Beiträge zum Internationalen und Europäischen Strafrecht

Studies in International and European Criminal Law and Procedure

Band / Volume 51

Technological Surveillance of Communication in American, German and Chinese Criminal Procedure

Von

Jiahui Shi

Duncker & Humblot · Berlin

JIAHUI SHI

Technological Surveillance of Communication in American, German and Chinese Criminal Procedure

Beiträge zum Internationalen und Europäischen Strafrecht

Studies in International and European Criminal Law and Procedure

Herausgegeben von / Edited by
Prof. Dr. Dr. h.c. Kai Ambos, Richter am Kosovo Sondertribunal
Berater (amicus curiae) Sondergerichtsbarkeit für den Frieden, Bogotá, Kolumbien

Band / Volume 51

Technological Surveillance of Communication in American, German and Chinese Criminal Procedure

Von

Jiahui Shi

Duncker & Humblot · Berlin

Unter Beteiligung des Göttinger Vereins zur Förderung der Strafrechtswissenschaft und Kriminologie sowie ihrer praktischen Anwendung e. V.

Die Rechtswissenschaftliche Fakultät der Universität zu Köln hat diese Arbeit im Jahre 2021 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Typesetting: 3w+p GmbH, Rimpar
Printing: buchbücher.de GmbH, Birkach
Printed in Germany

ISSN 1867-5271
ISBN 978-3-428-18566-5 (Print)
ISBN 978-3-428-58566-3 (E-Book)

Printed on no aging resistant (non-acid) paper
according to ISO 9706 ♾
Internet: http://www.duncker-humblot.de

To My Parents

Foreword

My work on this comparative study started in 2014 and has been finalized in the summer of 2021. It was accepted as a doctoral dissertation by the Law Faculty of the University of Cologne in October 2021.

I would like to express my gratitude to many persons who contributed to my work and supported my studies in the past years. My greatest thanks are due to my supervisor, Prof. Dr. Thomas Weigend. He continuously supported this study with great patience. He read, word by word, sentence by sentence, five lengthy drafts before this final version, and each time made valuable comments. Some of these comments were quite critical, and I had to work hard to meet his demands. But all the work was worthwhile, and his professional comments and supervision guaranteed the quality of my work. Without his time spent on my work, this book could not have been published. An old saying in Chinese goes: "He who teaches me for one day is my father for life." I have learned from him not only how to write a dissertation but also high academic standards and a serious attitude toward scholarship. I am sure that my experience with him will inspire me for the rest of my life when I work in the academic sphere. Moreover, he is a kind and considerate person, ever ready to help me with challenges I encountered in Germany, supporting me with visa matters as well as funding and job applications. The enjoyable time I had with his family for the Christmas and New Year holidays will remain unforgettable. I have been very lucky to have had him as my supervisor. I wish him "Alles Gute"!

I would also like to thank Prof. Dr. Cornelius Nestler who as the second reviewer read my work thorougly and made helpful remarks at the doctoral disputation.

Since this work is written in English, which is not my mother language, my best friend, Dr. Jenny Sager from England, an expert on Shakespeare, did not hesitate to agree to do the proofreading of the manuscript. She could have rejected my request since the job was time-consuming and probably also boring for her. She did an excellent job and I owe her a big hug.

I owe great thanks to my teachers of the German language, my German friends and colleagues, who practiced German with me with great patience. This made it possible for me to learn to manage this difficult language from level zero within a short time. Without my ability to speak German, I could not have finished this comparative study.

Last but not least, I would like to thank the foundations which financially supported my doctoral research and my stay in Germany in the past seven years, namely, the Chinese Scholarship Committee (9.2014 – 8.2018), Dr. Wilhelm Westhaus

Stiftung (9.2018 – 12.2018), and Konrad Adenauer Stiftung (1.2019 – 10.2021). Their generous support permitted me to concentrate on my research without any financial pressure. This publication has been financially supported by the Konrad Adenauer Stiftung and the Law Faculty of the University of Cologne. I would also like to thank Prof. Dr. Kai Ambos, who kindly agreed to accept my work for the series "Beiträge zum Internationalen und Europäischen Strafrecht".

Cologne, February, 2022 *Jiahui SHI*

Content Overview

Contents

Introduction

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

(Benjamin Franklin, 1755)

I. The Background of the Study

The speed of long-distance communication has dramatically increased since the invention of the telegraph, the telephone and, more recently, with the ascendancy of the mobile phone and the internet. For law enforcement to keep abreast with this massive rise in communication technologies, a sophisticated method of interceptive technology was required; hence wiretapping was born. The rise of organized crime and the rapid development of surveillance technologies have led to their widespread use for the purpose of criminal investigation. The interception of private telecommunication and conversations are covert measures. They are most valuable investigation tools because, given their covert nature, they can uncover information that the suspect does not intend to make public. On the other hand, the use of highly intrusive measures, such as online searches of private computers and covert surveillance of private property, can undermine society's trust in the police and an individual's right to privacy. It is therefore necessary to devise a legal framework that balances the need for efficient law enforcement with individuals' privacy rights.

Rules on technological investigative measures (including electronic surveillance) were introduced into *Chinese Criminal Procedure Law* (hereafter referred to as *CCPL*) only in 2012. It is an achievement, but far from satisfactory. It is well recognized that the rules on technological investigative measures in the *CCPL* need to be further improved and reformed. Given this background, a comparative study on this topic can be of importance to Chinese politicians or legislators interested in improving these rules and in solving problems caused by the current arrangement. Looking into foreign experience can broaden their horizons[1] and help them in identifying deficiencies in the Chinese legal system.[2]

Another practical reason for conducting a comparative study on electronic surveillance results from its characteristics. Modern communication technology easily

[1] *Goldsworthy*, in: Rosenfeld/Sajó (eds.), Handbook, 2013, 689, 694.

[2] *Mack*, Comparative Criminal Procedure, 2008, ix.

transcends national boundaries and can connect with the whole world within a second. This facilitates our as well as criminals' communications. All countries must deal with the same problems and challenges. This makes comparison possible and necessary. Different solutions to the same problems can be interesting and inspiring to legal professionals in different jurisdictions.[3]

To conduct a comparative study is, however, not an easy task. A simple comparison between legal texts is far from enough and sometimes even misleading. Similar legal texts do not necessarily lead to the same practice. Moreover, approaches effective in one jurisdiction might not have the same effect in another jurisdiction, given each country's unique historical, cultural, political, and social circumstances.[4] The criminal justice system is closely related to these unique circumstances as well as to each country's legal system as a whole.[5] Components of the criminal procedure system are interrelated with other procedural arrangements and with the court system. For example, any discussion of the admissibility of evidence from surveillance must consider the general role of judges and the purpose of criminal procedure. Therefore, this study will not analyze rules on electronic surveillance independently but will strive to place them within the general constitutional and procedural context of each country.

II. The Three Jurisdictions

For this comparative study, the author has selected the United States of America (the U.S.), Germany, and P.R. China. Each country represents a different legal tradition. The U.S. legal system represents the common law system, many legal principles of which have historically been created by judges through case law.[6] Germany typifies the civil law system which mainly relies on codes and statutes.[7] The Chinese legal system, including its criminal procedure, is basically organized like a civil law system, but the influence of the socialist ideology can be observed. On the other hand, both practice and theories of criminal procedure in China have, especially in recent years, been influenced by the U.S. system. For instance, the design of the Chinese plea bargaining system has been influenced by the U.S. system, and the American "fruit of the poisonous tree" doctrine is a popular topic among Chinese academics. Given this background, the ways of solving problems in Germany and the U.S. may have become more acceptable to Chinese jurists. In addition, the discussion

[3] *Dubber/Hörnle*, Criminal Law, 2014, xx.

[4] *Goldsworthy*, in: Rosenfeld/Sajó (eds.), Handbook, 2013, 689, 694.

[5] *Mack*, Comparative Criminal Procedure, 2008, ix.

[6] *Keiler/Roef*, in: *Keiler/Roef* (ed.), Comparative Concepts of Criminal Law, 2019, 4.

[7] *Id.* at 5. For a general comparison of the two systems see *Mack*, Comparative Criminal Procedure, 2008, 1–20. For a historical introduction to inquisitorialism see *Dezza*, Geschichte des Strafprozessrechts in der Frühen Neuzeit, 2017, 15–24.

of technological surveillance in these two jurisdictions started much earlier than in China. Therefore, they both have developed relatively comprehensive and well-organized systems and approaches to soften the tension between surveillance and the right to privacy even though they rely on different values and procedural arrangements. Although problems exist in these two jurisdictions, it is of great value for Chinese reform efforts to examine how their different approaches work in practice.

Some might argue that when legal systems are very different from each other, it is less useful to compare them. This argument is not convincing. It is true that there are evident differences among the three jurisdictions due to their differing legal traditions. The distinction between the common law and civil law systems should, however, not be overstated.[8] Especially in recent years, the two models have approached each other. The U.S. has a growing body of statutes, which have become essential legal sources, such as U.S. Code chapter 18 *Title III* on the interception and disclosure of wire, oral, or electronic communications.[9] In Germany, the case law of higher courts is well recognized and generally followed by lower courts. The same tendency can be observed in China. The Chinese Supreme Court began to operate a nation-wide database of judgments several years ago and selects "guideline judgments" that are published.[10] These guideline judgments are normally followed by other courts. Moreover, more adversarial elements have been introduced into Chinese criminal procedure. For example, the role of the defense lawyer has been enhanced, and cross-examination of witnesses at trials is encouraged.

In light of these developments, this research on surveillance in the U.S., Germany and China focuses on specific and practical problems rather than entering into a general discussion of the two theoretical models.

III. Presentation of Problems

In all three jurisdictions, the development of communication technology necessitates a closer analysis of the relation between the protection of the right to privacy and electronic surveillance in the criminal process. On the one hand, surveillance measures are effective in obtaining information in the fight against serious crime, especially organized crime. On the other hand, however, such measures may intrude deeply into the right to privacy. Therefore, defining the constitutional rights of criminal suspects has become an important topic for debate. In the U.S. and in Germany, different approaches have been taken to balance the need for crime investigation with the need to protect privacy. In the P.R. China, however, surveillance

[8] *Id.* at 4.

[9] Pub. L. No. 90–351, 82 Stat. 197 (codified at 18 U.S.C. §§ 2510–2520 (Supp. V 1965–1969), later at 18 U.S.C. §§ 2510–2522).

[10] All published "Guideline Judgements": http://www.court.gov.cn/fabu-gengduo-77.html, visited at 22.02.2020.

measures are regarded as normal investigative practices, which can be applied without a judicial order. Moreover, details about the surveillance process are not recorded, and defendants therefore have little opportunity for challenging the legality of the measures. Given that digitalization has come to be seen as a symbol of modernity and progress, and as such is promoted by politicians, it is highly likely that intensive surveillance measures will increasingly be adopted, thus creating a threat to the fundamental right to privacy.

Given these problems, this comparative study is intended to promote a better understanding of the various solutions to this issue in different legal systems. To determine the advantages and disadvantages of surveillance systems in each jurisdiction, their constitutions, statutes and case law will be analyzed and compared. Analysis will focus on the following questions:

- What legislation exists in each country concerning surveillance of wire and oral communication and the protection of privacy?
- What legal theories have been developed in the three countries in response to this issue? What are the similarities and differences between them?
- What are the practical effects of the laws in each of the three jurisdictions?

IV. Structure of the Study

In the first three parts of this study, the legal systems of the U.S., Germany and the P.R. China are discussed separately. Each Part starts from the constitutional foundation of surveillance of wire and oral communications, and then treats the statutory rules on surveillance. This is followed by a discussion of the relevant procedural arrangements, such as judicial control of surveillance, the contents of surveillance orders, and remedies in case of illegal surveillance. The following chapter deals with the use of evidence that has been obtained, legally and illegally, from surveillance. The second but last Chapter in Part I and Part II respectively pursues an empirical study on official statistics on surveillance, while the reports on questionnaires on surveillance practice in China can be found in the Appendix. The last chapter in each Part gives a preliminary conclusion to the surveillance practice in the specific legal system discussed in that Part. Part IV, as the Conclusion to the whole project, provides a horizontal comparison of the three legal systems. Important and common issues regarding technological surveillance are listed. Solutions offered by each jurisdiction are compared in order to identify those legal solutions which achieve a proper balance between the protection of the right to privacy and the effective combat of crime.

Part I

Surveillance of Wire and Oral Communications in the U.S.

The right of privacy in the law of the U.S. was developed as a penumbra right of the *Bill of Rights*, even though this was probably not the original intention of the authors of *the Bill of Rights.* The right to privacy was based upon the 1st Amendment's freedoms of expression and association, the 4th Amendment's protection of persons, places, papers, and effects against unreasonable searches and seizure, and the 5th Amendment's privilege against self-incrimination and requirement of due process.[11]

Given the rise of organized crime and the rapid development of technology, interceptive technologies are widely used in crime detection,[12] such as in the investigation of drug trafficking[13] and mob-related offenses like racketeering. Since *Olmstead v. United States (1928)*[14], the first wiretapping case decided by the U.S. Supreme Court[15], the constitutionality of such measures and their relationship with the right to privacy have been continuously reviewed and discussed mainly within the framework of the 4th Amendment. Decades later, *Title III of The Omnibus Crime Control and Safe Streets Act of 1968* [16], also referred to as the *"Federal Wiretap Act"* (hereafter referred to as *Title III*), was enacted to specifically regulate the interception practices adopted by law enforcement agencies.

This Part will discuss the constitutional protection provided by the U.S. Constitution and case law concerning the interception of wire and oral communications by law enforcement agencies.

---

[11] Some scholars argue that the 9th Amendment and the 14th Amendment should also be regarded as the origin of this right to privacy. See, e. g., *Bomser*, Fordham L. Rev. 6 (1995), 697, 739.

[12] *Rosenzweig*, Cornell Law Quarterly 32 (1946–1947), 514, 514.

[13] Drug offenses were the most prevalent type of criminal offense investigated using wiretaps. The Wiretap Report 2018 indicates that 46 percent of all applications for intercepts (1,354 wiretap applications) in 2018 cited narcotics as the most serious offense under investigation. Applications citing narcotics combined with applications citing other offenses, which include other offenses related to drugs, accounted for 77 percent of all reported wiretap applications in 2018. See Graph 5. Source: https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at: 21. 11. 2019.

[14] *Olmstead v. United States*, 277 U.S. 438 (1928).

[15] For example, *Doenges*, Tulsa L. J. 2 (1965), 180, 180 ("The Olmstead case, decided in 1928, was the first case in which the Supreme Court heard argument concerning wiretapping.").

[16] Pub. L. No. 90–351, 82 Stat. 197 (codified at 18 U.S.C. §§ 2510–2520 (Supp. V 1965–1969), later at 18 U.S.C. §§ 2510–2522).

I. Constitutional Protection

The 4th Amendment plays an essential role in protecting privacy regarding surveillance in criminal investigations. Its main doctrine has evolved in the last century from the old common law "trespass doctrine" to the "reasonable expectation of privacy".

1. Trespass Doctrine

The 4th Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[17]

Looking back at the history of the 4th Amendment, the original purpose of this Amendment was to protect people from writs of assistance, which entitled customs officers to enter any house or other place in order to search for smuggled goods without having to obtain a specific warrant with a more detailed description of the search.[18] Writs of assistance were regarded as one of the most prominent causes of the American Revolution.[19] As a consequence, the permanent prohibition of such general writs was integrated into the new constitution to protect people from unreasonable searches and seizures. The boundaries and the scope of the 4th Amendment, however, have been the subject of extensive legal argument because of the ambiguity of the text. There are two distinct methods of interpretation: one emphasizes particularity, the other generality.[20] Particularity theorists interpret the text in a historical way, limiting its understanding to the historical background; proponents of generality, by

[17] U.S. Const. amendment IV.

[18] For more details, see *Howard*, Preliminaries of the Revolution, 1763–1775, 1905; *Smith*, Writs of Assistance Case, 1978, 29–34; *Hutchinson*, The History of the Colony of Massachusetts Bay (3 vols. 1764–1828; 1765–1828); and *Taylor*, Two Studies in Constitutional Interpretation, 1969, 35–41.

[19] James Otis in the 1760s led a protest movement against the issuance of new writs of assistance, arguing that writs of assistance violated the liberty of the people. The "Malcom Affair" of 1766, which involved the application of a writ of assistance, pushed the conflict between the British authorities and the colonies to a new level. William Cuddihy described this search action as "the most famous search in colonial America". See *Stephens/Glenn*, Unreasonable Searches and Seizures: Rights and Liberties under the Law, 2006, 39. See also *Dickerson*, in: Morris (ed.), The Era of the American Revolution: Studies Inscribed to Evarts Boutell Greene, 1939, 40; see also *Chimel v. California*, 395 U.S. 752, 761 (1969) ("…the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence.").

