret surveillance, he is not aware that third parties are monitoring his conversations and movements. This is less likely to happen in everyday situations. Both investigation techniques should therefore be well-regulated given their privacy invasive impact, but based on this US logic the author has developed a preference for the statement that systemic police observation is more privacy intrusive than police infiltration.

The principle of the prohibition of provocation during undercover operations is shared between Belgium and the United States. Both countries recognize the mutual influence that a suspect and an undercover agent may have on each other’s behavior, and therefore the suspect can request the court to quash the case if he can prove that he was unduly provoked by law enforcement to commit the criminal offense. This applies to provocation committed by law enforcement officials as well as by private individuals commissioned by the government. Sole deception and the creation of opportunity are not provocation. In order to establish whether provocation occurred, the courts in both countries will examine the suspect’s predisposition to commit the crime (subjective test) combined with the level of government persuasion and inducement to make the suspect commit the crime (objective test). These tests are in Belgium not as explicitly mentioned as in US law, but can be derived implicitly. Both legal systems provide therefore sufficient safeguards against provocation.

The last principle, the prohibition to commit criminal offenses, is in both Belgium and the United States adjusted, and it is accepted that undercover agents may commit criminal offenses during their undercover operations as long as certain conditions are fulfilled. Situations of self-

defense, situations where it is necessary to ensure other people's safety and where it is necessary for closing an investigation or obtaining necessary evidence, are under Belgian as well as US law considered justifying grounds for committing criminal offenses. These can in any case only be committed after prior authorization granted by the undercover agent's supervisor. An exception exists for situations where it is impossible for the undercover agent to safely contact his supervisor for prior permission, and therefore he will in these specific circumstances be allowed to notify his supervisor as soon as possible after the commitment of the crime. Belgium works with an enumerated list of criminal offenses that an undercover agent can commit and this list is drawn up before the initiation of each undercover operation. In the United States, prior authorization suffices for an undercover agent to commit the criminal offense he requested. Both countries require in any case that all the crimes committed by undercover agents have to be proportionate to and may never be more severe than the crime being investigated. If these conditions will be fulfilled, immunity will most likely be granted to the police infiltrator for the crimes he committed during his undercover operation. The Belgian enumerated list of criminal offenses can be considered more suspect-friendly than the US legal system. This list provides a more strict framework for law enforcement with which they have to comply. This may sometimes however turn out to be too strict, since it is difficult to predict up front which criminal offenses should be allowed and which not. An undercover agent works in the field and he is sometimes confronted with unexpected situations. In those cases, he has to make quick decisions and if he will be forced to commit a criminal offense which is not on the enumerated list, he might be worried that he can be held liable for it. A middle ground between both systems would therefore seem to be the best solution. Certain broad categories of allowed crimes could be enumerated before each undercover operation based on the specific needs of that particular case.

The investigation technique of offline systemic police observation has only recently been granted a legal basis in Belgium, namely in 2003. In the United States, also this investigation method has been employed and developed for a long time, and has therefore served as an example model. Offline systemic police observation is in both Belgium and the United States regulated by law and requires a warrant in order to initiate this investigation method. There is one exception, which allows the FBI to warrantlessly conduct in person surveillance for an unlimited amount of time. This contradicts however the reasonable expectation of privacy which emerges after a period of approximately seven days. The Belgian legal system provides therefore a better protection for potential suspects in these situations and is as a consequence

preferable. The use of technical resources during surveillance operations is in both countries considered to be more privacy invasive and therefore additional requirements are set forth.

If the warrant requirement is not fulfilled, the systemic observation will be considered illegal and the evidence obtained during surveillance will have to be excluded. An observation is considered to be systemic when it aims at gaining insight into someone's private life and might as a consequence infringe someone's reasonable expectation of privacy. The Belgian four principles (subsidiarity, proportionality, the prohibition of provocation, and the prohibition to commit criminal offenses) can also be retrieved in the US regulation of police surveillance and apply therefore likewise. The subsidiarity and proportionality principles are for police surveillance operations in Belgium and in the United States applied in a reversed way, however, in the exact opposite way as for police infiltration. Systemic police observation is in the United States considered to be more Fourth Amendment's privacy invasive than police infiltration, and can therefore only occur based on a warrant. In Belgium on the contrary, police infiltration is considered to be more privacy invasive than systemic police observation. This difference has already been discussed and analyzed above, and a reference to that analysis is therefore made.

Online systemic police observation did, in contrast to its offline counterpart, not receive a legal basis in Belgium nor in the United States, and the offline regulation is as a consequence used by analogy in both countries. Given the rapid evolution of the internet and the adaptability of the offline regulation to this online situation, it can be understood that the legislators did not find it necessary to make a new law governing solely these online situations. However, this should be analyzed regularly and kept up to date with the technological evolution. For now, the offline regulation can be translated to and applied in the virtual world. With the emergence of encrypted platforms and data, the publicly available information may become limited and more adequate legislation may be needed.

Information that is online publicly available can be accessed and monitored by Belgian as well as US law enforcement under the same conditions as someone's movements in public places. Law enforcement is in general allowed to access and surveil public places in order to check whether there is compliance with law and order, independent of whether these places are real or virtual. A difference can however be noticed between both systems when this online publicly available information is systemically being accessed and monitored. In the United States, this information is not protected by the Fourth Amendment's right to privacy, given that once someone decides to make certain information publicly available, he renounces his right to privacy for that information. The frequent monitoring of this online publicly available

information can in Belgium however be qualified as systemic police observation, which will require a warrant. If the Belgian police will moreover store this information in a systemic way, a reasonable suspicion of involvement in a criminal offense will have to be proven. Online publicly accessible information that is being monitored in a systemic way can as a consequence be considered more protected in Belgium than in the United States. The US reasoning is on the one hand logical, since someone who publicly shares information on the internet should be aware that anyone, including law enforcement, can access that information. On the other hand, a link could be made with the case law on offline police surveillance where it was first considered that surveilling a car which is driving on public ways does not constitute of a violation of someone's privacy, but later this reasoning was adapted and it was decided that based on the mosaic theory "a whole is different from the sum of its individual parts" and "the whole of one's movements over the course of a month is not constructively exposed to the public because ... the whole reveals far more than the individual movements it comprises".⁵⁴⁰ A specific duration was not established by the US courts, but in general a time frame of seven days can be identified as the demarcation period between publicly available and non-publicly available information. This case law could, in conformity with the analogy theory, also be transposed to the online counterpart of systemic police observation. In Belgium, the demarcation period has been set on five consecutive days and could in that situation be considered similar. The question is however which approach should be preferable. It is true that someone should be aware that when he publicly posts information on the internet, this can be accessed by anyone. It is for law enforcement however also more easy to monitor publicly accessible information on the internet than in real life, since they only need a computer in order to do this. This is in contrast to offline police surveillance, which often requires a time and resource consuming approach in order to be able to monitor the suspect's movements and conversations. Given that nowadays most people are aware of the possibilities of the internet to share their information in a public or private way (by adjusting the privacy settings) and that they should foresee the consequences if they publicly share too much information, the author's preference goes to the US approach where no warrant is required in order to systemically monitor online publicly available information.

Information that is not online publicly available can in both Belgium and the United States only be accessed by law enforcement based on a warrant. Firstly, a warrant is in both countries necessary for accessing the content of this communication. The US practice of circumventing

⁵⁴⁰ United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

the warrant requirement by asking a Facebook or Twitter friend of the suspect to show or share the information on the suspect's profile or their private messages with law enforcement is however in the author's opinion questionable. It is true that someone who is sharing private information with a 'friend' should be aware that this friend can share or show this information to other people, but in most cases people will trust that their private messages will be kept private. This is also the case for information posted on someone's Facebook page for which the privacy settings have been activated. This shows the intent of the person to preserve this information as private between him and his virtual friends. This situation is different from information shared in real life conversations, since in those cases it is less clear that a person wants to keep this information private. The other party might assume that the information shared should stay between him and the other person, but if the person does not clearly state that this information should be kept private, this cannot be taken for granted. In the virtual world, it is however possible to make this intention of keeping information private clear by adjusting the privacy settings. In the author's opinion, it should therefore not be possible to circumvent the requirement of a warrant for accessing the content of this information through approaching someone's virtual friends with the request to share or show this private information. Secondly, information about the sole location where information was sent or received and data to identify the sender or receiver can in the United States be obtained by a subpoena, and therefore without a warrant, in contrast to Belgium where a warrant for obtaining this information is also required. The sole location where certain communication took place and the data to identify the person who has sent or received the information, also called metadata, are in the United States considered to be of a more public nature. This analysis is based on the Jackson ruling where "the outward form and weight of (...) mailings including the recipient's name and physical address" were found not to be constitutionally protected, since anyone had access to this information.⁵⁴¹ The metadata of for example an e-mail or private Facebook message is therefore by analogy not protected by the Fourth Amendment, and law enforcement does not need a warrant in order to obtain this information. It is however complicated to compare the information on an envelope with the location of a smartphone. The content of the communication is in the United States as a consequence more protected than its metadata, based on the difference in their respective privacy invasion. This is understandable, but the analogy between the location and identification information of letters on the one hand and the metadata of e-mails or private Facebook messages on the other hand seems to be quite outdated. E-mails