[20] *Alschuler*, in: Hickok (ed.), The Bill of Rights, 1991, 197.

contrast, define the objectives of the Constitution as broadly as possible.[21] The U.S. Supreme Court once declared, "time works changes, brings into existence new conditions and purposes."[22] The original authors of the U.S. constitution could never have foreseen the altered legal circumstances caused by the rapid introduction of new technology; therefore, the concept of "unreasonable searches and seizures" needs to be continuously updated.[23]

The first published ruling of the Supreme Court that tried to define the protection provided by the Constitution in the context of wiretapping is *Olmstead v. United States*[24], a case that was heard in 1928[25] against the background of the fast-developing telephone network[26]. Roy Olmstead was convicted of conspiracy under *the National Prohibition Act*.[27] The evidence collected by Federal agents against Olmstead was obtained by wiretapping telephone lines leading from his residences to his head office. The wiretap devices were installed on public telephone wires without physically trespassing upon any of his property[28] and the evidence obtained from the wiretapping was presented in court. Olmstead moved to suppress the evidence, arguing that wiretapping violated the 4th Amendment.[29] The key issue in this case was to decide whether a wiretap is a search and seizure under the 4th Amendment. If so, the evidence from a wiretap was likely to be suppressed; if not, the evidence obtained from the wiretap could not be excluded based on the 4th Amendment.[30]

---

[21] For example, the United States Supreme Court declared that a right of contraception is also created by 4th Amendment since the text intends to protect privacy. Cf. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[22] *Weems v. Hammond*, 217 U.S. 349, 373 (1910).

[23] Albert W. Alschuler said: "In resolving this central 4th Amendment issue, courts have responded to changing cultural norms, changing technologies, changing law enforcement needs and changing forms of governmental and private organization." *Alschuler*, in: Hickok (ed.), The Bill of Rights, 1991, 197–198.

[24] *Olmstead v. United States*, 277 U.S. 438 (1928).

[25] The reason that the first case regarding wiretapping came up much later than those in the states mainly lies in the enactment of *the National Prohibition Act* in 1919. Before the enactment of this Act, the 4th Amendment regulated only the Federal government, not states, therefore only quite few cases came to the Federal level. Later, because of this Act, the number of Federal cases increased dramatically and the search warrants for illegal alcohol obtained by the Federal officers also. As a result, the Federal courts started to deal with the 4th Amendment more frequently. See *Kerr*, Michigan L. Rev. 102 (2004), 801, 841–842; *Lerner*, Texas L. Rev. 81 (2003), 951, 986 ("Long before the 'war on drugs,' the National Prohibition (or 'Volstead') Act provided an engine for the expansion of federal criminal law enforcement."); *Simons*, New York University L. Rev. 75 (2000), 893, 911.

[26] Some scholars explained why telegraph had not drawn as much attention as telephone technology. See *Brenner*, Journal of Technology Law & Policy 7 (2002), 128.

[27] 27 U.S.C.A. § 1 et seq.

[28] *Olmstead v. United States*, 277 U.S. 438, 456–457 (1928).

[29] *Ibid.*

[30] *Kerr*, Michigan L. Rev. 102 (2004), 801, 844.

The Supreme Court acknowledged that the interpretation of the Constitution should adapt to changing circumstances.[31] In this case, however, the majority of the Court still favored the historical interpretation of the 4th Amendment, namely, that the 4th Amendment applies only to the situation where a physical trespass occurs. Since there was no physical trespass in the *Olmstead* case, the 4th Amendment was not violated.[32] Moreover, the Court observed that the United States provided less protection to telephone communications than to sealed letters, and therefore decided that neither a search nor a seizure had taken place because the evidence was secured only by "the sense of hearing".[33] Limiting the application of the 4th Amendment to a physical trespass, the ruling in the *Olmstead* case did not distinguish information carried by phone lines from the phone lines themselves. Only the latter was considered under the "trespass test", even though the wiretappers had obtained the information as a direct consequence of the audio transmissions through the phone lines. According to the opinion of the Court, the Constitution does not forbid evidence to be obtained by wiretapping unless it involved actual unlawful entry onto a person's property.[34] This opinion basically upheld the principles of the trespass law of the Eighteenth Century and left the large volume of private information exchanged via telephone without constitutional protection.[35] This so-called "trespass doctrine" was the dominant theory for the application of the 4th Amendment until the 1960s.[36] The lower courts felt bound by the ruling of the *Olmstead* Case; therefore, evidence obtained by wiretapping was admitted in court without reservation.[37]

---

[31] *Weems v. Hammond*, 217 U.S. 349, 373 (1910).

[32] *Olmstead v. United States*, 277 U.S. 438, 464–465 (1928) ("There was no entry of the houses or offices of the defendants… . The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.") (Taft, Chief J., opinion of the Court).

[33] *Id.* at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.") (Taft, Chief J., opinion of the Court).

[34] *Berger v. New York*, 388 U.S. 41, 51 (1967).

[35] Without the constitutional protection, the nonphysical trespass was dealt with by criminal law and also in civil cases at that time. See *Note*, Harvard L. Rev. 94 (1981) 1892, 1896; see also *Olmstead v. United States*, 277 U.S. 438, 480 (1928), Note 13 in dissenting opinion (J. Brandeis) (a list of states where intercepting a message sent by telegraph and/or telephone was a criminal offense.); *Moore v. New York Elevated R.R.*, 130 N.Y. 523, 527–28, 29 N.E. 997, 997–98 (1892).

[36] For example, *Goldman v. United States*, 316 U.S. 129 (1942), the Court held "no reasonable or logical distinction can be drawn between what federal agents did in the present case and state officers did in the Olmstead case" (*Id.* at 135) and held that the evidence obtained by installation of detectaphone against a wall in the office next door, was not inadmissible because the officers lawfully entered that office room; see also *On Lee v. United States*, 343 U.S. 747 (1952) (The Court held the evidence was admissible when a microphone was carried by a person who entered the defendant's room with his consent.).

[37] "This court, of course, cannot reverse it or overrule the fully-considered opinion of the majority (in the Olmstead case), and the Supreme Court in the Nardone Case did not do so. Until

Justice Brandeis disagreed with the opinion of the Court and argued that there was no difference between sealed letters and private telephone messages. He further pointed out that the invasion of privacy caused by wire-tapping telephones is far greater than that of tampering with mail. This is because "[w]henever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard."[38] Moreover, he foresaw an unceasing development of technology, which could furnish the government with increasingly advanced investigative measures besides wiretapping.[39] In his dissent, Justice Brandeis demonstrated his concern that the right to privacy would be lost completely if wiretapping was not regarded as a search or a seizure. Therefore, he suggested that "the protection guaranteed by the Amendment is much broader in scope",[40] namely, that the Amendment should be interpreted as protecting the right to privacy. By referring to statements in *Weems v. United States*,[41]he preferred a more dynamic method of interpreting the 4th Amendment and stated that the Constitution must be applied in terms of "what may be" rather than as "what has been",[42] in order to prevent more advanced technologies from intruding into privacy. His argument, however, did not convince the majority of the Justices in the Olmstead case.

The breakthrough came in the case of *Silverman v. United States.*[43] In this case, the police officers, with the owner's permission, entered a vacant house which shared a wall with the defendant's house. They inserted the spike of a "spike mike" (a microphone with a spike, amplifier and earphone) into the shared wall, until the spike touched the heating duct, which ran through the whole house of the defendant. Through this connection, the heating duct functioned as a conductor of sound and conveyed all the conversations taking place in the defendant's house to the police officers.[44] This case is comparable with the *Goldman* case[45], where a detectaphone was placed against an office wall, in order to intercept conversations taking place next door. In *Goldman*, the Court denied that this constituted a trespass, following

the Supreme Court itself shall reverse its decision on this point, this court is governed by it. [T]he tapping of telephone wires then is not a violation of the Fourth Amendment… ". See *Valli v. United States*, 94 F.2d 687, 691 (C. C. A. 1st, 1938). More cases following Olmstead opinion can be found in *Rosenzweig*, Cornell Law Quarterly 32 (1946–1947), 514, Fn. 130.

[38] *Olmstead v. United States*, 277 U.S. 438, 475–476 (1928).

[39] *Id.* at 474.

[40] *Id.* at 478.

[41] He argued this point by referring to the statement made in *Weems v. United States:* "Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes." *Weems v. United States*, 217 U.S. 349, 373 (1910).

[42] *Olmstead v. United States*, 277 U.S. 438, 474 (1928).

[43] *Silverman v. United States*, 365 U.S. 505 (1961).

[44] *Id.* at 506–507.

[45] *Goldman v. United States*, 316 U.S. 129 (1942).

Olmstead. The Court in *Silverman*, however, decided that there was a trespass. It ruled that the "spike mike" inserted through the wall constituted an unauthorized physical penetration of the suspect's home.[46] Although the Court still followed the "trespass doctrine", it recognized that conversations could be the subject of a seizure, which partially overruled the findings of *Olmstead*, where the Court had argued that collecting evidence by means of "the sense of hearing" could not constitute a seizure.[47] This case actually extended the 4th Amendment's protection from the tangible world to the intangible world.[48]

The Court, on the one hand, acknowledged that the 4th Amendment's right of the defendant was indeed violated.[49] On the other hand, the Court tried to remain consistent by applying the "trespass doctrine" from its precedents. As a result, the trespass was applied according to technical differences between the devices used in *Silverman* and in *Goldman.*[50] Justice Douglas clearly pointed out in his concurring opinion that the invasion of privacy in *Silverman* was actually the same as in *Goldman.*[51] He also stated that "the measure of the injury" should not be decided upon on the basis of "the depth of the penetration of the electronic device" and that the core issue was whether the home had been tapped.[52]

---

[46] *Silverman v. United States*, 365 U.S. 505, 509 (1961) ("For a fair reading of the record in this case shows that the eavesdropping was accomplished by means of an unauthorized physical penetration into the premises occupied by the petitioners.") (Stewart, J., opinion of the Court).

[47] *Olmstead v. United States*, 277 U.S. 438, 464 (1928).

[48] See also *Katz v. United States*, 389 U.S. 347, 353 (1967) ("we have expressly (in *Silverman*) held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard…") (Stewart, J., opinion of the Court); *Berger v. New York*, 388 U.S. 41, 51 (1967) ("…'conversation' was within the Fourth Amendment's protections, and that the use of electronic devices to capture it was a 'search' within the meaning of the Amendment…") (Clark, J., opinion of the Court).

[49] *Silverman v. United States*, 365 U.S. 505, 511–512 (1961) ("At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion… . This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard.") (Stewart, J., opinion of the Court).

[50] *Id.* at 511 ("[T]he officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office – a heating system which was an integral part of the premises occupied by the petitioners, a usurpation that was effected without their knowledge and without their consent.") (Stewart, J., opinion of the Court).

[51] *Goldman v. United States*, 316 U.S. 129 (1942).

[52] *Silverman v. United States*, 365 U.S. 505, 512–513 (1961) ("Yet the invasion of privacy is as great in one case as in the other (*Goldman*, 316 U.S.). The concept of 'an unauthorized physical penetration into the premises,' on which the present decision rests seems to me to be beside the point. Was not the wrong in both cases done when the intimacies of the home were tapped, recorded, or revealed? The depth of the penetration of the electronic device – even the degree of its remoteness from the inside of the house – is not the measure of the injury.") (Douglas, J., concurring). *Petersen*, Introduction to Surveillance Studies, 2013.

In this case, the Court focused on technical details, placing less attention to the 4th Amendment itself. It was not an effective solution to rely purely on certain technical details relating to the "spike mike" as a means to protect a fundamental right.[53] Moreover, there are more advanced technologies, which could possibly develop even further. The Court declined to consider this problem, even when they were informed about it.[54] The lower courts were confused by this decision and no general criteria for the similar situations were established.[55]

2. From Trespass Doctrine to the Reasonable Expectation of Privacy

The attitude of the Supreme Court began to change in *Silverman v. United States*[56]. In an endeavor to establish an overarching standard, which could be adapted to new interception technologies, the concept of "reasonable expectation of privacy" was introduced in *Katz v. United States*[57] in 1967. The FBI had installed a listening device to the outside wall of a public telephone booth, regularly used by Katz, in order to record the defendant's end of conversations, which included information regarding illegal gambling.[58] Again relying on *Goldman*[59], the lower courts accepted that the recordings obtained from this warrantless eavesdropping could be used as legal evidence, on the grounds that there had been no physical trespass into the booth.[60] The Court, however, reversed this decision, concluding that the FBI's activities here constituted a "search and seizure" under the 4th Amendment because the 4th Amendment "protects people, not places".[61] Therefore the evidence was held inadmissible.[62] Moreover, the Court explicitly overruled previous precedents, such as

[53] *Silverman v. United States*, 365 U.S. 505, 511 and 513 (1961) ("neither should the command of the Fourth Amendment be limited by nice distinctions turning on the kind of electronic equipment employed.") (Douglas, J., concurring).

[54] *Id.* at 508–509.

[55] For instance, in the per curiam opinion in *Clinton v. Virginia* regarding a "spike mike", the court followed the holding of *Silverman* and recognized an actual trespass. *Clinton v. Virginia*, 377 U.S. 158 (1964).

[56] *Silverman v. United States*, 365 U.S. 505 (1961).

[57] *Katz v. United States*, 389 U.S. 347 (1967).

[58] *Id.* at 348.

[59] *Goldman v. United States*, 316 U.S. 129 (1942)

[60] *Katz v. United States*, 369 F.2d 130, 134 (9th Cir. 1966).

[61] *Id.* at 351.

[62] *Katz v. United States*, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.") (Stewart, J., opinion of the Court).

Olmstead[63] and *Goldman*[64], by concluding that the trespass doctrine was no longer the guiding theory.[65] In establishing the scope of the 4th Amendment, the majority opinion emphasized the subjectivity of a person's conception of privacy.[66] In practice, the two-pronged test of "reasonable expectation of privacy" formulated by Justice Harlan in his separate concurring opinion[67] replaced the "trespass doctrine".[68] The courts now mainly apply *Title III* that provides regulations on the procedures and exclusionary rules regarding all electronic surveillance.[69] This does not mean, however, that the *Katz* decision is less significant. This test is still applied by courts as the standard to determine whether a surveillance is a "search" or "seizure" under the 4th Amendment in the post-Katz era.[70] Moreover, nearly every 4th Amendment decision refers to phrases from *Katz.*[71] Therefore, the *Katz* decision has had a big influence not only in the context of interception but also on the interpretation of the 4th Amendment generally.[72]

3. "Reasonable Expectation of Privacy" after *Katz*

The Supreme Court has dealt with several cases concerning modern technology after the *Katz* ruling, which contributed continuously to the development of the

[63] *Olmstead v. United States*, 277 U.S. 438 (1928).

[64] *Goldman v. United States*, 316 U.S. 129 (1942).

[65] *Katz v. United States*, 389 U.S. 347, 353 (1967) ("We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.") (Stewart, J., opinion of the Court).

[66] *Id.* at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection… . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protection.") (Stewart, J., opinion of the Court); see also *Id.* at 353 (" …once it is recognized that the Fourth Amendment protects people and not simply 'areas' – against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.") (Stewart, J., opinion of the Court). Some commenters have asserted, that Katz "marks a watershed in fourth amendment jurisprudence", see *Amsterdam*, Minnesota L. Rev. 58 (1974), 349, 382; and led to " a redefinition of the scope of the Fourth Amendment". See *Kitch*, Supreme Court Review 1968, 133.

[67] *Katz v. United States*, 389 U.S. 347, 360–361 (1967) (Harlan, J., concurring).

[68] Justice Harlan stated that 4th Amendment protects person's "reasonable expectation of privacy". While some other scholars insist that the "trespass" doctrine is not replaced, which still remains independent significant, and the expectation test only supplements this doctrine when this doctrine cannot offer sufficient protections. *Cf. Note*, Michigan L. Rev. 76 (1977), 154, 172–173.

[69] *Aynes*, Cleveland State L. Rev. 23 (1974), 63, 66.

[70] See, for example, *Smith v. Maryland*, 442 U.S. 735 (1979). In this decision, more cases were quoted which also rely upon "reasonable expectation" test.

[71] *Kamin/Marceau*, University of Miami L. Rev. 68 (2014), 589, 595.

[72] *Id.* at 596–597.

concept of privacy and the doctrine of "reasonable expectation of privacy". In order to better clarify the development of the doctrine "reasonable expectation of privacy" in the post-Katz era, these cases will be summed up in chronological order below.

The first technology case after *Katz* was the *White* case.[73] In this case, the Court held that an undercover agent could record conversations with the defendant without a warrant. Once the defendant disclosed information to the third party, he lost his reasonable expectation of privacy.[74] The Court established that an individual can no longer reasonably expect the privacy of shared information. Following this precedent, the Court decided in the *Smith* case concerning pen registers that the caller could not reasonably expect that his phone number remained private because he should have known that such information was shared with the recipient by his calling.[75]

Some years after the *Smith* case, the Court decided two cases on using tracking devices but reached opposite conclusions. In the first case, *United States v. Knotts*,[76] the law enforcement officer installed a tracking device inside a container which was later sold to the defendant. The officers tracked the container while the defendant transported it with his car to a cabin. The device was not used again after the cabin was located.[77] The Court held that such location information obtained from a tracking device was admissible because the defendant did not have a reasonable expectation of privacy of his location when driving a car in public streets.[78] The facts of the second case, *United States v. Karo*,[79] were highly similar to the *Knotts* case at the beginning, however, the officers kept obtaining information from the tracking device installed in a barrel with ether over the next few months to locate other houses and facilities after the first house of the defendant had been located.[80] The Court in this case emphasized that the device was used to "locate the ether in a specific house" and to "reveal a critical fact about the interior of the premises" which is out of public view.[81] Therefore, the defendant's reasonable expectation of privacy on his residence had been infringed upon. According to the Court, the key difference between these two

[73] *United States v. White*, 401 U.S. 745 (1971).

[74] *Id.* at 752 ("One contemplating illegal activities must realize and risk that his companions may be reporting to the police."). See Section 2, Chapter III, Part I.

[75] *Smith v. Maryland*, 442 U.S. 735 (1979).

[76] *United States v. Knotts*, 460 U.S. 276 (1983).

[77] *Id.* at 278–279.

[78] *Id.* at 276 ("Monitoring the beeper signals did not invade any legitimate expectation of privacy on respondent's part, and thus there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment. The beeper surveillance amounted principally to following an automobile on public streets and highways. A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.").

[79] *United States v. Karo*, 468 U.S. 705 (1984).

[80] *Id.* at 708–710.

[81] *Id.* at 714–715.

cases is whether the information is in public view or whether it "could not have otherwise been obtained without a warrant".[82]

In 1986, two cases involving aerial surveillance were decided by the Court. In *California v. Ciraolo*[83] and *Dow Chemical Co. v. United States*,[84] the agents employed planes to fly respectively over Ciraolo's backyard which was surrounded by a ten-foot-high fence and over Dow's chemical factory to take pictures. The Court admitted these pictures and argued that any person who flies a plane above the backyard or the factory could have seen what the agents observed.[85] If the public could obtain certain information, the expectation of privacy on such information is not recognized by the society as "reasonable". Thus, the law enforcement officers could obtain the information without warrants.

In 2001, the Court decided *Kyllo v. United States*[86] where the police used a thermal imager to detect whether heating machines were used in the defendant's house for growing marijuana. The Court held that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area" constitutes a search at least where the technology is not in "general public use".[87] The expression "not in general public use" indicates that the Court considered that society recognizes the expectation of privacy on the information obtained via thermal imagers as "reasonable" and thus the police needs a warrant.

The Court decided on GPS surveillance in *United States v. Jones* in 2012,[88] where the police installed a GPS tracking device to the defendant's car with a warrant authorizing ten-day surveillance; however, the police tracked the car for twenty-eight days outside the authorized district. Following *Knotts* and *Karo*, the District of Columbia Court suppressed the GPS data while the vehicle was parked at Jones's residence, but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets.[89] The Supreme Court suppressed all data and held that the *Katz* test was not applicable here because there was a physical intrusion into the defendant's "effects" protected by the 4th Amendment. The Court nevertheless emphasized the importance of the *Katz* test, which protects against unconstitutional invasions of privacy without a trespass.[90]

---

[82] *Id.* at 715.

[83] *California v. Ciraolo*, 476 U.S. 207 (1986).

[84] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).

[85] *California v. Ciraolo*, 476 U.S. 207, 213–14 (1986) and *Dow Chemical Co. v. United States*, 476 U.S. 227, 238 (1986).

[86] *Kyllo v. United States*, 533 U.S. 27 (2001).

[87] *Id.* at 34.

[88] *United States v. Jones*, 565 U.S. 400 (2012).

[89] *Ibid.*

[90] *Id.* at 954.

Compared to the large number of the 4th Amendment cases decided by the Court, the number of technology cases is extremely small.[91] Therefore, it remains unclear in what intensity and to what degree the Court will apply the *Katz* test to more advanced technology in the future. At least, the ruling in *Jones* indicates that the Court acknowledges that the *Katz* test still plays an important role in future technology cases under the 4th Amendment, especially when the technology does not require a physical trespass.

4. The Reasonable Expectation of Privacy

Justice Harlan did not intend to create a new concept, in opposition to the majority opinion, by proposing the "reasonable expectation of privacy" test, rather, his aim was to further clarify the majority's expression that the law enforcement activities "violated the privacy upon which he (*Katz*) justifiably relied". There is a large difference, however, between the majority opinion and Justice Harlan's concurring opinion. The protective scope of his interpretation of the term "reasonable expectation of privacy" is actually narrower than what is set forth by the majority opinion because he introduced an objective element – "a place" – into his theory.[92] The majority opinion only established a subjective standard, while "the reasonable expectation" introduced by Justice Harlan can only be recognized when the person is an occupant – temporarily or permanently – of a specific place.[93] According to Justice Harlan, the 4th Amendment protection is location-oriented.[94]

A wide range of investigative measures, including surveillance, are now subject to the "reasonable expectation of privacy" test. Therefore, it is important to provide a close examination of its "two-pronged requirement"[95], i.e., "an actual (subjective) expectation of privacy" and the expectation "that society is prepared to recognize as 'reasonable'".[96]

a) An "Actual (Subjective) Expectation of Privacy"

The first requirement mentioned in *Katz* is whether "… a person has *exhibited* an actual (subjective) expectation of privacy", as expressed in Justice Harlan's con-

[91] *Pesciotta*, Case Western Reserve Law Review 63 (2012), 187, 215.

[92] *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[93] *Id.* at 361 ("… that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable.") (Harlan, J., concurring).

[94] Cf. *Sobel/Horwitz/Jenkins*, Boston University Public Interest Law Journal 22 (2013), 1, 13–14; and more critics are discussed in *Amsterdam*, Minnesota L. Rev. 58 (1974), 349, 384–86.

[95] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[96] *Id.* at 361.

curring opinion,[97] or whether a person "*seeks* to preserve (something) as private"[98] according to the majority opinion. What is relevant here is the person's actual conduct, not his mental state,[99] because a person's behavior is the only means by which the person's subjective expectation can reliably be ascertained. It is unclear, however, what kind of behavior can be recognized as a proper indication of this expectation. In *Katz v. United States*, the Court determined that the defendant had fulfilled the first part of the test when he closed the door to the telephone booth even though the door could not really stop the sound.[100] In cases regarding aerial surveillance, however, the courts insist that a person is required to actually take measures to block the view from the aircraft to demonstrate his expectation of privacy and hence to pass the first test.[101]

The case law requires defendants to take effective measures to prevent surveillance by technical devices in order to preserve their privacy. This seems to eliminate the protective effectiveness of this test. The courts require citizens themselves to fight against the invasion of their privacy by advanced technology used by public authority. It is likely that citizens will lose this "war" in most situations because state authorities usually have the most advanced technology. This interpretation was criticized as "a perversion of *Katz*", since the defendant in *Katz* was not required to attempt to stop his communication from being intercepted via electronic devices. Instead, he only had to demonstrate his intention of not being overheard by closing the door.[102] Regarding this point, some courts have also shown their concern by bringing up more extreme instances; for example, everyone would lose their subjective expectation of privacy if the government suddenly made an announcement that all homes are subject to warrantless entry.[103] One State Court negated the defendant's subjective expectation of privacy in a fitting room of a department store just because a sign was posted on the mirror of the fitting room informing customers that the fitting rooms are under surveillance.[104] In this context, the first test would not play a substantive role in defining the protected domain of the 4th Amendment. Instead, it only provides an

[97] *Id.* at 361 (emphasis added).

[98] *Id.* at 351.

[99] Cf. e. g., *Bender*, New York University L. Rev. 60 (1985), 725, 743 – 744.

[100] *Katz v. United States*, 389 U.S. 347, 511 – 512 (1967) ("One who occupies it (telephone booth), shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

[101] *Bender*, New York University L. Rev. 60 (1985), 725, 746, Fn. 121 and companying texts. See also *California v. Ciraolo*, 476 U.S. 207 (1986) (The defendant's subjective expectation was rejected because he only exhibited his expectation to prevent observation from ground with a 10-foot fence without any effort to shield surveillance from the view of an aerial plane.); a similar case: *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986). See Section 3, Chapter I, Part I.

[102] *Bender*, New York University L. Rev. 60 (1985), 725, 753 – 754.

[103] *Smith v. Maryland*, 442 U.S. 735, 746 (1979).

[104] *Gillett v. States*, 588 S.W.2d 361, 362 (Tex. Crim. App. 1979).

excuse to evade the examination of the second part of the test or could be used to deny the defendant the protection of the 4th Amendment.[105] Therefore, the courts rely more upon the second prong of the expectation test, the normative standard,[106] rather than on the first one. Sometimes, this first prong is even ignored intentionally.[107] In addition, courts sometimes do not differentiate between the two prongs of this test, in other words, a person only enjoys the subjective expectation of privacy if such an expectation is objectively justified; or courts base their reasoning upon different prongs of the test in similar situations. This can be seen if we compare the findings of the two aerial plane cases, *California v. Ciraolo*[108] and *Dow Chemical Co.*[109] In the first case, the claim of subjective expectation of privacy was rejected because the defendant did not take effective measures to block the view from the air. In the second case, the defendant also did not block the photography from the air, but the Court denied the protection of the 4th Amendment on the grounds of the second prong of the test, not the first.[110]

b) An Expectation "that Society is Prepared to Recognize as 'Reasonable'"

The second prong requires that the expectation of privacy must be "supported by larger society or representative of the expectations held by larger society."[111] This is regarded as an objective test, since it is an inquiry into the social conception of the term "reasonable". What can be termed as "reasonable" in this context, however, is "a mystery".[112] According to the *Katz* and *White* rulings,[113] "reasonableness" requires the expectation to be constitutionally "justifiable" rather than "merely reasonable".[114] For example, people can reasonably expect privacy in a remote corner of a park in the middle of the night, but they cannot claim protection under the 4th Amendment if they are actually observed by someone. Their expectation here is not protected because "a high probability of freedom from intrusion"[115] does not

[105] *Bender*, New York University L. Rev. 60 (1985), 725, 753; see also *Julie*, American Criminal L. Rev. 37 (2000), 127, 133.

[106] *Smith v. Maryland*, 442 U.S. 735, 746 (1979).

[107] *Julie*, American Criminal L. Rev. 37 (2000), 127, 133.

[108] *California v. Ciraolo*, 476 U.S. 207 (1986).

[109] *Dow Chemical Co.*, 476 U.S. 227 (1986). See also Section 3, Chapter I, Part I.

[110] More discussion and criticism about *Dow* case can be found in Section 3, Chapter I, Part I.

[111] *Burkell*, Canadian Journal of Criminology and Criminal Justice 50 (2008), 307, 308.

[112] *United States v. White*, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting).

[113] *Katz v. United States*, 389 U.S. 347 (1967); *United States v. White*, 401 U.S. 745 (1971).

[114] *Note*, New York University 43 (1968), 968, 983 ("Justification, as here used, is intended to be a basis of differentiating those expectations which are merely reasonable from those expectations which are to be constitutionally enforced due to other social considerations."). See also *United States v. White*, 401 U.S. 745, 749 (1971).

[115] *Note*, New York University 43 (1968), 968, 983.

equal a *justified* "reasonableness". The literal interpretation of "constitutionally 'justifiable'" is that the action must be acceptable within the terms of the constitution or be defensible on a constitutional basis.[116] According to the *White* case, the question of what expectations of privacy are constitutionally "justifiable" is identical to the question of what expectations the 4th Amendment will protect in the absence of a warrant.[117] This reformulation, however, cannot contribute to further understanding of what is "constitutionally justifiable" because it leads back to the question of what is protected by the 4th Amendment.

aa) Social Conceptions of the Expectation of Privacy

In order to avoid this circular interpretation of what is "constitutionally justifiable" and to enhance the neutrality of the *Katz* test, a social aspect was introduced by the courts. In the *White* case, Justice Harlan argued that an expectation of privacy should be determined by an examination of the desires of society at large.[118] Moreover, in his dissent he also introduced the expression a "sense of security", in order to give a more balanced approach. He emphasized that what is protected by the 4th Amendment "must … be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement".[119] The "sense of security" referred to attempts to balance the private and the public interests. He further explained that "the customs and values of the past and present" should be taken into account when determining the expectation of privacy.[120]

The use of the term "justifiable" shows that the Court intended to introduce a more consistent standard based on legal norms.[121] The term "sense of security" was created to establish a determination of the social expectation of privacy; however, it is still not a very clear definition and thus does not really contribute to a better understanding of social expectations of privacy.

In cases regarding houses, cars, closed telephone booths, etc., it has been well established that society recognizes the expectation of privacy in these locations.

[116] The meaning of "justifiable" is referred to the term in Black's Law Dictionary, 2019, 11th ed: "Legally or morally acceptable for one or more good reasons; excusable; defensible".

[117] *United States v. White*, 401 U.S. 745, 752 (1971) ("Our problem, in terms of the principles announced in Katz, is what expectations of privacy are constitutionally 'justifiable' – what expectations the Fourth Amendment will protect in the absence of a warrant.") (White, J., opinion of the Court).

[118] *Id.* at 786 ("Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society.") (Harlan, J., dissenting).

[119] *Ibid.*

[120] *Ibid.* ("Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.") (Harlan, J., dissenting).

[121] *Sobel* et al., Boston University Public Interest Law Journal 22 (2013), 1, 23.

There are also a large number of cases in which the expectation of society is debatable. For instance, in *Dow Chemical Co. v. U.S.*,[122] Dow had maintained ground security in order to protect the factory from public view from the ground. The Environmental Protection Agency, however, engaged in warrantless aerial photography of the factory from above. The Court did not clearly articulate its attitude towards Dow's subjective expectation of privacy and denied the claim on the basis on the second prong of the test. It argued that any individual could have used a plane to take photos of the factory, just as the Agency had done. Thus, in light of the further development of aerial photography, the Court decided that society does not recognize the reasonable expectation of privacy with regard to a view of a building from the air.[123]

According to this decision, the recognition of society of the reasonable expectation of privacy can be reduced or even eliminated by "the effect of modern life, with its technological and other advances".[124] This concern was reflected in the *Kyllo* case, where the Court decided that this constituted a search because the technology in question was not "in general public use".[125] Although the Court upheld the reasonable expectation of privacy of the defendant, the remaining issue of whether the technology was "in general public use" is still as problematic as in the *Dow* case. This is because any technology not in general public use at the current time might be used by the public in the future. If the expectation of society is based purely on the availability of technology, this could result in the destruction of the very conception of privacy as we currently understand it. As stated in the *Kyllo* case, this would demonstrate the "power of technology to shrink the realm of the guaranteed privacy".[126]

Besides the availability of technology, the government's regular conduct, legislation or regulations can also reduce society's expectation of privacy. When society takes certain conduct or phenomena for granted, an earlier expectation of society may no longer be recognized by the courts. In addition, the Court might use State or Federal legislation for determining the expectation of society,[127] such as in *New York v. Burger.*[128] This could result in the Government diminishing the scope of the protection of the 4th Amendment at will.[129] Furthermore, if legislation that was used

[122] *Dow Chemical Co.*, 476 U.S. 227 (1986).

[123] *Id.* at 231 ("The photographs at issue in this case are essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them. In common with much else, the technology of photography has changed in this century."). See also *Julie*, American Criminal L. Rev. 37 (2000), 127, 131–132.

[124] *Clancy*, Wake Forest L. Rev. 33 (1998), 307, 335.

[125] *Kyllo v. United States*, 533 U.S. 27, 28 (2001). See Section 3, Chapter I, Part I.

[126] *Id.* at 34.

[127] *Shaff*, Southern California Interdisciplinary L. J. 23 (2014), 409, 438.

[128] *New York v. Burger*, 482 U.S. 691 (1987). See also *Sobel* et al., Boston University Public Interest Law Journal 22 (2013), 1, 24.

[129] *Julie*, American Criminal L. Rev. 37 (2000), 127, 132.

as a basis for a court decision is modified or repealed, this could cast doubt on the validity of the court decision.[130]

From another perspective, legislation represents democracy and is assumed to reflect social values. More specifically, legislation might demonstrate the expectations of society more accurately than court decisions. "In circumstances involving dramatic technological change",[131] legislation can balance the needs of privacy and public security better than the courts. If courts do not utilize legislation as evidence when determining the expectations of society and instead base their decisions upon their own subjective evaluations, it is difficult to argue that courts demonstrate a better understanding of society than legislatures. Given these issues, it is doubtful whether the second prong of the *Katz* test contributes in a meaningful way to protecting privacy under the 4th Amendment.

bb) An Empirical Study of General Attitudes toward Privacy

In the *White* case, Justice Harlan stated in his dissent that judges should not "merely recite the expectations and risks without examining the desirability of saddling them upon society."[132] On the one hand, it seems impossible for courts to precisely determine the expectation of society as a whole without a scientific survey; on the other hand, however, it would be infeasible to conduct such a study before every court ruling. Whether a judgment is right or wrong thus depends upon whether the court correctly evaluates social attitudes in a dynamic way based on the considerations of "the customs and values of the past and present"[133] and "contemporary norms of social conduct and the imperatives of a viable democratic society".[134] This is referred to as "a value judgment".[135]

Moreover, it is important to consider whether different age groups, social classes, religious groups and genders have different attitudes towards privacy. For instance, would the "Facebook generation", who share their daily lives online, place less value on their privacy than the elderly? In order to establish the degree to which the

[130] *McCabe*, Temple L. Rev. 65 (1992), 1229, 1251.

[131] *United States v. Jones*, 565 U.S. 400 (2012) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.") (footnote omitted) (*Alito*, J., Concurring). See also *Shaff*, Southern California Interdisciplinary L. J. 23 (2014), 409, 439.

[132] *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[133] *Id.* at 786 (Harlan, J., dissenting).

[134] *United States v. Vilhotti*, 323 F. Supp. 425, 431 (S.D.N.Y. 1971). Other similar expressions, for example, "… to define fundamental constitutional values by referring to contemporary social values, goals, and attitudes", *Cloud*, UCLA L. Rev. 41 (1993), 199, 250.