⁵⁴¹ Ex parte Jackson, 96 U.S. 727 (1878); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).

or Facebook messages can be sent from someone's computer or smartphone and their location is not as publicly known as the contact details written on a letter. The location of a smartphone will moreover show in detail where a person was, came from or went to, when sending or receiving the message. This information is much more privacy invasive than the information revealed by an envelope. The communication can moreover be sent or received from someone's computer at home, and the Fourth Amendment prohibits searches in someone's home without a warrant. The Belgian requirement of a prior warrant in order to obtain information about the location where certain communication took place and prior authorization for requesting data to identify the people involved, on top of the warrant requirement in both the Belgian and US legal systems for accessing the content of the communication, is therefore preferable and could be an asset for the United States as well.

The fundamental rights to privacy, a fair trial and the freedom of speech are in Belgium as well as in the United States protected by the hierarchically highest legislation, namely the European Convention on Human Rights (ECHR) and the Belgian Constitution for Belgium, and the US Constitution for the United States. The previously discussed investigation techniques of (online) police infiltration and (online) systemic police observation have to comply with these fundamental rights and freedoms as a consequence.

The right to privacy is in Belgium and in the United States recognized to be endangered by the use of these investigation techniques. The right to privacy is not absolute and the Belgian and US legal systems allow therefore an interference with this right if certain conditions are fulfilled. A general condition for both investigation techniques is that a supervising agent should always control the legality of the actions of undercover and surveilling agents during their operations. The second condition which requires a prior warrant applies in the United States only for the investigation technique of electronic surveillance, whereas in Belgium this requirement is applicable for both (online) police infiltration and (online) systemic police observation. The warrant requirement does therefore not apply for (online) undercover operations in the United States, with a nuance for (online) undercover operations initiated by or in cooperation with the FBI where prior approval has to be obtained⁵⁴², which has been discussed above. Given the privacy implications of both undercover operations and systemic police surveillance, it would however be safer to require a warrant for both investigation

⁵⁴² J. ASHCROFT, *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>.

techniques. The Belgian as well as the US courts have additionally stressed that long-term (systemic) police observation is more privacy invasive than short-term police observation, given that during a systemic surveillance, law enforcement aims at gaining insight into someone's private life and this should therefore be more strictly regulated. The difference in approach on privacy intrusiveness of these investigation techniques has already been analyzed above in the discussion on the subsidiarity and proportionality principle, and a reference to that analysis is therefore made.

The right to a fair trial shows many similarities between the Belgian and the US legal systems. Both countries are aware that in order to safeguard the investigation, it will be necessary to modify the fair trial rights during the investigation or withhold certain information until and after the undercover or surveillance operation will be completed. Belgium as well as the United States have therefore created correction mechanisms in order to mitigate the interference at a later stage. Belgium has solved this issue through the creation of a confidential file containing the identity of the undercover agent and the special techniques used during surveillance, which regular use can only be reviewed by the Indictment Chamber on the request of the defendant. In this way, the defendant has the indirect option to check the regularity of the investigation methods used, while safeguarding that sensitive information such as the undercover agent's identity or special surveillance techniques will not become publicly known. In the United States, this is remedied by the Miranda warnings that will be given to the suspect after he will officially be charged with a criminal offense. These Miranda warnings must however not be given by undercover agents and as a consequence a suspect might incriminate himself without being warned. The Belgian creation of two investigation files, a public and a confidential one, is therefore preferable and could in the United States also provide a better balance between the defendant's and law enforcement's interests and rights.

The freedom of speech differs in its scope in Belgium and the United States, and might be infringed by (online) police infiltration and (online) systemic police observation operations. This freedom is in Belgium not considered to be an absolute freedom, and can most importantly be restricted by the rights of the other party that is targeted by the speech, since the free speech of one person might constitute of defamation and libel of another person. In the United States on the contrary, this is an absolute freedom which gets the highest level of constitutional protection and cannot be restricted. Therefore, all types of speech are allowed, even defamatory speech. If (online) police infiltration or (online) systemic police observation will be initiated on the sole basis of someone's exercise of his freedom of speech, even hate speech, this will in the

United States constitute of a violation of that freedom. Discriminatory or hate speech is in Belgium however considered a criminal offense as such and an additional surveillance investigation is therefore not needed. The Belgian and US approach are grounded in their Belgian respectively US historical and social context, and therefore there is no preferable model since each model functions in a different historical and social context.

Part VII: Conclusion

In this dissertation, the investigation techniques of (online) police infiltration and (online) systemic police observation were balanced with the fundamental rights to privacy, a fair trial, and the freedom of speech. These topics were in this comparative law research analyzed in three parts for Belgium and the United States. Firstly, the investigation technique of (online) police infiltration was discussed. Secondly, the legal framework on (online) systemic police observation was analyzed. And finally, these two investigation techniques were balanced with the rights to privacy, a fair trial and the freedom of speech. The aim of this functional comparative law research was to find topics that could be compared based on the fact that they fulfill the same function in different legal systems. It can be concluded that receiving feedback from both Belgian and US supervisors was an added value for this dissertation and led to conclusions and interpretations that could otherwise not have been reached. It is therefore important to not only study a foreign legal system from ‘the books’, but also find someone who is familiar with the legal system to explain how it works ‘in practice’. Some differences between both countries could be noted and based on these, the following suggestions were made. Firstly, it could be interesting for the United States to grant the Attorney General’s Guidelines on FBI Undercover Operations a legally enforceable status. In case of a violation, a suspect would then be able to rely on these guidelines in court and safeguard these procedural requirements. Secondly, due to globalization, cross-border crime is facilitated and more cooperation is required between different national law enforcement agencies. The use of similar definitions, such as the Belgian and US definitions of off- and online undercover operations, are therefore very useful for cross-border cooperation. Thirdly, the Belgian enumerated list of criminal offenses allowed to be committed during undercover operations may be too strict, since it is difficult to predict how these operations will evolve. A middle ground between the Belgian and US legal systems where certain broad categories of allowed crimes are enumerated before each undercover operation based on the specific needs of that particular case would seem to be a better solution. Fourthly, the US exception for the FBI to the warrant requirement in order to conduct long-term in person surveillance contradicts the ‘reasonable expectation of privacy’ principle, and should therefore be deleted. A warrant should be required for regular offline systemic police observation at all times. Fifthly, the US approach which does not require a warrant for systemic monitoring of online publicly accessible information, could also be interesting for Belgium. Publicly available information is by definition public and Belgium might therefore have a slightly too protective regulation for the systemic monitoring of this type

of information. Sixthly, online non-publicly available information should only be accessible by law enforcement based on a warrant, and this warrant requirement should in the United States not be circumvented by asking the suspect's virtual friends to show or share this private information with state officials. A warrant should in the United States moreover also be required for obtaining information about the location where certain communication took place and for requesting data to identify the sender or receiver, given that its reasoning for not requiring a warrant is based on an outdated analogy between computers or smartphones and letters. Finally, the fundamental rights to privacy, a fair trial and the freedom of speech have to be respected during undercover operations and police surveillance. These investigation techniques should be well-regulated based on their privacy invasive impact. The author follows the US approach in considering that (online) systemic police observation is more privacy intrusive than (online) police infiltration, but both investigation techniques should only be initiated based on a prior warrant. In order to safeguard the defendant's trial rights, the United States could consider adopting the Belgian approach of creating two investigation files, a public and a confidential one, of which the latter could only be reviewed by a particular judge and would contain sensitive information such as specific surveillance techniques or the identity of undercover agents. The freedom of speech has shown that a certain approach should always be understood within its broader historical and social context. A recommendation for future research is to conduct interviews with people working in the field as well in Belgium as in the United States. Their opinion on the (legal) changes suggested in this research will provide a valuable insight on how these theoretical and legal rules function in real life investigations. Globalization requires mutual understanding and cooperation. This research has shown that legal systems which seem different at first hand, can have many similarities when understood in their broader context. Law comparison is therefore useful, since it can facilitate mutual understanding and cooperation in a globalizing world.