[135] *Amsterdam*, Minnesota L. Rev. 58 (1974), 349, 403.

opinions of society differ from those of the judiciary, an American law professor[136] in 2011 conducted an empirical study among 589 people from various backgrounds including Facebook users. This study selected some of the leading precedents on the 4th Amendment regarding search and seizure and used the five-point Likert scale (from strongly disagree to strongly agree) to measure levels of agreement/disagreement among the participants with regard to these precedents.[137] 63.1 % of respondents agreed that a warrant is required to record a phone conversation, even on a public telephone, compared to only 23.1 % who disagreed (in reference to the *Katz* case). When the communication involved a private cell phone, 91.7 % of the respondents agreed that a warrant was required for wiretapping or other recording devices, while only 7.1 % disagreed.[138] Regarding the *Kyllo* case, where a warrant was needed for the adoption of a thermal-imaging device,[139] the agreement level was 59.9 %, while the disagreement level was 23.8 %.[140] 85.5 % disagreed with the judgement in the *Knott* case, where the court ruled that police did not need a warrant to install a tracking device on a private car.[141] This study demonstrates that the respondents expressed significant levels of agreement with the precedents which protected privacy but voiced significant levels of disagreement when the precedents upheld the government's warrantless surveillance. This indicates that the judges often misapprehend attitudes of the public regarding the protection of the 4th Amendment.[142]

With regard to the expectation of privacy of communications, the age and gender of the participants did not play a significant role for their attitudes. Republican Independents showed a significantly low support for the protection of the privacy of communications.[143] Another variable with strong impact in this domain is the education level of the participants. More educated participants placed a stronger emphasis on the need to protect the privacy of communications.[144]

The profound gap between the findings of courts and this empirical study suggests that judges should continuously try to "find and articulate those societal standards"[145]

---

[136] *Fradell*a et al., American Journal of Criminal Justice 38 (2011), 289. The expectations of privacy of 549 persons from various backgrounds were evaluated. Other empirical research can be found in *Slobogin*, Privacy at Risk: New Government Surveillance and the Fourth Amendment, 2007; *Blumenthal* et al., University of Pennsylvania Journal of Constitutional Law 11 (2009), 331, 341.

[137] *Fradell*a et al., American Journal of Criminal Justice 38 (2011), 289, 342.

[138] *Id.* at 366. The difference of statistics is significant ($p<0.001$).

[139] *Kyllo v. United States*, 533 U.S. 27, 28 (2001).

[140] *Fradell*a et al., American Journal of Criminal Justice 38 (2011), 289, 357, Table 6.

[141] *Ibid.*

[142] *Id.* at 371 – 372.

[143] *Id.* at 360, Table 8.

[144] *Ibid.*

[145] *Douse*, University of Michigan Journal of Law Reform 6 (1972), 154, 179 – 80.

which must be abstracted from "the flow of life".[146] This empirical study could serve as a quality control *ex post facto* to help judges adjust their reasoning in future cases.

5. The Minimal Expectation of Privacy

Although the "reasonable expectation of privacy" test has met with great approval, it has created new problems that did not exist under the "trespass" doctrine. One of the most serious defects of the new theory is its ineffectiveness with regard to the threat of new technologies that have shrunk "the realm of guaranteed privacy"[147], as discussed above.[148] If the courts rely upon the reach of technology to decide what kind of expectation of privacy is retained, then no aspect of privacy may remain, even for those "who live within windowless, sound-proof forts",[149] or it will become a luxury that almost no one can afford because huge amounts of money would have to be invested in anti-surveillance technology to safeguard privacy. This conflict is reflected in the *Kyllo* case,[150] where the majority opinion emphasized that "the minimal expectation of privacy" still exists and that the interior of the home falls within this category:[151] "To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[152]

The issue then becomes what should be regarded as falling under the "minimal expectation of privacy". Home, without question, should be included in this category,[153] but should not be the only location. Justice Harlan stated in *Mancusi v. DeForte*[154] that a constitutionally protected area can be independent from a property right, but that it depends upon whether one has a reasonable expectation in that particular place.[155] No physical trespass is required, and any invisible technical in-

[146] *Ibid.*

[147] *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

[148] See Section 4. b), Chapter I, Part I.

[149] *Aynes*, Cleveland State L. Rev. 23 (1974), 63, 72.

[150] *Kyllo v. United States*, 533 U.S. 27 (2001).

[151] *Id.* at 34.

[152] *Ibid.*

[153] For example, *Lewis v. United States*, 385 U.S. 206, 211(1966) ("Without question, the home is accorded the full range of Fourth Amendment protections".).

[154] *Mancusi v. DeForte*, 392 U.S. 364 (1968). In this case, the state officers, without a warrant, seized business records from an office shared by respondent and several other union officers. The Court found that the search here was a violation of the 4th Amendment. (*Id.* at 365 – 368.)

[155] *Id.* at 368 ("The Court's recent decision in *Katz v. United States*, 389 U.S. 347, also makes it clear that capacity to claim the protection of the Amendment depends not upon a property right in the invaded place, but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion.") (Harlan, J., opinion of the Court).

trusion into a place which allows information to be obtained "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area'" is regarded as an equivalent to a physical intrusion. A similar argument can be found in *U.S. v. Karo* where the Court stated that the use of a tracking device is the equivalent of a search of a home because both had the same potential to gather evidence.[156] In this case, the Court introduced a "hypothetical" approach, asking whether the information could have been obtained legally under the "trespass theory" without using the tracking device.[157] Some authors have referred to this interpretation as a "loose property-based approach".[158]

6. Other Constitutional Aspects of Electronic Surveillance

The legality of electronic surveillance of wire and oral communications by law enforcement officers can also be challenged on the basis of other constitutional rights.

a) 5th Amendment: Privilege against Self-incrimination

Electronic surveillance is done covertly in order to record self-incriminating statements of suspects to be used as evidence against them. The 5th Amendment provides that no one "shall be compelled in any criminal case to be a witness against himself". This constitutional privilege against self-incrimination is designed to prevent a person from being compelled to make self-incriminating statements.[159] In the following paragraphs, I will examine whether covert surveillance is regarded as a compulsory collection of self-incriminating evidence.

One landmark case for the right under the 5th Amendment is *Miranda v. Arizona.* In this case, the U.S. Supreme Court ruled that statements resulting from questioning initiated by law enforcement officers after a person has been taken into custody cannot be used against this person unless procedural safeguards were taken to secure the 5th Amendment's privilege against self-incrimination.[160] The *Miranda* safe-

[156] *United States v. Karo*, 468 U.S. 705, 715 (1984).

[157] *Ibid.*

[158] See *United States v. Jones*, 565 U.S. 400 (2012) (Justice Scalia stated that the Katz test was merely "added to, not substituted for, the common-law trespassory test".); see also *Kerr*, Michigan L. Rev. 102 (2004), 801, 820. The author also argued in this article that "loose property-based approach" towards the 4th Amendment protection merely articulated the legal standard that the Court had applied before, such as in *Jones v. United States*, 362 U.S. 257 (1960). See also *Junker*, Journal of Criminal Law & Criminology 79 (1989), 1105, 1125–26 ("What is remarkable, however, is how little was changed by Katz's abandonment of the 'trespass' standard of *Olmstead v. United States* and *Goldman v. United States.*").

[159] *United States v. White*, 322 U.S. 694, 698 (1944).

[160] *Miranda v. Arizona*, 384 U.S. 436, 436 (1966).

guards, however, only come into play when "a person in custody is subjected to either express questioning or its functional equivalent".[161] The main concern of the Court here was that custody and interrogation could create an "interrogation environment" that may "subjugate the individual to the will of his examiner" and thereby undermine the privilege against compulsory self-incrimination.[162] Interceptions adopted by police or undercover agents are, however, done covertly and thus do not create an "interrogation environment" that could undermine the free will of suspects. In addition, suspects whose communications are intercepted are normally not in custody or being questioned by the police. Therefore, *Miranda* is not applicable in most cases of interception.

In *Hoffa v. U.S.*, the defendant made self-incriminating statements on bribing members of a jury during conversations with a paid informant, who disclosed the information to the prosecutors. The U.S. Supreme Court held that the admission of such incriminating evidence is not a violation of the 5th Amendment[163] because there had been no compulsion. The defendant was voluntarily engaged in conversation with the informant.[164] Although this case is about an informant's testimony, not a recording, the rationale is the same. The 5th Amendment only protects against statements that are compelled.[165] In order to constitute compulsion, a specific threat needs to be made, which coerces the person into making the statement.[166] According to the interpretation of the courts, a fake identification by an undercover agent or informant is not deemed compulsion.[167] The same ruling has been applied to the monitoring of phone calls in a jail or in a wiretapping situation.[168]

b) The Attorney-Client Privilege

The attorney–client privilege refers to a "client's right to refuse to disclose and to prevent any other person from disclosing confidential communications between the client and the attorney",[169] in order "to encourage full and frank communication between lawyers and their clients and thereby promote broader public interests in

[161] *Rhode Island v. Innis*, 446 U.S. 291, 292 (1980). More discussion about the meanings of custody and interrogation in Miranda case can be found: *Roberson*, Constitutional Law and Criminal Justice, 2016, 141 – 145.

[162] *Miranda v. Arizona*, 384 U.S. 457 – 458 (1966).

[163] *Hoffa v. U.S.*, 385 U.S. 293, 303 – 304 (1966).

[164] *Id.* at 383.

[165] *King* and *Kilby*, Georgetown L. J. 90 (2002), 1690, 1691.

[166] *U.S. v. Harnage*, 662 F. Supp. 766, 780 (D. Colo. 1987).

[167] *Powers v. Coe*, 728 F.2d 97, 106 (2d Cir. 1984); *Illinois. v. Perkins*, 496 U.S. 292, 293 (1990) (no 5th Amendment violation when suspect made incriminating statements to undercover agent posing as cellmate because suspect was not compelled).

[168] *Carr* et al., The Law of Electronic Surveillance, 2020, § 2.61.

[169] *Garner* (ed.), Black's Law Dictionary, 2014, 1391.

observance of law and administration of justice".[170] Surveillance of privileged communications between a lawyer and his client, through electronic interception or by means of an informant, constitutes an intrusion into this privilege.[171] In addition, in *Caldwell v. United States*, the Federal Court of Appeals for the D.C. Circuit held that the participation of an undercover government agent in the defense team, who regularly reported to the prosecutor on the case at hand, violated the defendant's 6th Amendment right to counsel. The court argued that such a practice was equivalent to an intrusion through wiretapping.[172]

However, communications between the defendant and his counsel do not fall under the attorney-client privilege if third parties are present.[173] This limitation of the privilege can be explained on the basis of the "reasonable expectation of privacy" requirement,[174] according to which "the assertor of the privilege must have a reasonable expectation of confidentiality, either that the information disclosed is intrinsically confidential, or by showing that he had a subjective intent of confidentiality."[175] The defendant and his lawyer implicitly waive the protection of confidentiality if they allow a person who is not a member of the defense team to be present.

c) 6th Amendment: The Right to Counsel

The 6th Amendment provides that "in all criminal prosecutions, the accused shall enjoy the right to … have the assistance of counsel for his defense." This amendment guarantees both access to counsel and the right to effective assistance of counsel[176] in order to "protect an accused from conviction resulting from his own ignorance of his

---

[170] *Upjohn v. United States*, 449 U.S. 383, 389 (1981).

[171] See, e. g., *Briggs v. Goodwin*, 698 F.2d 486, 494–495 (D.C. Cir. 1983) (the attorney-client privilege is violated when government informer transmitted confidential conversations between the defendant and his attorney to the prosecution).

[172] *Caldwell v. United States*, 205 F.2d 879, 881 (D.C. Cir. 1953).

[173] *United States v. Pipkins*, 528 F.2d 559, 563 (5th Cir. 1976). See also *United States v. Melvin*, 650 F.2d 641, 646–47 (5th Cir. Unit B 1981) ("Disclosures made in the presence of third parties may not be intended or reasonably expected to remain confidential."); *United States v. Landof*, 591 F.2d 36, 39 (9th Cir. 1978) (presence of third person who was not "acting as an attorney or an agent at the meeting destroyed the privilege").

[174] *Jones/Rosen* et al., Federal Civil Trials and Evidence, 2020, Chapter 8H-B. See also *United States v. Pipkins*, 528 F.2d 559, 563 (5th Cir. 1976) ("It is vital to a claim of privilege that the communication have been made and maintained in confidence".).

[175] *United States v. Robinson*, 121 F.3d 971, 976 (5th Cir. 1997); *United States v. Pipkins*, 528 F.2d 559, 563 (5th Cir. 1976); *United States v. Melvin*, 650 F.2d 641, 646–647 (5th Cir. Unit B 1981) ("It is not enough for the meeting to be between a lawyer and would-be client, or that the meeting take place away from public view.").

[176] *Friedman*, Washington University Journal of Urban and Contemporary Law 40 (1991), 109, 111. See also *Note*, Journal of Criminal Justice 7 (1983) 97.

legal or constitutional rights."[177] The Supreme Court explained that such right to counsel begins only at, or after, the time that adversarial judicial proceedings have been initiated against the defendant.[178] Therefore, the involved persons cannot claim the right to counsel if the police have applied for a surveillance order or an arrest warrant before they have been charged with a crime. Surveillance, however, can violate the right to counsel of the intercepted person if it is conducted after official proceedings have begun. For example, in *Massiah v. United States*[179] the defendant was released on bail after his indictment and was invited by a co-defendant, who was cooperating with law enforcement, to discuss the case in the co-defendant's car, where a radio transmitter was installed. During this conversation, the defendant made self-incriminating statements, which were overheard by a police agent. The Court did not decide this case on the basis of the 4th Amendment but the 6th Amendment, stating that such a conversation was actually an interrogation of the defendant, that he was not even aware that it was conducted, and that the statement was elicited from him in the absence of counsel.[180] Therefore, the defendant's right to counsel was violated and his statements could not constitutionally be used as evidence against him at his trial.[181]

d) Summary

Generally speaking, the constitutionality of surveillance, regarding other constitutional issues besides the 4th Amendment, is as follows: (1) The covert interception of conversations does not violate the 5th Amendment, which only protects individuals from being compelled to make self-incriminating statements; (2) After the initiation of judicial proceedings, interceptions are restricted by the right to counsel. The interception of interrogation-style conversations which take place in the absence of counsel violates the 6th Amendment;[182] (3) conversations between an attorney and his client are protected by the attorney-client privilege. The privilege is deemed to be waived if the attorney and his client allow a third person to be present at the conversation; in this situation, the recording made by this third person may be used as evidence.

---

[177] *Johnson v. Zerbst*, 304 U.S. 458, 465 (1938).

[178] According to the case law, the initiated point can be "formal charge, preliminary hearing, indictment, information, or arraignment." *Kirby v. Illinois*, 406 U.S. 682, 689 (1972).

[179] *Massiah v. United States*, 377 U.S. 201 (1964).

[180] *Id.* at 206. A Federal court of Appeals, however, later decided that if the interception is totally conducted by codefendant as a private activity without involvement of law enforcement, such activity does not violate the ruling in Massiah since Massiah only prevent individuals from elicitation of law enforcement. See *U.S. v. Johnson*, 4 F.3d 904, 910–912 (10th Cir. 1993) and *Carr* et al., The Law of Electronic Surveillance, 2020, § 2.63.

[181] *Massiah v. United States*, 377 U.S. 201, 204 (1964).

[182] *Carr* et al., The Law of Electronic Surveillance, 2020, § 2.63.

II. Surveillance of Wire and Oral Communications in Federal Statutes

Wiretapping is the use of a device to intercept a communication sent by wire.[183] The history of wiretapping began as soon as communication could be transmitted by wires. As early as in 1864, people intercepted news of stock operations and sold the information.[184] During the Civil War, soldiers were trained specifically in wiretapping. In the 1900s, wiretapping was also used to intercept news stories.[185] The intrusive nature of such activities soon gave rise to criticism and led to the prohibition of private wiretapping in several states.[186] In 1918, Congress adopted a temporary measure to protect government secrets from wiretapping.[187] Surveillance of oral communications refers to the use of electronic devices to overhear or record one's conversation and can be more intrusive than a wiretap.[188] Given this context, the legislature regulated surveillance of wire and oral communications through statutes.

1. Early Regulation

Although the Court in the *Olmstead* case declined to recognize that wiretapping was covered by the 4th Amendment, the majority opinion of the Court invited Congress to pass a statute to regulate wiretapping.[189] Six years later, Congress passed

[183] *Kerr*, Michigan L. Rev. 102 (2004), 801, 840.

[184] He was charged under the statute against wiretapping telegraph passed by California in 1862. See Long, *The intruders*, 1967, 36.

[185] *Long*, The intruders, 1967, 36.

[186] "At least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both" before *Olmstead v. United States*, 277 U.S. 438 (1928). See *Doyle*, Privacy, 2012, 2. For example, telephone wiretapping was prohibited in New York and Illinois in 1895; California extended its ban on telegraph interception to telephones in 1905. By 1928, more than half of the states had enacted criminal bans on wiretapping. See *Kerr*, Michigan L. Rev. 102 (2004), 801, 841. More detailed information about which states have forbidden interception can be found *Berger v. New York*, 388 U.S. 41, 48–49 (1967), Fn. 268.