Bibliography

§1. Legislation

European law and legislative documents

European Convention on Human Rights of 4 November 1950 (ECHR), *BS* 19 August 1955.

The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, *Official Journal L 239*, 22/09/2000 P. 0019 – 0062.

Belgian law and legislative documents

Grondwet (Gw.), *BS* 17 February 1994.

Wetboek van Strafvordering (Sv.) – Eerste Boek, *BS* 27 November 1808.

Wetboek van Strafvordering (Sv.) – Boek II, Titel I, *BS* 29 November 1808.

Wetboek van Strafvordering (Sv.) – Boek II, Titel II, *BS* 19 December 1808.

Strafwetboek (Sw.), *BS* 9 June 1867.

Wet van 17 april 1878 houdende de Voorafgaande Titel van het Wetboek van Strafvordering (V.T.Sv.), *BS* 25 April 1878.

Wet op het Politieambt (WPA), *BS* 22 December 1992.

Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 May 2003.

Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en

bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS* 17 January 2017.

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 September 2018.

KB van 17 oktober 2018 tot uitvoering van artikel 46*sexies*, §1, tweede lid van het Wetboek van Strafvordering, *BS* 19 November 2018.

Ministeriële Omzendbrief van 24 april 1990 betreffende de bijzondere opsporingstechnieken om de zware of georganiseerde criminaliteit te bestrijden, *Parl.doc.* nr. 1-447/4 A.

MvT bij het wetsontwerp betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *Parl.St.* Kamer 2001-02, nr. 1688/001.

MvT bij het wetsontwerp van 8 juli 2016 betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, *Parl.St.* Kamer 2015-16, nr. 54-1966/001.

Tweede tussentijds verslag van de parlementaire commissie van onderzoek naar de georganiseerde criminaliteit in België over De impact van de bestrijding van de georganiseerde criminaliteit, onder meer door het gebruik van bijzondere opsporingsmethoden, op de organisatie van de politiediensten en het openbaar ministerie, *Parl.doc.* nr. 1-326/8.

US law and legislative documents

First Amendment to the United States Constitution, 15 December 1791.

Fourth Amendment to the United States Constitution, 15 December 1791.

Fifth Amendment to the United States Constitution, 15 December 1791.

Sixth Amendment to the United States Constitution, 15 December 1791.

Fourteenth Amendment to the United States Constitution, 9 July 1868.

Privacy Act 5 U.S.C. §552a - Records maintained on individuals.

18 U.S.C. §2518 - Procedure for interception of wire, oral, or electronic communications.

18 U.S.C. §2703 - Required disclosure of customer communications or records.

Undercover Operations Act: Hearing Before the S. Subcomm. on Criminal Law of the S. Comm. on the Judiciary, 98th Cong. 8 (1984), <https://www.congress.gov/bill/98th-congress/senate-bill/804> (consultation 13 December 2020).

ASHCROFT, J., *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations*, 2002, <https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf>, 19 p.

ATTORNEY GENERAL, *The Attorney General's Guidelines for Domestic FBI Operations*, 2008, <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, 46 p.

OFFICE OF THE ATTORNEY GENERAL, *Undercover and sensitive operations unit, attorney general's guidelines on FBI undercover operation*, 1992, <https://www.justice.gov/archives/ag/undercover-and-sensitive-operations-unit-attorney-generals-guidelines-fbi-undercover-operations>.

THE ONLINE INVESTIGATIONS WORKING GROUP, *Online investigative principles for federal law enforcement agents*, 1999, <https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf>, 67 p.

U.S. DEPARTMENT OF JUSTICE, 29. *Electronic Surveillance—Title III Affidavits*, 2018, <https://www.justice.gov/archives/jm/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits>.

U.S. DEPARTMENT OF JUSTICE, *FBI Domestic Investigations and Operations Guide, Part I*, 2016, <https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view>, 457 p.

§2. Case law

European case law

ECtHR 24 November 1986, Unterpertinger/Austria, *Publ.Eur.CourtH.R.* 1987, Serie A, nr. 110.

ECtHR 21 June 1988, nr. 10730/84, Berrehab/The Netherlands, *Publ.Eur.CourtH.R.* 1988, Serie A, nr. 138.

ECtHR 20 November 1989, Kostovski/The Netherlands, *Rev.trim.DH* 1990, 267, *Publ.Eur.CourtH.R.* 1989, Serie A, nr. 166.

ECtHR 24 April 1990, Huvig/France, *Publ.Eur.CourtH.R.* 1990, Serie A, nr. 176-B.

ECtHR 19 December 1990, Delta/France, *Rev.trim.DH* 1992, 47, *Publ.Eur.CourtH.R.* 1991, Serie A, nr. 191-A.

ECtHR 15 June 1992, Lüdi/Switzerland, *Juristenkrant* 2006, Vol.121, 2, *Rev.trim.DH* 1993, 309, *Publ.Eur.CourtH.R.* 1992, Serie A, nr. 238.

ECtHR 16 February 2000, nr. 27052/95, Jasper/United Kingdom, *Juristenkrant* 2000, Vol.5, 4, *RW* 2002-03, Vol.6, 233.

ECtHR 4 May 2000, nr. 28341/95, Rotaru/Romania, *Rev.trim.DH* 2001, 137.

ECtHR 8 April 2003, nr. 39339/98, M.M./The Netherlands, *T.Strafr.* 2003, Vol.6, 288.

ECtHR 8 July 2003, nr. 36022/97, Hatton a.o./United Kingdom, *Amén.* 2003, Vol.4, 239, *J.T.dr.eur.* 2003, Vol.101, 213, *MER* 2003, Vol.3, 271, *NJW* 2004, Vol.61, 228, *RW* 2004-05, Vol.12, 476.

ECtHR 2 December 2008, nr. 2872/02, K.U./Finland, *AM* 2009, Vol.1-2, 123, *Juristenkrant* 2009, Vol.181, 5, *RDTI* 2009, Vol.34, 93, *T.Strafr.* 2009, Vol.1, 38.

ECtHR 21 June 2011, nr. 30194/09, Shimovolos/Russia, *T.Strafr.* 2011, Vol.5, 360, *TVW* 2011, Vol.3, 263, *Vigiles* 2012, Vol.5, 446.

ECtHR 17 April 2012, nr. 20071/07, Piechowicz/Poland.

ECtHR 11 February 2014, nr. 16463/08, Sandu/Moldova.

ECtHR 24 April 2014, nr. 6228/09, 19678/07, 52340/08, 7451/09, 19123/09, Lagutin a.o./Russia, *T.Strafr.* 2014, Vol.3, 199.

ECtHR 1 July 2014, nr. 43835/11, S.A.S./France, *Juristenkrant* 2014, Vol.295, 2, *RW* 2015-16, Vol.23, 916, *T.Strafr.* 2014, Vol.5, 328.

ECtHR 12 January 2016, nr. 37138/14, Szabo and Vissy/Hungary, *TVW* 2016, Vol.2, 159.

ECtHR 23 February 2016, nr. 11138/10, Mozer/Republic of Moldova and Russia, *RW* 2016-17, Vol.36, 1436.

ECtHR 23 May 2017, nr. 67496/10, 52936/12, Van Wesenbeeck/Belgium, *JLMB* 2017, Vol.23, 1079, *RW* 2017-18, Vol.38, 1514.

Belgian case law

Arbitragehof 21 December 2004, nr. 202/2004, A.A. 2004, Vol.5, 2283, *BS* 6 January 2005, 368, *Juristenkrant* 2005, Vol.101, 7, *NJW* 2005, Vol.104, 340, *RW* 2004-05, Vol.33, 1290, *Rev.dr.pén.* 2005, Vol.6, 629, *T.Strafr.* 2005, Vol.3, 199, *TBP* 2006, Vol.2, 106.

GwH 19 July 2007, nr. 105/2007, *BS* 13 August 2007, 42941, *JLMB* 2008, Vol.14, 598, *NJW* 2007, Vol.168, 695, *RABG* 2008, Vol.1, 3, *Rev.dr.pén.* 2007, Vol.12, 1118, *RW* 2007-08, Vol.2, 85, *RW* 2007-08, Vol.43, 1811, *TBP* 2008, Vol.5, 286, *TGR-TWVR* 2008, Vol.1, 55, *T.Strafr.* 2007, Vol.4, 254.

GwH 31 July 2008 (preliminary question), nr. 111/2008, *A.GrwH* 2008, Vol.3, 1809, *BS* 15 September 2008, 47853, *Juristenkrant* 2008, Vol.174, 3, *Rev.dr.pén.* 2009, Vol.1, 65, *RW* 2008-09, Vol.1, 44, *RW* 2008-09, Vol.9, 360.

GwH 30 September 2009 (preliminary question), nr. 150/2009, *BS* 29 December 2009, 82208.

GwH 3 December 2009, nr. 196/2009, *A.GrwH* 2009, Vol.5, 2693, *BS* 4 January 2010, 2, *RW* 2009-10, Vol.19, 813, *RW* 2010-11, Vol.10, 420.

GwH 6 December 2018, nr. 174/2018, *BS* 22 January 2019, 7686, *Computerr.* 2019, Vol.2, 134, *NJW* 2019, Vol.398, 201, *NC* 2019, Vol.5, 436, *Rev.dr.pén.* 2019, Vol.5, 684, *RW* 2018-19, Vol.29, 1159, *T.Strafr.* 2019, Vol.5, 243, *TVW* 2019, Vol.1, 40.

Cass. 3 April 2001, *Arr.Cass.* 2001, Vol.4, 595, *Pas.* 2001, Vol.4, 589, *T.Strafr.* 2001, 338.

Cass. 31 October 2006, *Arr.Cass.* 2006, Vol.10, 2198, *Pas.* 2006, Vol.11, 2235, *Rev.dr.pén.* 2007, Vol.6, 616.

Cass. 31 October 2006, *Vigiles* 2007, Vol.3, 93.

Cass. 31 October 2006, *NC* 2007, Vol.1, 61.

Cass. 14 October 2008, *Arr.Cass.* 2008, Vol.10, 2226, *Juristenkrant* 2008, Vol.180, 5, *JT* 2008, Vol.6333, 755, *NC* 2008, Vol.6, 458, *Pas.* 2008, Vol.10, 2215, *Rev.dr.pén.* 2009, Vol.1, 92, *TBP* 2009, Vol.8, 492-493.

Cass. 16 February 2010, *Arr.Cass.* 2010, Vol.2, 460, *NC* 2010, Vol.2, 127, *Pas.* 2010, Vol.2, 483, *P&B* 2010, Vol.6, 212, *T.Strafr.* 2011, Vol.3, 195.

Cass. 27 July 2010, *Arr.Cass.* 2010, Vol.6-7-8, 2052, *Pas.* 2010, Vol.6-8, 2145.

Cass. 14 September 2010, *Arr.Cass.* 2010, Vol.9, 2186, *Pas.* 2010, Vol.9, 2263, *RW* 2011-12, Vol.38, 1670, *TGR-TWVR* 2011, Vol.2, 136, *T.Strafr.* 2011, Vol.3, 196.

Cass. 23 November 2010, *Arr.Cass.* 2010, Vol.11, 2823, *Pas.* 2010, Vol.11, 3011, *T.Strafr.* 2011, Vol.3, 198.

Cass. 9 October 2013, *Arr.Cass.* 2013, Vol.10, 2061, *Pas.* 2013, Vol.10, 1903.

Cass. 26 February 2014, *Arr.Cass.* 2014, Vol.2, 534, *Pas.* 2014, Vol.2, 507, *Rev.dr.pén.* 2014, Vol.7-8, 791.

Cass. 28 May 2014, *Arr.Cass.* 2014, Vol.5, 1361, *Pas.* 2014, Vol.5, 1336, *RABG* 2015, Vol.1, 36, *Rev.dr.pén.* 2014, Vol.9-10, 959, *T.Strafr.* 2015, Vol.1, 26.

Cass. 10 February 2015, *Arr.Cass.* 2015, Vol.2, 244, *Pas.* 2015, Vol.2, 310, *T.Strafr.* 2015, Vol.3, 139.

Cass. 25 March 2015, *Arr.Cass.* 2015, Vol.3, 830, *NC* 2017, Vol.5, 490, *Pas.* 2015, Vol.3, 811, *Rev.dr.pén.* 2015, Vol.9-10, 979.

Cass. 30 June 2015, *Arr.Cass.* 2015, Vol.6-8, 1802, *Pas.* 2015, Vol.6-7-8, 1784, *T.Strafr.* 2016, Vol.2, 170.

Cass. 6 September 2016 (R.E.J.P.).

Cass. 28 March 2017, *Juristenkrant* 2017, Vol.351, 3, *NC* 2017, Vol.4, 381, *Rev.dr.pén.* 2019, Vol.5, 702, *T.Strafr.* 2017, Vol.5, 329.

Brussels 19 November 1984, *Pas.* 1985, II, 37, *RW* 1984-85, 2563.

Bergen 5 May 1992, *JLMB* 1993, 12, *Rev.dr.pén.* 1992, 890.

Antwerp 6 January 1993, *Turnh. Rechtsl.* 1993, 28, *Turnh. Rechtsl.* 1993, 68.

Brussels 7 September 1994, *JLMB* 1994, 1135, *Journ. proc.* 1994, Vol.268, 25, *Pas.* 1993, II, 112, *Rev.dr.pén.* 1995, 419.

Antwerp 21 May 1997, *Limb.Rechtsl.* 1997, 223.

Antwerp 10 November 2016, *Limb.Rechtsl.* 2018, Vol.2, 132.

Corr. Brussels 12 April 1994, *Rev.dr.pén.* 1995, 423.

Corr. Antwerp 27 October 2016, *Computerr.* 2017, Vol.1, 35, *Juristenkrant* 2016, Vol.337, 4, *NJW* 2016, Vol.353, 921, *NC* 2017, Vol.1, 89, *TRNI* 2017, Vol.1, 91.

KI Ghent 6 December 2004, *RABG* 2005, Vol.13, 1215, *T.Strafr.* 2005, Vol.3, 227.

US case law

Ex parte Jackson, 96 U.S. 727 (1878).

Sorrells v. United States, 287 U.S. 435 (1932).

Brown v. Mississippi, 297 U.S. 278 (1936).

Everson v. Board of Education, 330 U.S. 1 (1947).

Rochin v. California, 342 U.S. 165 (1952).

Sherman v. United States, 356 U.S. 369 (1958).

NAACP v. Patterson, 357 U.S. 449 (1958).

Gideon v. Wainwright, 372 U.S. 335 (1963).

Lopez v. United States, 373 U.S. 427 (1963).

Massiah v. United States, 377 U.S. 201 (1964).

Griswold v. Connecticut, 381 U.S. 479 (1965).

Miranda v. Arizona, 384 U.S. 436 (1966).

Lewis v. United States, 385 U.S. 206 (1966).

Hoffa v. United States, 385 U.S. 293 (1966).

Osborn v. United States, 385 U.S. 323 (1966).

United States v. Robel, 389 U.S. 258 (1967).

Katz v. United States, 389 U.S. 347 (1967).

United States v. White, 401 U.S. 745 (1971).

State v. Rowan, 288 N.E.2d 829 (Ohio Ct. App. 1972).

United States v. Russell, 411 U.S. 423 (1973).

Socialist Workers Party v. Attorney General, 419 U.S. 1314 (1974).

United States v. Miller, 425 U.S. 435 (1976).

Hampton v. United States, 425 U.S. 484 (1976).

United States of America v. Michael Leja and John M. Cody, 563 F.2d 244 (6th Cir. 1977).

Brewer v. Williams, 430 U.S. 387 (1978).

United States v. Prairie, 572 F.2d 1316 (9th Cir. 1978).

United States of America v. James B. Borum, 584 F.2d 424 (D.C. Cir. 1978).

Smith v. Maryland, 442 U.S. 735 (1979).

United States v. Jannotti, 501 F.Supp. 1182 (E.D. Pa. 1980).

United States v. Wylie, 625 F.2d 1371 (9th Cir. 1980).

United States v. Myers, 527 F.Supp. 1206 (E.D.N.Y. 1981).

United States v. Fekri, 650 F.2d 1044 (9th Cir. 1981).

United States v. Kelly, 539 F.Supp. 363 (D.D.C. 1982).

State v. Hohensee, 650 S.W.2d 268 (Mo. Ct. App. 1982).

United States v. Parisi, 674 F.2d 126 (1st Cir. 1982).

United States v. Knotts, 460 U.S. 276 (1983).