[187] 40 Stat.1017–18 (1918) ("whoever during the period of governmental operation of the telephone and telegraph systems of the United States … shall, without authority and without the knowledge and consent of the other users thereof, except as may be necessary for operation of the service, tap any telegraph or telephone line … or whoever being employed in any such telephone or telegraph service shall divulge the contents of any such telephone or telegraph message to any person not duly authorized or entitled the receive the same, shall be fined not exceeding $1,000 or imprisoned for not more than one year or both"); 56 Cong. Rec. 10761–765 (1918). See also *Doyle*, Privacy, 2012, 2.

[188] *Carr* et al., The Law of Electronic Surveillance, 2020, § 1.2.

[189] "Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence. But the courts may not adopt such a policy by

the first Federal wiretapping law. *The Communications Act of 1934.* Section 705, which was later codified as 47 U.S.C. § 605,[190] included a prohibition of intercepting and divulging radio or wire communications.[191] This statute made wiretapping a criminal offense,[192] however, it did not expressly state that it also regulated wiretapping conducted by law enforcement officers. In 1937, the Supreme Court made it clear in *Nardone v. United States* that the conduct of law enforcement officers is also subject to this statute.[193] The Justice Department, however, found a way to bypass this case law and stated that the statute only prohibits the admission of wiretap evidence, not the act of wiretapping itself.[194] This resulted in the practice that law enforcement intercepted wire communications whenever they liked but did not present the findings in court.[195] Due to the rise of the need to fight organized crime, this practice led to serious criticism[196] in the 1960s, because this practice neither protected privacy nor helped law enforcement to win cases.[197] Therefore, a reform of wiretapping law was demanded.[198] In this context, the Supreme Court got an opportunity to elaborate on several criteria for a constitutional statute in *Berger v. New York.* In that case, the State Supreme Court of New York had permitted a recording device to be placed in an

attributing an enlarged and unusual meaning to the Fourth Amendment." *Olmstead v. United States*, 277 U.S. 438, 465–466, (1928).

[190] Sec. e. g. 605(a), 48 Stat. 1064, 1103–04 (1934).

[191] 48 Stat. 1103–104 (1934), 47 U.S.C. 605 (1940 ed.).

[192] See *Kerr*, Michigan L. Rev. 102 (2004), 801, 845; and also *Kapla/Matteo* et al., The History and Law of Wiretapping, ABA Section of Litigation 2012 Section Annual Conference April 18–20, 2012, 3.

[193] *Nardone v. United States*, 302 U.S. 379 (1937) ("the phrase 'no person' comprehends federal agents, and the ban on communication to 'any person' bars testimony to the content of an intercepted message. To recite the contents of the message in testimony before a court is to divulge the message."). It is also argued, however, that there is precedence decided by the Court that general wording does not apply to governmental conducts, and the testimony of the content of the wiretapping could also not be defined as "divulging". See *Rosenzweig*, Cornell Law Quarterly 32 (1946–1947), 514, 535 and Fn. 137–38.

[194] *Kerr*, Michigan L. Rev. 102 (2004), 801, 845–846.

[195] *Ibid.*

[196] For example, "One of the most serious consequences of the present state of the law is that private parties and some law enforcement officers are invading the privacy of many citizens without control from the courts and reasonable legislative standards… The present status of the law with respect to wiretap ping and bugging is intolerable." President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society, 1967, 203.

[197] See "it serves the interests neither of privacy nor of law enforcement." *Ibid.* It was also criticized as both "overprotection and under protection". Overprotection refers to the fact that the wiretapping evidence was not allowed to be used in Federal Court at all; however, it was also underprotection because law enforcement could wiretap as long as they did not present the evidence in court. *Kerr*, Michigan L. Rev. 102 (2004), 801, 847.

[198] See "… the present controversy with respect to electronic surveillance must be resolved… . Congress should enact legislation dealing specifically with wiretapping and bugging." *Ibid.*

attorney's office for a period of 60 days.[199] The U.S. Supreme Court held that the statute must require a surveillance warrant to include a specific description of the location, the persons and the things to be searched or seized; a specific description of the crime under investigation; a specific description of the conversation to be intercepted; a clear termination point of the interception; a requirement for the prompt execution of the order; sufficient demonstration of probable cause for an extension of the order; the requirement of a return of service to the issuing court of the records of the intercepted conversations; and a demonstration of exigent circumstances to overcome the requirement of prior notice.[200]

This decision, together with *Katz*, gave Congress a clear instruction on how to enact a new statute without violating the 4th Amendment. *Title III* came into force within this context and authorizes law enforcement agencies to intercept wire and oral communications according to the criteria described in *Berger v. New York*[201].

2. The Modern Statute

The revised Title III, i. e., 18 U.S.C. §§ 2510 – 2522 (Chapter 119), is part of the *Electronic Communications Privacy Act* (ECPA).[202] The title of this chapter is *Wire and Electronic Communications Interception and Interception of Oral Communications*, which indicates that it applies not only to wire but also to oral and electronic communications. Generally speaking, *Title III* prohibits the interception of wire, oral and electronic communications without authorization and introduces judicial supervision. *Title III* incorporated, to a large degree, the "reasonable expectation of privacy" concept of the *Katz* case discussed above. In order to avoid potential conflicts with constitutional standards established by courts, the Senate took the case law of the U.S. Supreme Court, such as the *Silverman*, *Berger* and *Katz* judgments, into account when drafting the new legislation.[203] After this statute came into force, most case law interpreted its rules, as opposed to referring directly to the 4th Amendment. Although the constitutional arguments concerning the 4th Amendment, such as in *Berger* and *Katz*, are still referred to, *Title III* is more commonly

[199] *Berger v. New York*, 388 U.S. 41 (1967).

[200] *Berger v. New York*, 388 U.S. 41, 54 – 60 (1967). See also *Kerr*, Michigan L. Rev. 102 (2004), 801, 848; Doyle, Privacy, 5; *Pikowsky*, Michigan Telecommunications and Technology L. Rev. 1 (2003), 31.

[201] *Berger v. New York*, 388 U.S. 41 (1967).

[202] The other two parts of ECPA are *The Stored Communications Act* (18 U.S.C. §§ 2701 – 2712) regulating the government's access to stored electronic communications, and *The Pen Register Statute* (18 U.S.C. §§ 3121 – 3127) which contains rules regarding the use of pen registers and trap and trace devices.

[203] S.Rep. No. 1097, 90th Cong., 2d SeS. (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2178.

applied directly in everyday practice.[204] This indicates that statutory protection is ultimately the most significant tool in this area of law.[205]

a) The Definition of "Wire Communication" under § 2510(1) of *Title III*

The wire communications protected by *Title III* are defined under § 2510(1) as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection … including the use of such connection in a switching station…".[206] "Aural transfer" is further described in § 2510(18) as "a transfer containing the human voice at any point between and including the point of origin and the point of reception", which excludes "computer-generated or otherwise artificial voices".[207] Compared to the original version of *Title III* enacted in 1968, the ECPA enlarged the scope of "wire communications". First, the ECPA protects wire communications transmitted by "private networks and intra-company communications systems",[208] instead of only by "a common carrier";[209] secondly, the ECPA added the expression "including the use of such connection in a switching station" to clarify that cell phone communications are covered by the definition of "wire communications"[210] because cell phones without "wire" communicate through switching stations. The language "in whole or in part…by the aid of wire…" still excludes communications transmitted only via radio,[211] although cellular and radio communications[212] are both "wireless". Another

[204] For example, *U.S. v. White*, 746 F.2d 426, 427(1984). Although there were still cases challenging the constitutionality of this statute, the claims were normally rejected. *Kerr*, Michigan L. Rev. 102 (2004), 801, 850–851, and Fn. 304. See also *United States v. King*, 335 F. Supp. 523, 531–32 (S.D.Cal.1971).

[205] It is also regarded as the symbol of "modern era" of wiretapping law. *Kerr*, Michigan L. Rev. 102 (2004), 801, 850.

[206] U.S.C. § 2510(1).

[207] See S.Rep. No. 541, 99th Cong., 2d SeS. 12 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 16. https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf, visited at 28.08.2020.

[208] *Id.* at 12.

[209] S.Rep. No. 1097, the formal legislative history of Title III, explained "wire communications" "to include all communications carried by a common carrier, in whole or in part, through our Nation's communications network." See 1968 U.S. Code Cong. & Admin. News at 2178 (discussing 18 U.S.C. §§ 2510(1) & (2)).

[210] S.Rep. No. 541, 11.

[211] *Id.* at 14–15. See for example, *United States v. Hall*, 488 F.2d 193, 196 (9th Cir. 1973). In this case, the radio communications into the air by radio waves were categorized as "oral communications in a loud voice or with a megaphone" rather than as wire communications. Meanwhile, regarding to the radio-telephone conversations, the court had to draw the conclusion that "when part of a communication is carried to or from a land-line telephone, the entire conversation is a wire communication and a search warrant is required," although the court admitted that such conversations should not enjoy more protection than radio-radio conversations. (*United States v. Hall*, 488 F.2d 193, 196–98 (9th Cir. 1973)).

similar communication device is the cordless phone.[213] Before the ECPA, the courts decided that cordless phones were not protected by *Title III*[214] since the radio waves between the base unit and the handset can be easily picked up by a normal radio scanner.[215] Due to the anxiety that persons might be subject to criminal and civil liability just by listening to a radio,[216] Congress expressly excluded protection for cordless telephone communications in the ECPA in 1986.[217] When cordless phone conversations became more difficult to intercept because of the development of technology, Congress passed *The Communications Assistance for Law Enforcement Act* (known as CALEA or the Digital Telephony Bill) to amend *Title III*, in order to include cordless telephone conversations.[218]

Contrary to the definition of "oral communication" provided in § 2510(2), the definition of wire communication does not reflect the test of the expectation of privacy. This could be interpreted as Congress trying to prohibit any warrantless wiretapping by statute.[219] Even under the *Katz* test, a reasonable expectation of privacy during wire communication is largely recognized, and a warrant for the

---

[212] Certain radio communications fall within the scope of "electronic communications" in § 2510(12). 18 U.S.C. §§ 2510(12).

[213] There is no doubt that the transmission between one end and the basic unit of cordless phone in the other end is subject to the rule of wire communications, however, the radio transmission between the base unit and the handset was used to be under discussion. One of the first cases to deal specifically with cordless phone was *State v. Howard*, 235 Kan. 236 (1984).

[214] Before the ECPA, the courts treated the conversations via cordless phone the same as radio transmission. See, e. g., *State v. Howard*, 235 Kan. 236, 204 (1984); and *State v. Delaurier*, 488 A.2d 688, 693 (R.I. 1985) ("But the communications broadcast over the AM airwaves were the result of the generation of radio waves by defendant's hand-held mobile unit and base unit. The transmission lines played a part only in that they carried signals to or from the base unit. These signals were not interfered with."); *Tyler v. Berodt*, 877 F.2d 705 (8th Cir. 1989); *Price v. Turner*, 260 F.3d 1144, 1146–47 (9th Cir. 2001).

[215] See *McKamey v. Roach*, 55 F.3d 1236, 1239–40 (6th Cir. 1995); *United States v. Smith*, 978 F.2d 171, 178–79 (5th Cir. 1992).

[216] *State v. Delaurier*, 488 A.2d 688, 694 (R.I. 1985). See S.Rep. No. 541, 16.

[217] "'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) the radio portion of a cordless telephone communication that is transmitted between the cordless handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; or (D) any communication from a tracking device (as defined in section 3117 of this title)," 18 U.S.C. 2510(12) (1986) (*emphasis added*).

[218] *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.3; see also H.R.Rep. No. 827, 103d Cong., 2d SeS. 10, 17–18, 30 (1994), *reprinted in* 1994 U.S.C.C.A.N. *Price v. Turner*, 260 F.3d 1144, 1148 (9th Cir. 2001). Even though it is clear that cordless phones are protected by the statute, there are still arguments about what category of radio communication a cordless phone falls within, whether it is considered to be a wire communication or an electronic communication. See *Mangano*, Cleveland State L. Rev. 44 (1996), 99.

[219] *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.3.

interception is always needed. Therefore, *Title III* and the *Katz* test may reach the same result.

If, for example, law enforcement officers overhear one end of a conversation without using a wire, this does not fall within the concept of "wire communications",[220] because the conversation was not transmitted "between the point of origin and the point of reception".[221] Such surveillance would be subject to the standards for oral communications.[222] This ruling also has further implications. For example, the legal status of background conversations recorded by a tapped telephone which has been left off the hook is still unclear. According to the courts' understanding of "between the point of origin and the point of reception", the courts distinguished two situations, i. e., "between background discussions during a point-to-point phone call and face-to-face discourse while no point-to-point call is in progress".[223] In the former situation, the court decided that background conversations overheard by law enforcement are part of wire communications, since the parties of such a conversation could expect their conversations to be transmitted via wire to the other end of the line.[224] For the latter, the court upheld the view that background conversations are not "wire communications" and therefore are not covered by the legislation regarding wiretapping,[225] because such conversations only involve one communication device and no other "point of reception".[226]

b) The Definition of "Oral Communication" under § 2510(2) of *Title III*

The definition of "oral communications" in § 2510(2) covers "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication."[227] According to the legislative explanation, this definition "is intended to reflect existing law"[228] rather than creating a new protected scope for "oral communications". It fully adopts the two-pronged test in *Katz* and limits the application of *Title III* to oral communications that pass the

[220] *United States v. McLeod*, 493 F.2d 1186, 1188 (7th Cir. 1974).

[221] 18 U.S.C. § 2510(1).

[222] *United States v. Carroll*, 332 F. Supp. 1299, 1301 (D.D.C. 1971).

[223] *United States v. Borch*, 695 F. Supp. 898, 901 (E.D. Mich. 1988). Cf. *People v. Basilicato*, 474 N.E.2d 215, 217 (1984) and *United States v. Feola*, 651 F. Supp. 1068 (S.D.N.Y.1987).

[224] *People v. Basilicato*, 474 N.E.2d 215, 217 (1984).

[225] *United States v. King*, 335 F. Supp. 523, 548 (S.D.Cal.1971).

[226] *United States v. Borch*, 695 F. Supp. 898, 901 (E.D. Mich. 1988).

[227] 18 U.S.C. § 2510(2).

[228] S.Rep. No. 1097, 2178.

expectation test, i. e., the speaker demonstrates his expectation to keep his conversation private and the circumstances justify his expectation.[229]

Applying *Title III*, courts have summarized the following non-exclusive factors for deciding whether oral communications pass the test: "(1) the volume of the communication or conversation; (2) the proximity or potential of other individuals to overhear the conversation; (3) the potential for communications to be reported to authorities;[230] (4) the affirmative actions taken by the speakers to shield their privacy; (5) the need for technological enhancements to hear the communications; and (6) the place or location of the oral communications as it relates to the subjective expectations of the individuals who are communicating."[231] In practice, the number of warrants for the surveillance of oral communications is extremely limited, especially when compared with the large number of wiretaps.[232]

c) The Definition of "Intercept" under § 2510(4) of *Title III*

§ 2510(4) defines an "intercept" as the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. From this text, it is not clear whether recordings are covered by this definition. Some states expressly include recordings in the definition of intercept in their statutes, while others prohibit warrantless recordings as well as interception. Since § 2510(4) provides for aural "or other" acquisition of the contents of communications, recordings should be interpreted as a form of interception in need of better protection under *Title III*.[233]

A further question caused by the ambiguity of *Title III*'s definition of intercept is whether conversations may be intercepted without simultaneous monitoring. In principle, the minimization requirement is violated because non-pertinent conversations cannot be minimized without simultaneous monitoring.[234] However, a Federal Court of Appeals allowed the recording of telephone conversations conducted in Spanish without simultaneous monitoring.[235] The Court held that the minimization provision of § 2518(5) was satisfied when all conversations were recorded in their entirety first and heard by Spanish-speaking agents afterwards to determine which parts of the conversation were pertinent. Although *Title III* requires

---

[229] 18 U.S.C. § 2510(2); and see also *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.5.

[230] This consideration comes from *United States v. White*, 401 U.S. 745, 749 (1971) (finding that individuals take the risk that their conversations will be reported to authorities).

[231] *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.5 (Quoting from *Kee v. City of Rowlett*, *Tex.*, 247 F.3d 206, 213 – 14 (5th Cir. 2001)).

[232] See Graph 4.

[233] *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.15.

[234] Cf. *U.S. v. Daly*, 535 F.2d 434 (442).

[235] *U.S. v. Padilla-Pena*, 129 F.3d 457 (8th Cir. 1997).

the government to make reasonable efforts to provide for simultaneous translation, "non-simultaneous minimization is acceptable if done as soon as practicable after interception" where simultaneous interpreters are not easily available.[236]

III. Exceptions from the General Prohibition of Warrantless Surveillance

§ 2511(2)(a) provides that "except as otherwise specifically provided in this chapter any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication shall be punished … .", unless there is an authorization by a warrant that has been issued in accordance with § 2516 and § 2518. There are several situations, however, which involve actual interception but do not require a warrant, either because the communications do not fall within the scope of the definition provided for in *Title III* or because the law provides an exception.