United States v. Karo, 468 U.S. 705 (1984).

California v. Greenwood, 486 U.S. 35 (1988).

Patterson v. Illinois, 487 U.S. 285 (1988).

Vaden v. State, 768 P.2d 1102 (Alaska 1989).

United States of America v. Marian Fusko, 869 F.2d 1048 (7th Cir. 1989).

Illinois v. Perkins, 496 U.S. 292 (1990).

Jacobson v. United States, 503 U.S. 540 (1992).

U.S. v. Skarie, 971 F.2d 317 (9th Cir. 1992).

United States v. Daniel A. Gendron, 18 F.3d 955 (1st Cir. 1994).

Anderson v. Davila, 125 F.3d 148 (3rd Cir. 1997).

U.S. v. Kennedy, 81 F.Supp.2d 1103 (D. Kan. 2000).

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

Osburn v. Nevada, 118 Nev. 323 (Nev. 2002).

Sealed Case, 310 F.3d 717 (F.I.S.C. 2002).

United States v. Nettles, 400 F.Supp.2d 1084 (N.D. Ill. 2005).

United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).

Montejo v. Louisiana, 556 U.S. 778 (2009).

United States v. Smith, 387 Fed.Appx. 918 (11th Cir. 2010).

United States v. Marquez, 605 F.3d 604 (8th Cir. 2010).

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

United States v. Jones, 132 S.Ct. 945 (2012).

United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012).

People v. Harris, 949 N.Y.S.2d 590 (City Crim. Ct. 2012).

Bland v. Roberts, No. 12-1671 (4th Cir. 2013).

United States v. Gatson, Criminal No. 13-705 (D.N.J. Dec. 15, 2014).

Arquiett v. United States, No. 13-CV-0752, *Stipulation for Voluntary Dismissal, Compromise Settlement, and Release of Claims*, http://online.wsj.com/public/resources/documents/2015_0120_Arquiettsettlement.pdf.

Hassan *et al.* v. City of New York, No. 14-1688 (3rd Cir. 2015).

United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).

Packingham v. North Carolina, 137 S.Ct. 1730 (2017).

Carpenter v. United States, No. 16–402, 585 U.S. (2018).

§3. Literature

Legal Doctrine

ARSHAD IMTIAZ, A., “Off the Record: Police Surveillance, Muslim Youth and an Ethnographer’s Tools of Research”, *Equity & Excellence in education* 2018, Vol.51(3-4), 431-449.

AUVRET-FINCK, J., *L'Union européenne et la lutte contre le terrorisme*, Brussels, Larcier, 2010, 331 p.

BAIL, C., MERHOUT, F. and DING, P., “Using Internet search data to examine the relationship between anti-Muslim and pro-ISIS sentiment in U.S. counties”, *Science Advances* 2018, Vol.4(6), 1-9.

BARD, J., “Unpacking the Dirtbox: Confronting Cell Phone Location Tracking with the Fourth Amendment”, *Boston College Law Review* 2016, Vol.57(2), 731-764.

BEIRENS, L., “De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace”, *Orde van de dag* 2010, Vol.3, 51-68.

BELL, B.W., “Secrets and lies: news media and law enforcement use of deception as investigative tool”, *University of Pittsburgh Law Review* 1999, Vol.60(3), 745-837.

BELL, B.W., “Theatrical Investigation: White-Collar Crime, Undercover Operations, and Privacy”, *William & Mary Bill of Rights Journal* 2002, Vol.11(1), 151-208.

BERKMOES, H., “De koudwatervrees voor de wettelijke regeling van de bijzondere opsporingsmethoden”, *Orde van de dag* 2003, Vol.4, 25-36.

BERKMOES, H., “Identificatie van (gebruikers van) elektronische communicatie” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Samsom, 2018, 3/01-3/55.

BERKMOES, H., “Actualia BOM en enige andere opsporings- en onderzoekshandelingen”, *NC* 2019, Vol.5, 361-388.

BERKMOES, H., “Bijzondere opsporingsmethoden (observatie, infiltratie, informantenwerking)” in *Postal-Memorialis: lexicon strafrecht, strafvordering en bijzondere wetten*, Brussels, Ced.Sansom, 2019, 216/01-216/78.

BERRY, D., “The First Amendment and Law Enforcement Infiltration of Political Groups”, *Southern California Law Review* 1982, Vol.56(1), 207-240.

BILLIS, E., “On the methodology of comparative criminal law research: Paradigmatic approaches to the research method of functional comparison and the heuristic device of ideal types”, *Maastricht journal of European and comparative law* 2017, Vol.24(6), 864-881.

BIRCHALL, C., “Introduction to ‘Secrecy and Transparency’: The Politics of Opacity and Openness”, *Theory, Culture & Society* 2011, Vol.28, 7-25.

BLANTON, T., “The World’s Right to Know”, *Foreign Policy* 2002, Vol.131, 50-58.

BLOSS, W., “Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects”, *Surveillance & Society* 2007, Vol.4(3), 208-228.

BORKOWSKI, R., “Kontrterrorizm i antyterrorizm (aspekty teoretyczne i praktyczne)”, *Bezpieczeństwo. Teoria i Praktyka* 2016, Vol.XXIV(3), 39-50.

BRAAT, E., “In voor- en tegenspoed: Het huwelijk tussen parlement en inlichtingen- en veiligheidsdiensten”, *Justitiële verkenningen* 2018, Vol.44(1), 33-48.

BRUGGEMAN, W., “Politie, justitie en (nieuwe) sociale media”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), 199-204.

BURN, O.S., “Abscam Ethics: Moral Issues And Deception In Law Enforcement edited by Gerald M. Caplan”, *Journal of Criminal Justice* 1984, Vol.12(1), 93-94.

CARLON, A., “Entrapment, Punishment, and the Sadistic State”, *Virginia Law Review* 2007, Vol.93(4), 1081-1134.

CARLSON, J.C., “The Act Requirement and the Foundations of the Entrapment Defense”, *Virginia Law Review* 1987, Vol.73(6), 1011-1108.

CHAWKI, M., DARWISH, A., KHAN, M.A. and TYAGI, S., *Cybercrime, Digital Forensics and Jurisdiction*, Switzerland, Springer International Publishing, 2015, 145 p.

CHIN, Y.-L., “Evgeny Morozow, The Net Delusion: How Not to Liberate the World: Reviewed”, *New Media & Society* 2012, Vol.14(5), 890-892.

CLEMENTE, D., “The net delusion: how not to liberate the world by Evgeny Morozow: reviewed”, *International Affairs* 2013, Vol.89(1), 197-198.

CONINGS, C. and VAN LINTHOUT, P., “Sociale media: Een nieuwe uitdaging voor politie en justitie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), 205-230.

CONINGS, C. and ROYER, S., “Verzamelen en vastleggen van digitaal bewijs in strafzaken” in *Topics bewijs- en procesrecht*, Mortsel, Intersentia, 2017, 99-151.

CONINGS, C., “De politie op het darknet”, *T.Strafr.* 2017, Vol.5, 331-334.

CONINGS, C., “Wetgever maakt digitaal speurwerk makkelijker”, *Juristenkrant* 2017, Vol.19, 3.

CONINGS, C., “Grondwettelijk Hof buigt zich over de wet digitale recherche”, *T.Strafr.* 2019, Vol.5, 257-261.

CUNHA, A., SILVA, M. and FREDERICO, R., *The borders of Schengen*, Brussels, P.I.E. Peter Lang, 2015, 195 p.

DANNEMANN, G., “Comparative Law: Study of Similarities or Differences?” in REIMANN, M. and ZIMMERMANN, R., *The Oxford handbook of comparative law*, Oxford, Oxford University press, 2019, 391-422.

DE BONO, E., “Investigating Social Networking Sites” in SHIPLEY, T.G. and BOWKER, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, 315-344.

DELMULLE, J., “Wat na het arrest van 21 december 2004 van het Arbitragehof? De kamer van inbeschuldigingstelling als onpartijdige en onafhankelijke rechter belast met de controle over de toepassing van de bijzondere opsporingsmethoden observatie en infiltratie? Een eerste toetsing aan de praktijk.”, *T.Strafr.* 2005, Vol.3, 230-234.

DEN BOER, M., *Undercover Policing and Accountability from an International Perspective*, Maastricht, EIPA, 1997, 218 p.

DE PAUW, E., “Sociale controle in onlinegemeenschappen: een taak voor de overheid of volstaat zelfregulering?”, *Orde van de dag* 2010, Vol.3, 5-14.