1. Plain Hearing

The term "interception" referred to in § 2510(2) and § 2511(2)(a) is defined in § 2510(4).[237] With regard to oral communications, this definition clearly excludes unaided overhearing, i. e., overhearing without the aid of an electronic, mechanical, or other device as defined in § 2510(5).[238] Therefore, the U.S. courts developed the "plain hearing" doctrine according to which "the intrusion of a human ear …is not an unlawful 'seizure' of a conversation in a hotel or motel room."[239] No search occurred when a police officer listened to a person talking into a telephone on the street[240] or

[236] *United States v. Gambino*, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990). See also *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.16; *Hyatt*, Vanderbilt L. Rev. 64 (2011), 1347, 1349.

[237] See Section 2. b), Chapter II, Part I.

[238] 18 U.S.C. § 2510(5): "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than – (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal."

[239] *U.S. v. Mankani*, 738 F.2d 538, 544 – 545 (2d Cir. 1984).

[240] *U.S. v. McLeod*, 493 F.2d 1186, 1188 (7th Cir. 1974).

outside the defendant's apartment door[241]. A Federal Court of Appeals further held that police officers may carry out investigations "in a place where they had a right to be and they were relying upon their naked ears".[242]

2. Consent to Surveillance under *Title III*

Consent to surveillance is provided for in § 2511(2)(c) as an exception to the general prohibition of warrantless surveillance.[243] Consensual surveillance can be accomplished in several ways: (1) A party to a conversation may himself record the conversation; (2) A party to a conversation may use or even wear a concealed electronic device to transmit the conversation to a non-party; or (3) A party to a conversation may consent to the use of an electronic device by a non-party to overhear the conversation.[244] The "party" and "non-party" can be law enforcement officers or informants. In the case of consensual surveillance, the conversation can be recorded without the need of a warrant and without the consent of other parties to the conversation. Consent can be express or merely implied.[245] The same outcome would be achieved if consensual surveillance were examined under the *Katz* test. A person cannot have a reasonable expectation of privacy if he allows others to participate who have no obligation to keep the conversation secret. Senate Report 1097 also stated that the consent exception "largely reflects existing law"[246] by referring to *Lopez*[247] and *On Lee*[248]. The practical meaning of the consent to surveillance, as an exception to a warrant requirement, is mainly to simplify the work of undercover agents and informants because it enables them to record or transmit the conversation in which they are engaged without a warrant.[249] This rule was first developed by courts and then adopted in § 2511(2)(c) of *Title III*, and is regarded as the principal exception to the warrant requirement.[250]

---

[241] *United States v. Llanes*, 398 F.2d 880 (2d Cir. 1968).

[242] *United States v. Fisch*, 474 F.2d 1071, 1076 (9th Cir 1973).

[243] § 2511(2)(c) provides: "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." § 2511(2)(d) concerns the private parties.

[244] S.Rep. No. 1097, 2236.

[245] S.Rep. No. 1097, 2182.

[246] S.Rep. No. 1097, 2182.

[247] *Lopez v. United States*, 373 U.S. 427 (1963).

[248] *On Lee v. United States*, 343 U.S. 747 (1952).

[249] 18 U.S. Code § 2511(2)(c) uses the term "acting under color of law". It means to "act under the direction of or on behalf of a law enforcement officer when conducting consent overhearing or interception". The private persons who give the consent to the law enforcement and who record for the law enforcement for an investigatory purpose should be deemed as "acting under color of law". See *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.54.

[250] *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.51.

Previously, when the trespass doctrine was still the controlling principle, the U.S. Supreme Court had ruled in *On Lee v. United States*[251] that it was not an unlawful search and seizure for an agent to record an incriminating conversation with a hidden microphone after he had obtained consent to enter the building.[252] Similarly, in *Lopez v. United States*,[253] when an undercover agent had secretly carried a recording device, the Court, following the ruling made in *On Lee*, concluded that no "eavesdropping" had occurred, since the agent had not recorded any communication that he could not otherwise have heard; the recording device had served only the purpose of collecting reliable evidence. Moreover, the agent was a party to the conversation and therefore no unlawful trespass was committed.[254]

The *Katz* decision cast some doubt on this case law until *United States v. White*[255] confirmed it. In *White*, a government informant conducted various conversations with the defendant in a restaurant, the defendant's home and the informant's car while he was secretly carrying a warrantless radio transmitter.[256] The situation was very similar to the two cases referred to above, but the extent of the recording was far greater. Justice White, writing the opinion of the Court, stated that the defendant's expectation of privacy during such conversations could not pass the two-pronged test proposed in *Katz*.[257] From a subjective perspective, "one contemplating illegal activities must realize and risk that his companions may be reporting to the police"; and from an objective perspective, society does not recognize significant differences "between the electronically equipped and the unequipped agent".[258] This rationale indicates that wherever "plain hearing" occurs, the undercover agent or informant is entitled to recording what he can hear with his naked ear. Moreover, the majority

[251] *On Lee v. United States*, 343 U.S. 747(1952).

[252] This decision was a 5–4 decision, with 4 separate dissenting opinions. *On Lee v. United States*, 343 U.S. 747 (1952). See also *LaFave*, Search and Seizure, 2020, § 2.2(f), Fn. 308 and companying texts.

[253] *Lopez v. United States*, 373 U.S. 427(1963).

[254] *Id.* at 437–40.

[255] *United States v. White*, 401 U.S. 745 (1971).

[256] *Id.* at 748–54.

[257] *Id.* at 749 ("… however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities.") Moreover, even the defendant got a promise of confidentiality or anonymity from the undercover agent may not suffice to create a justified expectation of privacy. See *People v. Maury*, 30 Cal. 4th 342 (2003).

[258] *Id.* at 752–53 ("At least there is no persuasive evidence that the difference in this respect between the electronically equipped and the unequipped agent is substantial enough to require discrete constitutional recognition, particularly under the Fourth Amendment which is ruled by fluid concepts of 'reasonableness'.").

opinion emphasized that such recordings enable officers to obtain reliable evidence.[259]

Another way for the undercover agent to hide a recording device or transmitter is to install the equipment at a certain place without a warrant. In *United States v. Yonn*, the court decided that the "location of the electrical equipment does not alter the irrefutable fact that Yonn had no justified expectation of privacy in his conversation with" the informant.[260] The device had been installed in a room which the informant subsequently rented to the defendant and the device was only activated when the informant was also in the room. The ruling in *United States v. Lee*[261] followed this rationale and further listed three standards which need to be fulfilled if a recording device is installed in a certain place without a warrant. i. e., first, the entry to install the device must not be an illegal trespass[262]; second, "the cooperating individual" must be present when the device is functioning;[263] and third, the recording device should only be able to collect evidence that the cooperating individuals could also "have heard or seen while in the room".[264]

Consent to surveillance can be given even in one's own home without a prior search warrant.[265] The consent to surveillance via wire communications follows the rules described above.

[259] *Id.* at 753 ("Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable. An electronic recording will many times produce a more reliable rendition of what a defendant has said than will the unaided memory of a police agent. It may also be that with the recording in existence it is less likely that the informant will change his mind, less chance that threat or injury will suppress unfavorable evidence and less chance that cross-examination will confound the testimony.").

[260] *United States v. Yonn*, 702 F.2d 1341 (11th Cir. 1983).

[261] *United States v. Lee*, 359 F.3d 194 (3d Cir. 2004).

[262] *Id.* at 203 ("monitoring devices were installed in the suite's living room at a time when Lee had no expectation of privacy in the premises.").

[263] *Ibid.* ("no evidence that conversations were monitored when [government informer] Beavers was absent from the room, and Beavers was plainly there at the time of the incriminating meetings shown on the tapes that were introduced at Lee's trial.").

[264] *Id.* at 202 ("First, if the defendant had an expectation of privacy in the premises at the time when the device was installed, the entry to install the device would constitute a search. Second, the cases involving consensual monitoring do not apply if recordings are made when the cooperating individual is not present. Third, the logic of those cases is likewise inapplicable if the placement of the recording device permits it to pick up evidence that the cooperating individual could not have heard or seen while in the room. Unless one of these circumstances is present, however, it does not matter for Fourth Amendment purposes whether the device is placed in the room or carried on the person of the cooperating individual. In either event, the recording will not gather any evidence other than that about which the cooperating witness could have testified.").

[265] See *United States v. White*, 401 U.S. 745 (1971) (Four conversations took place in the informant's home, two in the informant's car, one in a restaurant, and one in defendant's home.) and *U.S. v. Scarborough*, 43 F.3d 1021, 1025 (6th Cir. 1994) and *U.S. v. Eschweiler*, 745 F.2d 435, 437 (7th Cir. 1984). Meanwhile, some states do not permit warrantless consent surveillance in private homes. See *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.55.

In the consent to surveillance situation, the courts make a clear distinction between devices with a simple recording function and those with sense-enhancing functions, by stating that only the evidence that the consenting party can also hear with his naked ear is admissible without a warrant.[266]

In sum, warrantless consent to surveillance only needs to meet two requirements, i. e., consent must be given by one party to the conversation and the recorded/transmitted conversation must be limited to what can be heard with the naked ear. This rule encourages undercover agents and informants to behave like good "actors" in order to gain the trust of the suspect so that they will make incriminating statements. In this way, a large percentage of surveillance takes place outside of judicial control. There is a risk that undercover agents and informants will abuse this rule to record irrelevant conversations or to record material completely at random.

In addition, there is a paradox at work in this case law. Under the two-pronged test in *Katz*, if a person tells something to another person, this person does not expect to keep this conversation private, because the other parties to the conversation are not obliged to keep it secret. His expectation of privacy with regard to such a conversation therefore cannot be recognized as "reasonable". According to *United States v. White*,[267] a person accepts the risk of incrimination and loses the expectation of privacy when they pass information on to others. Once the information is exposed to any third party, this piece of information is regarded as being exposed to the public.[268] Under this argument, no conversation, only thoughts that are not spoken, enjoy an expectation of privacy. Yet, one can argue that a person has no expectation that the other party to the conversation will keep it confidential but can expect the conversation to remain private among the partner and himself. Since the person, however, cannot prohibit other parties from recording and handing over this material to anyone else, including to the police, this person also loses his expectation of privacy against anyone else. Under this logic, there is no significant difference between those who are party to the conversation and those who are not; both groups can record the conversation. It means that even the police can make recordings without a warrant or the consent of any party in the conversation because the parties have already lost their expectation of privacy, simply by speaking. Obviously, this scenario contradicts the statute and the *Katz* ruling.

[266] *United States v. Llanes*, 398 F.2d 880, 884 (2d Cir. 1968), and *United States v. Agapito*, 620 F.2d 324, 330 and Fn. 7 (2d Cir. 1980).

[267] *United States v. White*, 401 U.S. 745 (1971).

[268] For example, *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. White*, 401 U.S. 745 (1971).

IV. Procedure

Title III requires that all interceptions must be authorized in advance by judicial warrant except in exigent circumstances. The primary purpose of the warrant system in *Title III* is to introduce judicial control over electronic surveillance and to guarantee that such practice is in compliance with the 4th Amendment.[269] The statutory system consists of substantive requirements for the authorization of surveillance (§ 2516) and the procedure and criteria for issuing a warrant (§ 2518).

1. Application Process for a Surveillance Warrant at the Federal Level

At the Federal level, before an application is submitted to a court, it must first be authorized by the Department of Justice. An internal review process is regarded as "a critical precondition to any judicial order."[270] It serves to accelerate the matter, to reduce the workload of the issuing court, and to contribute to a higher quality of the warrant. The success of this process relies on the centralization of the prosecution system at the Federal level. By contrast, at the state level, application authority is still in the hands of local prosecutors.[271]

a) Who can Make and Authorize an Application

§ 2516(1) imposes a centralized authorization system at the Federal level:[272] "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge…" for "an order authorizing or approving the interception of wire or oral communications".[273] Decisions regarding applications for an order are thus made in a single Federal office, i.e., the Office of the Attorney General. This system has a dual purpose, i.e., to impose uniform standards, which prevent different practices from taking place in different

[269] S.Rep. 1097, 2153; *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.3.

[270] *United States v. Giordano*, 416 U.S. 505, 515–16 (1974); see also *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.11.

[271] *National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance*, NWC report, 1976, 55.

[272] The Court expressly evaluated such system as a centralizing system in *United States v. Giordano*, 416 U.S. 505 (1974).

[273] More details can be found: *Shields*, American Law Reports, Fed.169 (2001), 169.

Federal districts, and to "establish lines of responsibility" which lead to a specific person.[274]

Besides the Office of the Attorney General, another important department in the authorization process is the Electronic Surveillance Unit (ESU) of the Criminal Division's Office of Enforcement Operations. ESU handles all requests pursuant to *Title III* regarding Federal surveillance submitted by law enforcement and assists "in the preparation of *Title III* applications and to answer questions on any Title III-related issue".[275] According to the U.S. Attorneys' Manual regarding electronic surveillance, ESU will conduct the initial review of all submitted application documents[276], which are either prepared by the prosecutor in charge of the case or by the agent investigating the case.[277] After a review by ESU, the whole package, including the memorandums, will be submitted to the Assistant Attorney General Office to await final authorization.[278] Although ESU has no final approval power over the application, it plays a coordinating role and assists the attorneys.

b) Exigent Circumstances

Whereas a judicial warrant is generally a requirement for any surveillance or interception, § 2518(7) of *Title III* allows for warrantless interception in exigent circumstances. Law enforcement officers may conduct an interception without prior judicial approval if they reasonably determine that there exist exigent circumstances and grounds "upon which an order could be entered under this chapter (Chapter 119) to authorize" such conduct.[279] The scope of an "emergency situation" is defined in § 2518(7)(a): "An emergency situation exists that involves (i) immediate danger of

[274] S.Rep. 1097, 2185. NWC Report, 1976, 55. With this pressure, a responsible determination can also be guaranteed. *Cf. U.S. v. Vogt*, 760 F.2d 206 (8th Cir. 1985).

[275] Electronic Surveillance Manual, p. 1, 2005, https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf, visited at 22.4.2021.

[276] U.S. Attorneys' Manual, Section 9–7.110. https://www.justice.gov/usam/usam-9-7000-electronic-surveillance, visited at 22.4.2021. The documents reviewed by ESU consist of: (1) The affidavit of the agent of the United States who is in charge of the investigation of the case for which the electronic surveillance method might be needed; (ibid.) (2) the application by any United States Attorney or his/her Assistant which should demonstrate "the probable cause exhaustion of alternative methods of investigation, and results of any prior surveillance"; (NWC Report, at 55. Such application can be prepared by the attorney in charge of the case or directly by the agent investigating the case, or through their cooperation.) (3) the proposed order which needs to be signed later by the court to make it valid; (ibid.) (4) A completed *Title III* cover sheet with "the signature of a supervising attorney who reviewed and approved the *Title III* papers". (Ibid. The supervising attorney in this situation is the Assistant United States Attorney, he or she needs to review all the documents in case that they are prepared by the attorney working for them and then signs the *Title III* cover sheet.)

[277] NWC Report, at 55. Merely drafting of application materials is likely to take several days. *Fishman*, Georgia L. Rev. 22 (1987), 1, 42.

[278] NWC Report, 1976, 2–3.

[279] 18 U.S.C. § 2518(7).

death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime".[280]

The Senate Committee explained that the intended scope of § 2518(7)(a)(i) relates to any situation involving imminent danger to life, namely, a situation involving the taking of a hostage, the kidnapping of a victim, or the planning of an execution, or similar situations which involve a serious and imminent threat to life. Moreover, the use of electronic surveillance would prioritize the prevention of serious injury or death over the collection of evidence.[281] In addition, exigent surveillance is not authorized merely to gather evidence of criminal activity,[282] for instance, if surveillance is conducted when a prisoner is suspected of agreeing to kill a prosecution witness.[283]

The Senate Report 1097 on *Title III* regarded the "exigent circumstances" provision as an important tool in fighting organized crime and further explained what might constitute "exigent circumstances": "Often in criminal investigations a meeting will be set up and the place finally chosen almost simultaneously. Requiring a court order in these situations would be tantamount to failing to authorize the surveillance."[284] This Report sought to establish the constitutionality of this provision by drawing an analogy to other emergency searches that were recognized by the courts.[285] Due to the vague language of § 2518(7)(a)(iii), however, the organized crime clause has rarely been invoked.[286]

Using "exigent circumstances" as an exception works differently from consent to surveillance because the former still requires a warrant at a later stage, while the latter is totally exempt from the warrant requirement. This means that exigent circumstances can only be considered if there is probable cause to believe that a warrant could be issued at the time of surveillance. The application for a warrant in such a situation can be postponed for forty-eight hours "after the interception has occurred or begins to occur".[287] The courts also require that the situation must be sufficiently exigent. Various features may be taken into consideration, for example, the gravity of the crime under investigation; the amount of time needed to obtain a warrant;

[280] The original proposal for § 2518(7)(a) had referred to all the offenses provided in§ 2516(1). See 114 Cong. Rec. 14745(1968). Since the definition of "organized crime" is not given in *Title III*, however, it is still possible to interpret this term to include nearly all offenses under§ 2516(1) and even offenses not referred in§ 2516(1). See *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.75.

[281] S.Rep. No. 225, 98th Cong., 2d SeS. 396, reprinted in 1984 U.S. Code Cong. & Admin. News 3182, 3535.

[282] *Fishman*, Georgia L. Rev. 22 (1987), 1, 46.

[283] NWC report, 1976, 111.