DE PAUW, E., *Veilig online: over sociale controle bij netwerksites*, Mechelen, Kluwer, 2010, 70 p.

DE SMET, S., “Een sociale media-strategie voor de politie”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), 231-245.

DIAZ, A., *New York City Police Department Surveillance Technology*, New York, New York University School of Law, 2019, 16 p.

DRIPPS, D.A., “At the Borders of the Fourth Amendment: Why a Real Due Process Test Should Replace the Outrageous Government Conduct Defense”, *University of Illinois Law Review* 1993, Vol.2, 261-284.

DWORKIN, G., “The Serpent Beguiled Me and I Did Eat: Entrapment and the Creation of Crime”, *Law and Philosophy* 1985, Vol.4(1), 17-39.

FERNANDEZ-SANCHEZ, P.A., *International legal dimension of terrorism*, Leiden, Martinus Nijhoff Publishers, 2009, 512 p.

FIELD, S. and PELSER, C., *Invading the private: state accountability and new investigative methods in Europe*, Aldershot, Ashgate, 1998, 388 p.

FIJNAUT, C., *De zaak-François: beschouwingen naar aanleiding van het vonnis*, Antwerp, Kluwer, 1983, 192 p.

FIJNAUT, C., “The Schengen Treaties and European Police Co-operation”, *European Journal of Crime, Criminal Law and Criminal Justice* 1993, Vol.1(1), 37-56.

FIJNAUT, C. and MARX, G.T., *Undercover: police surveillance in comparative perspective*, The Hague, Kluwer Law International, 1995, 337 p.

FIJNAUT, C., “De exfiltratie van verdachte en veroordeelde criminelen”, *Justitiële verkenningen* 2012, Vol.38(3), 68-84.

FIJNAUT, C., *Een vreedzame revolutie*, Morsel, Intersentia, 2018, 1068 p.

FORAN, T., “Covert Operations on the Internet” in SHIPLEY, T.G. and BOWKER, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, 233-252.

FUSON, H., “Fourth Amendment Searches in First Amendment Spaces: Balancing Free Association with Law and Order in the Age of the Surveillance State”, *The University of Memphis law review* 2020, Vol.50(1), 231-285.

GERSHMAN, B.L., “Abscam, the Judiciary, and the Ethics of Entrapment”, *The Yale Law Journal* 1982, Vol.91, 1565-1591.

GUENTER, S. and SCHUERMANS, F., “Enkele recente Antigoon-evoluties en de toepassing ervan op een onregelmatige observatie en/of infiltratie”, *T.Strafr.* 2013, Vol.5, 329-335.

GUIORA, A.N., “Transnational Comparative Analysis of Balancing Competing Interests in Counter-Terrorism”, *Temple International & Comparative Law Journal* 2006, Vol.20(2), 363-394.

HARVARD LAW REVIEW ASSOCIATION, “First Amendment – Freedom of Speech – Public Forum Doctrine – Packingham v. North Carolina”, *Harvard Law Review* 2017, Vol.131(1), 233-242.

HEFFERNAN, W.C., “Fourth Amendment Privacy Interests”, *The Journal of Criminal Law and Criminology* 2001/2002, Vol.92(1/2), 1-126.

HUGHES, T. and BURTON, C., “Police GPS Surveillance on Vehicles and the Warrant Requirement: For a While I’ve Been Watching You Steady”, *Am.J.Crim.Just.* 2013, Vol.38, 535-550.

HUTSEBAUT, F. and VAN CAUWENBERGHE, K., “De wet betreffende de bijzondere opsporingsmethoden (B.O.M.). Waarheen met de rechtszekerheid?”, *Orde van de dag* 2003, Vol.4, 7-14.

INTERNATIONAL BAR ASSOCIATION, *International terrorism: legal challenges and responses: a report by the International bar association's task force on international terrorism*, London, International bar association, 2003, 186 p.

JOH, E.E., "Breaking the law to enforce it: Undercover police participation in crime", *Stanford Law Review* 2009, Vol.62(1), 155-199.

JOH, E.E., "Bait, Mask, and Ruse: Technology and Police Deception", *Harvard Law Review Forum* 2015, Vol.128, 246-252.

JOHNSON, N.F., ZHENG, M., VOROBYEVA, Y., GABRIEL, A., QI, H., VELASQUEZ, N., MANRIQUE, P., JOHNSON, D., RESTREPO, E., SONG, C. and WUCHTY, S., "New online ecology of adversarial aggregates: ISIS and beyond", *Science* 2016, Vol.352(6292), 1459-1463.

KOOPS, B.-J., "Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research" in AKHGAR, B. and BREWSTER, B., *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Switzerland, Springer International Publishing, 2016, 3-15.

KORF, D.J., KLEEMANS, E., DECORTE, T. and BOEKHOUT VAN SOLINGE, T., "Drugs en drugshandel in Nederland en België", *Tijdschrift voor Criminologie* 2006, Vol.48(2), 115-130.

KOWALCZYK, D. and SHARPS, M.J., "Consequences of Undercover Operations in Law Enforcement: a Review of Challenges and Best Practices", *Journal of Police and Criminal Psychology* 2017, Vol.32, 197-202.

KRUISBERGEN, E.W. and DE JONG, D., "Undercoveroperaties: een noodzakelijk kwaad?", *Justitiële verkenningen* 2012, Vol.38(3), 50-67.

LASSER, M. De S.-O.-L'E., "The question of understanding" in LEGRAND, P. and MUNDAY, R. (eds.), *Comparative legal studies: traditions and transitions*, Cambridge, Cambridge University Press, 2003, 197-239.

LEIGH, I., "Undercover: Police Surveillance in America By G.T. Marx: Reviewed", *British Journal of Criminology* 1991, Vol.31(1), 100-101.

LEMMENS, K., “Misbruiken van de meningsvrijheid via internet: is het recht Web 2.0-compatibel? Pleidooi voor een technologieneutrale bescherming van de uitingsvrijheid”, *Orde van de dag* 2010, Vol.3, 15-22.

LETSCHERT, R., PEMBERTON, A. and STAIGER, I., *Assisting Victims of Terrorism*, The Netherlands, Springer, 2010, 375 p.

LEVINSON, S., “The Hidden Costs of Infiltration”, *The Hastings Center Report* 1982, Vol.12(4), 29-37.

LEVINSON-WALDMAN, R., “Government Access to and Manipulation of Social Media: Legal and Policy Challenges”, *Howard Law Journal* 2018, Vol.61(3), 523-562.

LEVINSON-WALDMAN, R., “Private Eyes, They’re Watching You: Law Enforcement’s Monitoring of Social Media”, *Oklahoma Law Review* 2019, Vol.71(4), 997-1012.

LIEBERMAN, A.V., “Terrorism, the Internet, and Propaganda: A Deadly Combination”, *Journal of National Security Law & Policy* 2017, Vol.9(1), 95-124.

LUSTGARTEN, L., “Undercover: police surveillance in comparative perspective: Reviewed”, *Public Law* 1997, 575-577.

MARSHALL, E.W., GROSCUP, J.L., BRANK, E.M., PEREZ, A. and HOETGER, L.A., “Police surveillance of cell phone location data: Supreme Court versus public opinion”, *Behavioral Sciences & The Law* 2019, Vol.37(6), 751–775.

MARX, G.T., “The New Police Undercover Work”, *Journal of Contemporary Ethnography* 1980, Vol.8(4), 399-446.

MARX, G.T., “Who really gets stung? Some issues raised by the New Police Undercover Work”, *Crime & Delinquency* 1982, Vol.28(2), 165-193.

MARX, G.T., *Undercover: police surveillance in America*, Berkeley, University of California press, 1988, 283 p.

MARX, G.T., “A Tack in the Shoe: Neutralizing and Resisting the New Surveillance”, *Journal of Social Issues* 2003, Vol.59(2), 369-390.

MEARES, T.L., “Law of Community Policing and Public Order Policing” in BRUINSMA, G. and WEISBURD, D. (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, 2823-2827.

MEESE, J., “Bijzondere opsporingsmethoden en andere onderzoeksmethoden”, *NJW* 2003, Vol.11, 1134-1153.

MICHAELS, R., “The Functional Method of Comparative Law” in REIMANN, M. and ZIMMERMANN, R., *The Oxford handbook of comparative law*, Oxford, Oxford University press, 2019, 346-389.

MITCHELL, K.J., WOLAK, J. and FINKELHOR, D., “Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working?”, *Sexual Abuse: A Journal of Research and Treatment* 2005, Vol.17(3), 241-267.

MOROZOV, E., “WikiLeaks and the Perils of Extreme Glasnost”, *New Perspectives Quarterly* 2011, Vol.28(1), 7-11.

NADELMANN, E.A., *Cops across borders: the internationalization of US criminal law enforcement*, University Park, Pennsylvania State university press, 1993, 524 p.

OERLEMANS, J.-J., “Facebookvrienden worden met de verdachte”, *Justitiële verkenningen* 2018, Vol.44(5), 83-99.

PATAKI, G., “Conducting Reactive and Proactive Internet Investigations” in SHIPLEY, T.G. and BOWKER, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Syngress, 2014, 253-268.

RADLER, M., “Privacy is the Problem: United States v. Maynard and a Case for a New Regulatory Model for Police Surveillance”, *Geo.Wash.L.Rev.* 2012, Vol.80(4), 1209-1254.

ROIPHE, R., “The Serpent Beguiled Me: A History of the Entrapment Defense”, *Seton Hall Law Review* 2003, Vol.33(2), 257-302.

ROSENZWEIG, P., “Civil Liberty and the Response to Terrorism”, *Duquesne Law Review* 2004, Vol.42(4), 663-724.

ROSS, J.E., “Valuing inside knowledge: Police Infiltration as a problem for the law of evidence”, *Chicago-Kent Law Review* 2004, Vol.79(3), 1111-1149.

ROSS, J.E., “The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany”, *The American Journal of Comparative Law* 2007, Vol.55, 493-579.

ROSS, J.E., “Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint”, *Annu.Rev.Law Soc.Sci.* 2008, Vol.4, 239-273.

ROSS, J.E., “Law of Undercover Policing” in BRUINSMA, G. and WEISBURD, D. (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, 2865-2871.

ROYER, S., “Medewerkingsplicht van een telecommunicatiedienst”, *NJW* 2016, Vol.353, 928-929.

ROYER, S., “Wet 25 december 2016 digitaal spoorwerk op twee punten vernietigd (noot onder GwH 6 december 2018)”, *NJW* 2019, Vol.398, 212.

SCHBLEY, A., “Defining Religious Terrorism: A Causal and Anthological Profile”, *Studies in Conflict & Terrorism* 2003, Vol.26(2), 105-134.

SCHEPPELE, K., “Other People's Patriot Acts: Europe's Response to September 11”, *Loyola Law Review* 2004, Vol.50(1), 89-148.

SCHOUKENS, P., HENDRICKX, K., TERRY, E. and KESTEMONT, L., *Rechtswetenschappelijk schrijven*, Leuven, Acco, 2012, 135 p.

SCHUERMANS, F. and BERKMOES, H., “De BOM-reparatiewet van 27 december 2005: het klein onderhoud, de reparatie en de revisie van de bijzondere en enige andere opsporingsmethoden”, *T.Strafr.* 2006, Vol.2, 65-77.

SCHUERMANS, F., “Grondwettelijk Hof plaatst politie en magistraten voor praktische en juridische 'BOM-problemen'”, *Juristenkrant* 2008, Vol.165, 8.

SCHUERMANS, F., “Cassatie zet nieuwe BOM-bakens uit”, *Juristenkrant* 2008, Vol.180, 5.

SCHUERMANS, F., “De wettigheidscontrole van de observatie en infiltratie”, *T.Strafr.* 2015, Vol.1, 27-28.

SCHUERMANS, F., “Cassatie vult wettelijke leemte op over politionele internetpatrouille- en recherche”, *Juristenkrant* 2017, Vol.351, 3.

SEIDMAN, L.M., “The Supreme Court, Entrapment, and Our Criminal Justice Dilemma”, *Supreme Court Review* 1981, 111-156.

SHAMAS, D. and ARASTU, N., *Mapping Muslims: NYPD Spying and its Impact on American Muslims*, Long Island City NY, Muslim American Civil Liberties Coalition (MACLC) and Creating Law Enforcement Accountability & Responsibility (CLEAR) Project, 2013, 51 p.

SHERMAN, J., “A Person Otherwise Innocent: Policing Entrapment in Preventative, Undercover Counterterrorism Investigations”, *Journal of constitutional law* 2009, Vol.11(5), 1475-1510.

SHIPLEY, T.G. and BOWKER, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, Elsevier, 2014, 472 p.

SINGLETON, S., “Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques”, *Ohio Northern University Law Review* 2004, Vol.30(3), 417-450.

SIO-LOPEZ, C.B., “Dialogues beyond the ‘Fortress Europe’: Tracing back the genesis and evolution of the ‘free circulation of persons’ concept through EP Schengen Area debates, 1985-2015” in CUNHA, A., SILVA, M. and FREDERICO, R., *The borders of Schengen*, Brussels, P.I.E. Peter Lang, 2015, 32-50.

SMITH, C.E., “The Bill of Rights after September 11th: Principles or Pragmatism”, *Duquesne Law Review* 2004, Vol.42(2), 259-292.

SPAPENS, T., KOLTHOFF, E. and STOL, W., “Georganiseerde misdaad in de 21^{ste} eeuw”, *Tijdschrift voor Criminologie* 2016, Vol.58(2), 1-18.

STOL, W., “Filteren van internet: een politietaak?”, *Orde van de dag* 2010, Vol.3, 43-50.

STOL, W.PH., LEUKFELDT, E.R. and KLAP, H., “Cybercrime en politie: een schets van de Nederlandse situatie anno 2012”, *Justitiële verkenningen* 2012, Vol.38(1), 25-39.

TAWIL, D.D., “Ready-Induce-Sting: Arguing for the Government’s Burden of Proving Readiness in Entrapment Cases”, *Michigan Law Review* 2000, Vol.98(7), 2371-2394.

TEMMERMAN, K., *Terreurbestrijding in België en Europa: de interactie tussen inlichtingendiensten, politie en justitie*, Antwerp, Maklu, 2007, 205 p.

THIENPONT, A., “Nieuwe BOM-wet legt bom onder fundamentele rechten en vrijheden”, *Juristenkrant* 2006, Vol.1, 2-3.

THOMAS, G.C. and LEO, R.A., “Law of Police Interrogation” in BRUINSMA, G. and WEISBURD, D. (eds.), *Encyclopedia of Criminology and Criminal Justice*, New York, Springer, 2014, 2835-2840.

TILLEMANN, B., DIRIX, E. and VAN ORSHOVEN, P., *De Valks juridisch woordenboek*, Antwerp, Intersentia, 2011, 621 p.

TURAN, T., “War on Terror in the US and UK: An Evaluation with Regard to Civil Liberties”, *Uluslararası Hukuk ve Politika* 2006, Vol.7, 111-126.

VAN GAEVER, J., “Eén jaar evolutie van de wettigheidcontrole op de bijzondere opsporingsmethoden”, *T.Strafr.* 2007, Vol.1, 61-65.

VAN KOKSWIJK, J., “Sociale controle in onlinegemeenschappen: voordelen van zelfregulering op internet”, *Orde van de dag* 2010, Vol.3, 23-34.

VANWALLEGHEM, P., “Infiltratie mag ook om verdachte te arresteren”, *De Juristenkrant* 2014, Vol.4, 2.

VERMEULEN, M. and DE HERT, P., “Toegang tot sociale media en controle door politie: Een eerste juridische verkenning vanuit mensenrechtelijk perspectief”, *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), 258-272.

WASCHKE, M., *Personal Cybersecurity: How to avoid and recover from cybercrime*, Berkeley, Apress, 2017, 240 p.

WASSERMAN, M.A., “First Amendment limitations on police surveillance: The case of the Muslim surveillance program”, *New York University Law Review* 2015, Vol.90(5), 1786-1826.

WERNERT, S., “L’Union européenne et la lutte contre le terrorisme”, *Politique étrangère* 2018, Vol.2, 133-144.

X, "Police infiltration of dissident groups", *The Journal of Criminal Law, Criminology, and Police Science* 1970, Vol.61(2), 181-194.

YAFFE, G., "The government beguiled me: The entrapment defense and the problem of private entrapment", *Journal of Ethics & Social Philosophy* 2005, Vol.1(1), 1-50.

YPERMAN, W., ROYER, S. and VERBRUGGEN, F., "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, Vol.5, 389-416.

ZIMMERMANN, D., "The European Union and Post-9/11 Counterterrorism: A Reappraisal", *Studies in Conflict & Terrorism* 2006, Vol.29(2), 123-145.