[284] S.Rep. 1097, 2193.

[285] S.Rep. 1097, 2193.

[286] *Fishman*, Georgia L. Rev. 22 (1987), 1, 39, Fn. 172.

[287] 18 U.S.C. § 2518(7).

whether the exigency was unnecessarily triggered by law enforcement; and whether law enforcement agents attempted to obtain a warrant at the earliest opportunity.[288]

Although the Justice Department, in order to reduce the controversial aspects of *Title III*, has used exigent surveillance sparingly, there are several objections to the "exigent circumstances" provision, based on the concern that it might lead to an abuse of power.[289] Some opponents argue that this provision could give too much power to local prosecutors to conduct surveillance without a judicial warrant.[290] Some fear that exigent surveillance could be covered up, in order to avoid any potential suits brought by target persons, when no useful information was obtained, since no one else is aware of the activity.[291] This issue is extremely serious if authority to conduct an interception is given to all members of a specific unit with a general designation. In order to reduce the potential abuse of § 2518(7), it has been suggested that the designation should only be given to one specific officer in each specific case[292] and that prior notice should be given to the judicial department – it might only take the form of a short informal telephone call – to ensure that an ex post facto application will be made and also in order to protect the individual agent from potential lawsuits.[293]

c) Crimes that Can be Investigated by Intercepting Communications

§ 2516 adopts different standards for the surveillance of wire and oral communications on one hand and electronic communications on the other. Fewer crimes can be investigated by intercepting wire or oral communications than electronic communications. The latter can be intercepted during the investigation of any Federal felony.[294]

The Federal crimes that can be investigated by means of authorized wiretapping and bugging are enumerated in § 2516(1) in no particular logical order.[295] Taking § 2518(7)(a) into consideration, these crimes can be divided into three categories:

[288] *Fishman*, Georgia L. Rev. 22 (1987), 1, 18 – 19.

[289] NWC Report, 1976, 111 – 112. The opposite opinion criticized this provision as an encouragement to the random interception. *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.69.

[290] NWC Report, 1976, 112.

[291] *Ibid.* See also *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.71.

[292] *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.75.

[293] NWC Report, at 18 ("Section 2518 should be amended to require the oral notification of a judge prior to installation of an emergency electronic surveillance, the notification to be followed as soon as practicable, but within a limited period of time, by a formal application for judicial approval of the surveillance.") And see also *Carr* et al., The Law of Electronic Surveillance, 2020, § 3.77.

[294] § 2516(3) ("… when such interception may provide or has provided evidence of any Federal felony.").

[295] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.3.

crimes threatening national security, crimes resulting in death or serious injury to persons, and activities characteristic of organized crime.[296] The first category consists of the crimes relating to atomic and nuclear energy and other serious crimes, such as espionage or the sabotage of military facilities, listed in Title 18 of the U.S. Code. The second category involves crimes targeting the life and property interests of individuals, such as murder, kidnapping and robbery.[297] The third category covers the largest number of crimes, which are mostly provided for in § 2516(1)(c) - (s),[298] such as narcotic offenses,[299] gambling,[300] and hijacking.[301] These crimes are frequently committed by organized crime because they require a large network of persons.

According to the Wiretap Reports made by the Administrative Office of the U.S. Courts on behalf of the Federal Judiciary, drug offenses are the prevalent type of criminal offenses investigated by means of electronic surveillance, in the U.S. as a whole and at the Federal level. For instance, 46 % of all applications for intercepts in the whole of the U.S. (1,354 wiretap applications) in 2018 cited narcotics crime as the most serious offense under investigation. Applications citing narcotics, combined with applications citing other offenses, which include other offenses related to drugs, accounted for 77 % of all reported wiretap applications in 2018.[302]

The approach of enumerating crimes adopted by § 2516(1) in order to restrict the use of interception techniques has met with criticism. Many argue that the categorization of crimes is too broad and that some more unusual crimes cannot be "identified by the name of the crime it represents."[303]

d) The Contents of an Application

§ 2518(1) regulates the information that should be included in an application for an order authorizing or approving the interception of a wire, oral, or electronic communication under *Title III*. The information can be divided into two categories.

---

[296] *Ibid.*

[297] The crimes in these first two categories can also have the characteristics of organized crime, according to how they were committed. The three categories do not exclude one another.

[298] The crime relating biological weapons listed in § 2516(1)(a) also shares the characteristics of organized crime. *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.6.

[299] 18 U.S.C.A. § 844(d) to (i) (1982).

[300] 18 U.S.C.A. §§ 1084, 1955 (1982).

[301] 18 U.S.C.A. § 659 (1982).

[302] Many applications referred to multiple criminal offenses under investigation but the statistics cited here include only the most serious criminal offenses, listed on an application. Statistic resource: https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 15.05.2020. See also Graph 5.

[303] *Uviller*, NWC Commission Hearings, June 10, 1975. The suggestion was to reduce the number of crimes and establish criteria according to the seriousness of particular crimes. NWC Report, 1976, 45.

The first category includes a requirement that also applies to conventional search warrants, namely, a statement of probable cause for the suspected criminal activity, i. e., "a full and complete statement of the facts and circumstances" to justify the application.[304] The probable cause statement is the most substantial part of an application. In accordance with § 2518(1)(b)(i)-(iv), four pieces of information should be included: a description of the offense; the nature and location of the facilities or the place where the interception is to be conducted; the type of communication to be intercepted; and the identity of the target persons.[305] All of this information should be supported by sufficient evidence, otherwise the application will be denied by the courts.[306]

The second category includes unique information required for an electronic surveillance order,[307] i. e., "the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application" which can be indicated by the series of signatures made during the authorization process described above;[308] "a statement concerning the inadequacy of investigative alternatives"[309] to ensure that surveillance will only serve as the last resort for criminal investigation; the suggested period of time for the interception;[310] facts about any previous related application;[311] and a report on the outcome of previous applications for an extension of an order.[312]

---

[304] § 2518(1)(b). Some information required by the probable cause statement for an electronic surveillance is also unique, for example, the type of communication intercepted should be described in the statement. § 2518(1)(b)(iii).

[305] § 2518(1)(b) and *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.22.

[306] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.22.

[307] NWC Report, 1976, 62.

[308] § 2518(1)(a) ("a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted.").

[309] § 2518(1)(c) ("a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous".) and NWC Report, 1976, 62.

[310] § 251(1)(d) ("a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.").

[311] § 2518(1)(e) ("a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application.").

Preparation of this information in accordance with *Title III* plays an essential role in the investigation, which has been described as "the apex of an inverted pyramid".[313] Drafting an application is likely to take several days. If the defense lawyer claims that the evidence in the application is insufficient or incorrect, and the court agrees, all evidence collected by the interception can be excluded.[314]

e) Review Criteria

Four criteria will be considered by officers involved in the internal review process: the compliance of the application with the Constitution and *Title III*; the necessity for conducting the requested electronic surveillance; the ability of the technology to provide the desired results; and the cost of conducting the proposed surveillance.[315]

aa) Legality and Necessity

Applications must contain all elements required by § 2518(1).[316] Moreover, given the intrusive character of interception and the requirement of § 2518(1)(c), officers must consider all facts and circumstances when deciding whether it is necessary to use electronic surveillance[317]and whether the seriousness of the offense justifies the intrusion into privacy.

bb) Effectiveness of the Technology

Law enforcement officers must consider the effectiveness of the technology to achieve the desired results,[318] including the feasibility of installing a device and the possible negative consequences if the surveillance technology is discovered by the targeted person.

---

[312] § 2518(1)(f) ("where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.").

[313] NWC Report, 1976, 62.

[314] See Section 4. c) aa), Chapter V, Part I.

[315] NWC Report, 1976, 56–58.

[316] The constitutionality of § 2518 has been already approved by the courts, therefore, the constitutionality of the application will not be examined separately.

[317] NWC Report, 1976, 57. More discussion on last resort can be found in Section 2. b) cc), Chapter IV, Part I.

[318] *United States National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance*, Strategy and Tactics in the Prosecution and Defense of Complex Wire-Interception Cases, 1976, 33 ("No choice for wire interception ought to be made without full assurance that a sufficient technical basis exists upon which properly to conduct the tap and to convert its fruits into usable trial evidence.").

cc) Cost

Electronic surveillance is very expensive, time-consuming,[319] and demands a large amount of human resources,[320] especially if the surveillance is conducted over a longer period of time. According to the Wiretap Report 2018 the average cost of an installed warrant in 2018 was $67,926.[321] The cost of surveillance can vary according to the offense; for instance, the investigation of narcotics offenses usually costs more than the investigation of gambling offenses.[322]

Such high cost and the demand on human resources can deter "too frequent and lengthy eavesdropping".[323] Limited budgets and manpower can only support a limited number of interceptions at any given time. Consequently, officers have to be very selective when choosing which cases to pursue, even among offenses that fulfil all criteria for an interception.[324]

In practice, the higher hierarchy level frequently exerts an influence over decision-making in the centralized Federal system. If higher-ranking officers, i. e., reviewers in the Attorney General's Office, are supportive of *Title III* surveillance, lower-ranking officers will be encouraged to initiate applications more frequently.[325]

2. The Warrant

a) Jurisdiction

Under § 2516(1), "a Federal judge of competent jurisdiction", that is "a judge of a United States district court or a United States court of appeals" (§ 2510(9)(a)), has jurisdiction to approve an application made under *Title III*. The findings and determinations to be made by the judge are described in § 2518(3), which in a large degree reflects the contents of § 2518(1).

---

[319] *Ibid.*

[320] *Cleveland*, NWC Commission Hearings, May 20, 1975, commented the *Title III* surveillance as "manpower killers". Moreover, some surveillances, such as for gambling, have to be conducted during the night which are also a heavy burden to the law enforcements. See NWC Report, 1976, 57.

[321] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 15. 05. 2020.

[322] NWC Report, 1976, 58.

[323] *Ibid.*

[324] *Kotoske*, NWC Commission Hearings, May 21, 1975. The empirical analysis in Section 6, Chapter VI, Part I also supports this conclusion.

[325] NWC Report, 1976, 56.

b) Findings and Determinations

The 4th Amendment requires that "…no warrants shall issue, but upon probable cause…". If a warrant does not have probable cause, the search or surveillance will be regarded as unreasonable. The requirements of probable cause for different types of warrants are similar but not identical.[326] For example, before a conventional search warrant is issued, there must be probable cause to believe that the proposed item has a connection with criminal activity and that the item can probably be found in a certain place. It is not necessary, however, to name a person, the place and items are sufficient. In an arrest warrant, by contrast, the identity of a person and the crime he is suspected of must be named.

A general principle of the probable cause test has been established in *Camara v. Municipal Court*,[327] where the U.S. Supreme Court required that probable cause should balance "the need to search against the invasion which the search entails"[328] in each case. Since electronic surveillance has an "unusual degree of intrusiveness"[329], "only a most precise and rigorous standard of probable cause may justify an intrusion of this sort."[330] Thus, the probable cause for such a warrant includes not only the requirements of conventional search and arrest warrants, i.e., the identity of the involved person and alleged crimes (§ 2518(3)(a)),[331] the particular communications concerning the crime,[332] and the facilities or places (§ 2518(3)(d))[333]; but also "the last resort" requirement of interception relative to other investigative methods.[334]

When judges review applications, they may ask for more evidence to support the application.[335] During the judicial review process, formal and informal discussions among judges, prosecutors and law enforcement officers are frequently held.[336] Judges must check whether all materials required by § 2518(1) have been submitted.

[326] *LaFave* et al., Criminal Procedure, 2020, § 3.3(a).

[327] *Camara v. Municipal Court of the City and County of San Francisco*, 387 U.S. 523 (1967).

[328] *Id.* at 537.

[329] *LaFave* et al., Criminal Procedure, 2020, § 3.3(b).

[330] *Berger v. New York*, 388 U.S. 41, 69 (1967).

[331] § 2518(3)(a) ("there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter").

[332] § 2518(3)(b) ("there is probable cause for belief that particular communications concerning that offense will be obtained through such interception").

[333] § 2518(3)(d) ("There is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.").

[334] NWC Report, 1976, 77.

[335] § 2518(2): "The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application."

[336] NWC Report, 1976, 75.

They then must decide independently whether probable cause is sufficient to issue the order.[337] § 2518(3) reflects to a large degree the contents of § 2518(1) and provides a list of what findings and determinations need to be made by judges.

aa) Probable Cause

The "probable cause" requirement consists of two elements: the identity of the persons to be intercepted and the description of the offense, which reflects the contents of § 2518(1)(b)(i) and (iv).

Although the 4th Amendment does not require the identification of a person in a conventional search warrant, the U.S. Supreme Court ruled that "a wiretap application must name an individual if the Government … expects to intercept the individual's conversations over the target telephone."[338] Probable cause here only requires the identification of one or several "principal target(s)", not of all speakers who might be involved in the communications.[339] This also makes it possible for law enforcement officers to identify unknown suspects or offenses through intercepting suspects already known to them.[340] This practice is sometimes called "the primary benefit of eavesdropping"[341] or "strategic intelligence surveillance".[342] Such interception can result in a serious invasion of privacy because it is usually conducted without a specific focus and all the person's communications will be recorded.

The requirement of a description of a particular offense attempts to limit such invasion and requires that suspicion of a particular offense is the precondition, instead of the outcome, of obtaining a warrant.[343] In order to meet this requirement, probable cause must be supported by certain facts,[344] information or clues that are obtained from direct observation, testimony of informants or undercover agents, etc.[345] For instance, a court rejected an application for a search warrant that only included a statement made by an informant about criminal activity and stated that in order to meet the standard of probable cause, underlying information from which the in-

[337] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.70.

[338] *U.S. v. Donovan*, 429 U.S. 413, 428 (1977).

[339] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.36

[340] Such practice was used by law enforcements in New York in order to figure out to whom the principal members of a criminal organization was talking to and what illegal business they were doing. Such actions were prohibited in 1970. NWC Report, 1976, 63.

[341] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.36.

[342] NWC Report, 1976, 63.

[343] *Ibid.*

[344] *Gibson v. State*, 758 So.2d 782 (La. 2000) (However, at this stage, the probable cause "does not require the police to have direct, physical evidence.").

[345] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.23.

formant reached his conclusion would also have to be submitted.[346] Although this case was not about a surveillance warrant, the reasoning is applicable here too.

bb) Specific Communications to be Intercepted

§ 2518(3)(b) requires a precise description of the type of communication that is sought to be intercepted (§ 2518(1)(b)(iii)). Communications are subject to a *Title III* order, just like the item to be seized in a conventional search warrant. This requires that the communication to be intercepted should be specified and particularized in order to prevent random interception. This does not, however, provide clear guidelines for good practice. On the one hand, an insufficient description of particularity can fail the minimization requirement prescribed in § 2518(5) because the interception cannot be minimized unless the communications to be intercepted are defined clearly.[347] On the other hand, the communications are yet to occur and no one can precisely predict what they will be about.[348] On the basis of past judicial practice, it is sufficient that the warrant refers to the type of offense that the communications will refer to[349] and specific information, e. g., the identities of co-perpetrators or the exact time of the offense.[350]

cc) Inadequacy of Investigatory Alternatives

Judges need to determine probable cause on the basis of the information submitted by officers under § 2518(1)(c) if all other investigative alternatives are inadequate. This implies that surveillance is not allowed if "traditional investigative techniques would suffice to expose the crime."[351] Judges can invoke § 2518(2)[352] to ask for more details from applicants, or can discuss with applicants the possible alternatives.[353] The inadequacy of other investigative measures includes three situations in accordance with § 2518(1)(c): (1) other measures have been tried but failed; (2) other

[346] *Aguilar v. Texas*, 378 U.S. 108, 114 (1964) ("the magistrate must be informed of some of the underlying circumstances from which the informant concluded that the narcotics were where he claimed they were, and some of the underlying circumstances from which the officer concluded that the informant, whose identity need not be disclosed, was 'credible' or his information 'reliable'.") (Citation omitted).

[347] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.30.

[348] *Ibid.*; NWC Report, 1976, 65.

[349] *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.31.

[350] *Id.* § 4.30 (quoting from *U.S. v. Savage*, 2013 WL 1334169, *11 (E.D. Pa. 2013) (Information about "discussions concerning the continuing conduct, financing, managing, supervising or directing of all or part of the illegal drug trafficking organization, which will reveal the identities of the participants of the organization")).

[351] *U.S. v. Kahn*, 415 U.S. 143, 153 and Fn. 12 (1974).

[352] § 2518(2) ("The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.").

[353] NWC Report, 1976, 67.

measures appear unlikely to succeed if they were tried; or (3) other measures are too dangerous.

(1) Failure or the Unlikely Success of Other Measures

"Common" investigative alternatives to be considered are the investigative grand jury, immunity grants, consent to surveillance, physical surveillance, informants, and search warrants.[354] Federal courts have held, however, that it is not necessary to exhaust all possible alternatives before a *Title III* order is issued.[355] The alternatives also need not have been totally unsuccessful. Results from other investigative activities can be used as probable cause for a *Title III* order, with the understanding that more information could be discovered via electronic surveillance. In this situation, the courts will review whether traditional investigative measures, such as physical surveillance,[356] are so ineffective that alternative measures must be taken.