ZOURIDIS, S. and TOPS, P., "Sociale media: vehikels voor collectieve wijsheid of sociale verstoring?", *Panopticon: Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 2012, Vol.33(3), 246-257.

Internet Sources

BODNAR, A. and PUDZIANOWSKA, D., *Violation of the right to respect for private and family life in the case of K.U. vs. Finland*, <https://humanrightshouse.org/articles/violation-of-the-right-to-respect-for-private-and-family-life-in-the-case-of-k-u-v-finland/> (consultation 27 October 2020).

BOVÉ, L., *Politie mag infiltreren op internet*, <https://www.tijd.be/politiek-economie/belgie/federaal/politie-mag-infiltreren-op-internet/10037561.html> (consultation 19 November 2020).

BREWSTER, T., *Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops*, <https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/> (consultation 20 May 2021).

CLEMENT, J., *Global social networks ranked by number of users 2020*, <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (consultation 18 November 2020).

CLEMENT, J., *Number of global social network users 2017-2025*, <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/> (consultation 18 November 2020).

CLEMENT, J., *Share of internet users who have used technologies that allow access to the dark web as of February 2019, by country*, <https://www.statista.com/statistics/1015229/dark-web-access-technology-usage-by-country/> (consultation 10 December 2020).

CONGRESS CONSTITUTION ANNOTATED, *Amdt5.4.1 Right to Due Process: Overview*, https://constitution.congress.gov/browse/essay/amdt5_4_1/ (consultation 1 May 2021).

CONGRESS CONSTITUTION ANNOTATED, *Constitution of the United States: Fourteenth Amendment*, <https://constitution.congress.gov/constitution/amendment-14/> (consultation 1 May 2021).

CRIMINIS WOORDENLIJST, *Bijzondere opsporingsmethoden*, <https://joachimmeese.be/criminis/woordenlijst/bijzondere-opsporingsmethoden/> (consultation 10 October 2020).

CROOK, J., *Police Can Create Fake Instagram Accounts to Investigate Suspects*, <https://techcrunch.com/2014/12/24/police-can-create-fake-instagram-accounts-to-investigate-suspects/> (consultation 6 November 2020).

DATANNEWS, *Politie mag valse identiteit gebruiken om te infiltreren op internet*, https://datanews.knack.be/ict/politie-mag-valse-identiteit-gebruiken-om-te-infiltreren-op-internet/article-normal-1181521.html?cookie_check=1605805119 (consultation 19 November 2020).

DUKE, *Faculty David H. Schanzer*, <https://sanford.duke.edu/people/faculty/schanzer-david-h> (consultation 25 April 2021).

FACEBOOK, *Servicevoorwaarden*, <https://www.facebook.com/legal/terms> (consultation 27 October 2020).

FACEBOOK, *Welke namen zijn toegestaan op Facebook?*, https://www.facebook.com/help/112146705538576?helpref=faq_%20content (consultation 27 October 2020).

GORDON, P., *What's in a "Like"? Precedent-Setting Case Poses New Risk for Employers*, <https://www.littler.com/publication-press/publication/whats-precedent-setting-case-poses-new-risk-employers> (consultation 21 May 2021).

HEATHER, K., *Police embrace social media as crime-fighting tool*, <https://edition.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html> (consultation 18 November 2020).

HORWITZ, S., *Justice Dept. will review practice of creating fake Facebook profiles*, https://www.washingtonpost.com/world/national-security/justice-dept-will-review-practice-of-creating-fake-facebook-profiles/2014/10/07/3f9a2fe8-4e57-11e4-aa5e-7153e466a02d_story.html (consultation 6 November 2020).

JANSEN, J., *Belgische politie krijgt recht om te infiltreren op internet*, <https://tweakers.net/nieuws/141799/belgische-politie-krijgt-recht-om-te-infiltreren-op-internet.html> (consultation 19 November 2020).

JURECA, *Bijzondere opsporingsmethoden (BOM)*, <https://www.jureca.be/verklaring/bijzondere-opsporingsmethoden-bom> (consultation 10 October 2020).

KEMP, S., *Digital 2019: Global internet use accelerates*, <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates> (consultation 18 November 2020).

LICHTBLAU, E. and ARKIN, W.M., *More Federal Agencies Are Using Undercover Operations*, <https://www.nytimes.com/2014/11/16/us/more-federal-agencies-are-using-undercover-operations.html> (consultation 25 October 2020).

LINSHI, J., *Federal Drug Agency sued for creating fake Facebook profile*, <https://time.com/3479424/dea-fake-facebook-profile/> (consultation 19 November 2020).

NBC NEWS, *DEA agent sued over fake Facebook page in drug case*, <https://www.nbcnews.com/news/us-news/dea-agent-sued-over-fake-facebook-page-drug-case-n220461> (consultation 19 November 2020).

OFFICE OF THE INSPECTOR GENERAL, *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data*, <https://oig.justice.gov/reports/2019/o1901.pdf> (consultation 20 May 2021).

PETITJEAN, F., *Politie mag infiltreren via het internet*, <https://www.computable.be/artikel/nieuws/overheid/6427352/5440850/politie-mag-infiltreren-via-het-internet.html> (consultation 19 November 2020).

RAY, M., *ABSCAM United States history*, <https://www.britannica.com/topic/Abscam> (consultation 19 November 2020).

ROSMAN, C., *Terroristen communiceren ongestoord via Spelcomputer*, <https://www.ad.nl/nieuws/terroristen-communiceren-ongestoord-via-spelcomputer~ac9839ad/?referrer=https%3A%2F%2Fwww.google.com%2F> (consultation 25 October 2020).

SCHANZER, D., KURZMAN, C., TOLIVER, J. and MILLER, E., *The challenge and promise of using community policing strategies to prevent violent extremism: A call for community partnerships with law enforcement to enhance public safety, Final Report*, <https://www.ncjrs.gov/pdffiles1/nij/grants/249674.pdf> (consultation 14 November 2020).

SECURITY MANAGEMENT, *Belgische politie mag online undercover gaan*, https://www.securitymanagement.nl/belgische-politie-mag-online-undercover-gaan/?vakmedianet-approve-cookies=1&_ga=2.160358325.923604566.1605804501-1241609121.1605804501 (consultation 19 November 2020).

SULLIVAN, J., *Facebook letter to DEA*, <https://www.documentcloud.org/documents/1336541-facebook-letter-to-dea.html> (consultation 27 October 2020).

THE GUARDIAN, *Justice Department settles case after DEA set up fake Facebook page in woman's name*, <https://www.theguardian.com/us-news/2015/jan/20/justice-department-woman-settlement-fake-facebook-page-dea> (consultation 19 November 2020).

TWENEY, D., *Facebook is going after the DEA for creating fake profiles*, <https://www.businessinsider.com/facebook-is-going-after-the-dea-for-creating-fake-profiles-2014-10?IR=T> (consultation 19 November 2020).

U.S. DEPARTMENT OF JUSTICE, *Overview of the Law Enforcement Strategy to Combat International Organized Crime*, <https://www.justice.gov/sites/default/files/criminal-icitap/legacy/2015/04/23/04-23-08combat-intl-crime-overview.pdf>, (consultation 25 October 2020).

U.S. DEPARTMENT OF JUSTICE, *FBI: A brief history*, <https://www.fbi.gov/history/brief-history> (consultation 12 November 2020).

U.S. DEPARTMENT OF JUSTICE, *ABSCAM*, <https://www.fbi.gov/history/famous-cases/abscam> (consultation 19 November 2020).

U.S. DEPARTMENT OF JUSTICE, *645. Entrapment-Elements*, <https://www.justice.gov/archives/jm/criminal-resource-manual-645-entrapment-elements> (consultation 1 May 2021).

VAN HORENBEEK, J. and MEEUS, R., *Rekruteert IS nu ook jongeren via PlayStation? Hoe dan?*, <https://www.demorgen.be/nieuws/rekruteert-is-nu-ook-jongeren-via-playstation-hoe-dan~bb8de0fb/> (consultation 25 October 2020).

VERLAAN, D., *Hoe IS de PlayStation 4 inzet om aanslagen voor te bereiden*, <https://www.rtlnieuws.nl/geld-en-werk/artikel/778301/hoe-de-playstation-4-inzet-om-aanslagen-voor-te-bereiden> (consultation 25 October 2020).

4Gamers, *Waarom terroristen Playstation 4 als communicatiemiddel gebruiken*, https://www.nieuwsblad.be/cnt/blgpe_01972626 (consultation 25 October 2020).