The wide use of modern technology in communications, such as cell phones, makes some traditional investigative measures, such as physical surveillance, impractical. If it is likely that only limited information can be obtained from traditional measures, it is also possible to issue the surveillance order directly.[357]

(2) Dangers Arising from Other Measures

If the applicants can prove that other measures could expose individuals, including informants,[358] law enforcement officers,[359] witnesses,[360] or third persons,[361] to danger, the court should determine the existence of probable cause. Moreover, the risk of disclosing the ongoing investigation to the targets can also justify the adoption of electronic surveillance.[362]

---

[354] *Ibid.*; *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.46.

[355] *U.S. v. Ramirez-Encarnacion*, 291 F.3d 1219 (10th Cir. 2002); see also *Carr* et al., The Law of Electronic Surveillance, 2020, § 4.39.

[356] *Carr* et al., The Law of Electronic Surveillance, § 4.46.

[357] See *U.S. v. Blount*, 30 F. Supp. 2d 308, 311 (D. Conn. 1998) ("It (physical surveillance) can confirm a meeting, but not necessarily identify all participants. …. It does not record the words spoken nor can it eliminate lawful exchange of items, nor lawful receipt of money. It cannot be performed in all locations and is susceptible to detection when protracted. It is subject to counter-surveillance and is vulnerable when strangers in a location tarry long or appear repeatedly. Fixed surveillance is subject to dealers' mobility.").

[358] *Carr* et al., The Law of Electronic Surveillance, § 4.60.

[359] *Ibid.*

[360] *Ibid.*

[361] *Ibid.*

[362] The courts have ruled in several situations that conventional investigative techniques, such as informants, physical surveillance, trash searches, arrests, search warrants, "can potentially alert targets to the existence of the government's focus on them and their activities." *Ibid.*

(3) The Frustration of the "Last Resort" Requirement

In practice, however, neither applicants nor courts clearly distinguish among the three situations under § 2518(1)(c). They may only give a general declaration that other measures are "unlikely to succeed and, in certain circumstances, too dangerous to attempt…"[363] Such a vague declaration implies that this requirement is not taken seriously. In practice, no other measures need to be tried before a surveillance order is justified. Even an assumption can meet the requirements. In addition, since judges are hesitant to challenge law enforcement officers' experience concerning investigative issues, it is rare for judges to reject applications on the grounds that alternatives have not been exhausted. Therefore, the effectiveness of the last resort requirement is doubtful.

dd) Where Communications Can be Intercepted

The term "facilities" in § 2518(3)(d) refers to the particular telephones to be intercepted[364] and "places" means the locations where the communications will take place.[365] § 2518(4)(b) requires a surveillance warrant to specify "the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted". *Title III* does not provide in which way facilities and places should be specified. This depends upon the information that the officers have. For instance, the electronic serial number (ESN) is typically used to specify a cell phone.[366] Description of the house without specifying which room has been held to satisfy the requirement of specificity.[367] Errors in the description of facilities or places in the order can be tolerated as long as the remaining information still specifies the facilities or places to be intercepted.[368] Moreover, the language in § 2518(3)(d) emphasizes the substantial connection between the facilities or places in the application and the targets or the commission of the offense identified in § 2518(3)(1).

[363] For example, *U.S. v. Lawrence*, 2003 WL 22089778 (N.D. Ill.), 1 ("…traditional law enforcement techniques unlikely to succeed and, in certain circumstances, too dangerous to attempt. … The affidavits set forth the role that cooperating individuals, informants and undercover agents played in the investigation-and the limitations on the use of such investigative techniques. Thus, the affidavits satisfied the requirement of the statute.").

[364] *U.S. v. Tavarez*, 40 F.3d 1136, 1139 (10th Cir. 1994).

[365] Here "places" includes the body of a person. The court used to issue an order, which allowed law enforcement officers to hide a bugging device on a person's body without his consent. *Shell v. U.S.*, 2004 WL 1899013 (N.D. Ill. 2004) (The device was installed on a person who was visiting an inmate in prison.). *Carr* et al., The Law of Electronic Surveillance, § 4.25.

[366] *Carr* et al., The Law of Electronic Surveillance, § 4.75.

[367] *United States v. Lambert*, 771 F.2d 83, 91 (6th Cir. 1985).

[368] *United States v. Doolittle*, 507 F.2d 1368, 1371 (5th Cir. 1975).

ee) High Approval Rate of Applications

According to Table 1 in Chapter VI, Part I, from 2008 to 2018 U.S. judges rejected only 10 applications out of 34,794 (0.29 ‰). Several reasons can be suggested for this low rate: first, the internal review process by prosecutors works quite well to guarantee the quality of the applications they submit; second, issuing judges rely heavily upon and trust the materials submitted by law enforcement officers and thus do not review the applications extensively; third, the review standards of officers and judges are very similar (this is supported by *Title III*); fourth, there are informal communications between judges and law enforcement officers before applications are made and during judicial review.

c) The Contents of the Warrant (18 U.S. Code § 2518(4)-(6))

§ 2518(4)-(6) describes the contents of a surveillance order. The key part of an order are the findings and determinations of the issuing judge. Directives concerning the progress of the surveillance also have to be included. These directives instruct the law enforcement officers who are conducting the surveillance on how long the surveillance may last, when to terminate the surveillance, and how to conduct it. If these directives are ignored, the evidence obtained through surveillance can be excluded.

aa) The Duration Directive

A directive concerning the duration of the interception must be included in the order in accordance with § 2518(4)(e). It prescribes that an order must regulate "the period of time during which such interception is authorized", and § 2518(5) further limits this period of time to no "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days." The first alternative, i. e., that the interception should last no longer than necessary, is however, routinely ignored by applicants and judges. A 30-day order is always authorized in the U.S. and at the Federal level according to Table 3 and Table 4. Wiretap Reports show that it is quite common for interceptions to be terminated before the end of the authorized period (30 days).[369] The duration approved in the warrant can be extended under certain conditions.[370] In an extension warrant, a new duration directive is required, which normally authorizes another 30 days of surveillance (see Table 3 and Table 4).

[369] Statistic Source: https://www.uscourts.gov/statistics/table/wire-a1/wiretap/2018/12/31, visited at 16. 05. 2020.

[370] See Section 4, Chapter IV, Part I.

bb) The Termination Directive

The order shall also include a so-called "termination directive" indicating that the interception should be terminated "upon attainment of the authorized objective" under § 2518(5). This does not mean that the interception must be terminated after the first requested communication has been obtained.[371] The interception of further related communication is allowed as long as it is conducted within the valid period of a warrant. Law enforcement officers should terminate the interception when they think the evidence is sufficient for their purpose. Interception operations without extensions are more frequently terminated before the expiration of the order (30-day) than operations with extensions. The latter tend to continue until the extension has expired.[372]

cc) The Minimization Directive

§ 2518(5) requires that the order "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception". For a conventional search case, it is obvious that only items listed in the warrant can be searched and seized. In surveillance cases, however, since the contents of the intercepted communications are unpredictable, the interception of innocent conversations cannot be avoided entirely.[373] Therefore, § 2518(5) provides for a minimization requirement, which "instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations."[374] This requirement aims at preventing the potential abuse of power and at minimizing the amount of non-pertinent communication that is overheard. In this way, this provision is intended to confine the government's infringement upon privacy.[375]

According to one Federal Court of Appeals, "once the monitoring agent has had a reasonable opportunity to assess the nature of an intercepted communication, he or she must stop monitoring that communication if it does not appear relevant to the government's investigation."[376] Since *Title III* provides no further details on how to bring about minimization in practice, it is common that orders simply repeat the

[371] NWC Report, 1976, 82.

[372] Statistic Source: https://www.uscourts.gov/statistics/table/wire-a1/wiretap/2018/12/31, visited at 16.05.2020.

[373] *U.S. v. Bynum*, 485 F.2d 490, 500 (2d Cir. 1973) ("No electronic surveillance can be so conducted that innocent conversation can be totally eliminated."); similar with *U.S. v. Daly*, 535 F.2d 434, 442 (8th Cir. 1976).

[374] *Scott v. United States*, 436 U.S. 128, 139–140 (1978) ("The statute does not forbid the interception of all non relevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations.").

[375] *U.S. v. King*, 991 F. Supp. 77 (E.D. N.Y. 1998); see also *Lockhart*, American Law Reports, Federal 181 (2002), 419.

[376] *U.S. v. Mansoori*, 304 F.3d 635, 646 (7th Cir. 2002).

words of § 2518(5) as their minimization directive.[377] One warrant described the minimization directive in the following way: "If a conversation is minimized, monitoring agents shall spot check to ensure that the conversation has not turned to criminal matters."[378] Although "there is patently no mechanical, hard and fast formula applicable"[379] in case law, some criteria have been developed to determine whether the minimization directive has been fulfilled. In the *Bynum* case, the Court eliminated all calls of less than two minutes duration from its examination and regarded them as complying with the minimization requirement.[380] In addition, wide-ranging criminal activities can justify more extensive monitoring at an early stage.[381] The degree of judicial supervision during surveillance is also considered to be an important factor in determining whether law enforcement officers have attempted to minimize the interception in good faith.[382] For instance, the maintenance of monitoring logs can be upheld by the judge as being in compliance with the minimization requirement.[383] In a 1976 case,[384] the Federal Court of Appeals mentioned three factors. The first was "the scope of the criminal enterprise". More complicated or sophisticated conspiracies may justify more extensive interception than simple criminal activities.[385] The second factor was the Government's reasonable expectation as to the content of specific calls. This can depend on how much the Government knows about the identities of the suspects and their relationship to the conspiracies. If the monitor knows who is innocent, he can minimize the extent of the

[377] NWC Report, 1976, 82.

[378] *U.S. v. Goffer*, 756 F. Supp. 2d 588, 590 (S.D. N.Y. 2011).

[379] *Bynum*, 485 F.2d 490, 500 (2d Cir. 1973).

[380] *Ibid.* Other cases applied this 2-minute-regulation, e. g., *U.S. v. Daly*, 535 F.2d 434, 441 – 442 (8th Cir. 1976) ("spot-checking of such conversations is permissible especially in a case such as this involving a broad scope of criminal activity and a sophisticated criminal element."); *Drimal v. Tai*, 786 F.3d 219, 225 (2d Cir. 2015) (The reasonable minimization is generally justified whenever the monitoring of a call is less than 2 minutes, except some privilege communications where the law enforcement should figure out its privilege characteristic within seconds.); *U.S. v. Mansoori*, 304 F.3d 635, 647 – 48 (7th Cir. 2002).

[381] *Bynum*, 485 F.2d 490, 500 (2d Cir. 1973). See also See also *U.S. v. Bynum*, 360 F. Supp. 400, 410 (S.D. N.Y. 1973) (the court listed several factors to be considered when the court decided whether the effort of minimization has been made: "the type of criminal enterprise being investigated; the scope of that enterprise and the number of participants, known and unknown, involved therein; the number of days for which electronic surveillance is conducted; the scope of the authorizing order; the activity on the phone(s) being monitored; the number of calls; the number of monitored calls; the location of the phone(s); the length of calls; the participants in those calls; the content of calls as reasonably perceived at the time of the tap; the experience of the agents deployed for the investigation; the various pressures on the agents executing the investigation; the procedures planned and/or followed to monitor calls; the equipment employed in the surveillance; and, most of all, the supervision of the interception by the investigating agency, the supervising attorney, and by the authorizing Court.").

[382] *U.S. v. Bynum*, 485 F.2d 490, 501 (2d Cir. 1973).

[383] *Id.* at 502.

[384] *U.S. v. Daly*, 535 F.2d 434 (8th Cir. 1976).

[385] *Id.* at 441.

recording of this individual. This factor also means that when the monitors do not know who participated in the crimes and they wish to establish this, a more comprehensive monitoring may be justified.[386] The third factor was regular judicial supervision. [387] Furthermore, five elements were summarized by the Court of Appeal in *U.S. v. Yarbrough*[388] to decide whether law enforcement officers had made "an initial prima facie showing of reasonable minimization", namely,

> "(1) whether a large number of the calls are very short, one-time only, or in guarded or coded language; (2) the breadth of the investigation underlying the need for the wiretap; (3) whether the phone is public or private; and (4) whether the non-minimized calls occurred early in the surveillance. It is also appropriate to consider (5) the extent to which the authorizing judge supervised the ongoing wiretap."[389]

Moreover, "special instructions", "mid-search supervision" by the prosecutors and judges, and internal procedures followed by law enforcement officers have been approved by judges as sufficient methods with which to comply with the minimization directive.[390] Prosecutors can submit a statistical analysis of interception to show the percentage of communications which were pertinent to the investigation.[391]

The minimization requirement is more sensitive and demanding in the case of privileged communications between a husband and wife, or a client and his attorney.[392] One judge specifically instructed law enforcement officers that "you are to discontinue monitoring if you discover that you are intercepting a personal communication solely between husband and wife."[393] § 2517(4) of *Title III* provides that "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." This indicates that interception of privileged communications *per se* is not prohibited, if it is conducted in a way which meets the minimization requirement, but the content thereof is inadmissible in court.[394] The courts have, however, encouraged law enforcement officers to avoid intercepting such privileged communications. For instance, the court in *U.S. v. Lawrence*[395] approved of the

---

[386] *Id.* at 441.

[387] *Id.* at 442.

[388] *U.S. v. Yarbrough*, 527 F.3d 1092, 1098 (10th Cir. 2008).

[389] *United States v. Willis*, 890 F.2d 1099, 1102 (10th Cir. 1989).

[390] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.18.

[391] *Fishman/McKenna*, Wiretapping and Eavesdropping, 2019, § 35.64. An example of statistical report is showed.

[392] Here the communications between a husband and wife discussing criminal activities were no longer regarded as privilege communications. *U.S. v. Goffer*, 756 F. Supp. 2d 588, 591 (S.D. N.Y. 2011); *U.S. v. Harrelson*, C.A.5 (Tex.) 1985, 754 F.2d 1153.

[393] *U.S. v. Goffer*, 756 F. Supp. 2d 588, 591 (S.D.N.Y. 2011).

[394] NWC Report, 1976, 95. *U.S. v. Goffer*, 756 F. Supp. 2d 588, 593 (S.D. N.Y. 2011); *U.S. v. Malekzadeh*, 855 F.2d 1492 (11th Cir. 1988).

[395] *U.S. v. Lawrence*, 2003 WL 22089778,1.

practice that an agent should "turn off the monitor and stop recording"[396] if he hears privileged communication. If privileged communications were intercepted, the agent should "immediately notify the Supervising Agent"[397], who should then notify the authorizing court as soon as possible.[398] The court should then review the validity of the ongoing interception and make the necessary modifications to the order.

dd) The Progress Report System

As a form of judicial control over ongoing interceptions,[399] § 2518(6) introduced the progress report system.[400] Such a report system can effectively deter law enforcement agents from violating the minimization requirement[401] and give issuing judges an opportunity to terminate any illegal practice in a timely fashion. Moreover, it is suggested that judicial involvement makes "suppression more unlikely"[402] and thus can streamline and reduce the workload of law enforcement officers. From the wording of this provision, however, it can be assumed that it is not mandatory for reports to be submitted.[403] This has been criticized as a violation of the Constitution, and it was suggested that reports should be submitted for judicial control in every electronic surveillance case, as opposed to the current *ad hoc* system.[404] In order to eliminate arguments concerning constitutionality, the Justice Department adopted a regular reporting system that requires reports to be submitted every five days under a Federal surveillance order.[405] Reports shall include sufficient information for judicial review, for instance, a summary of the current findings and the total number of intercepted calls.[406]

---

[396] *Ibid.*

[397] *Ibid.*

[398] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.18; NWC Report, 1976, 95.

[399] For instance, such reports can be reviewed by the judge, as a way to decide if the minimization directive has been followed.

[400] § 2518(6): "the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require."

[401] See *U.S. v. Licavoli*, 604 F.2d 613 (9th Cir. 1979).

[402] NWC Report, at 96.

[403] See also NWC Report, at 84. In practice, some judges step back from reviewing the reports and rely on the prosecutor to do the supervision in order to preserve their neutral position in the trial.

[404] NWC Report, 1976, 96–97; *Lapidus*, NWC Commission Hearings, June 11, 1975.

[405] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.22; NWC Report, at 96.

[406] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.22.

3. The Role of Police and Prosecutors

Police officers are responsible for the implementation of a surveillance warrant.[407] Due to the minimization requirement, communication surveillance in the U.S. needs to be conducted live. That means that a police officer must be present while the recording is taking place in order to avoid recording non-pertinent conversations. At trial, this officer may be required to testify to the recording.[408] The police officers assigned to implement a warrant should also make reports and have an overview of the entire process of surveillance. Decisions on whether the warrant should be extended, or whether a new target or an additional location is to be added should be taken in a timely fashion. The police should also keep the prosecutor informed of all developments in the implementation of surveillance.[409]

Since the implementation is the responsibility of the police, prosecutors only offer administrative assistance, e. g., by way of communicating with the issuing judge, submitting reports as required by the warrant, helping the police comply with the warrant, and providing legal advice. Legal assistance can increase the likelihood of the admissibility of the evidence obtained through surveillance.[410] In addition, prosecutors should supervise the further development of the implementation of surveillance by reading police reports. For example, prosecutors can give instructions on strategies of minimization or consider whether the warrant should be modified. Prosecutors can also prompt the police to apply for an arrest or search warrant in a timely fashion.[411]

4. Extension of the Warrant

A warrant can be extended for "no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days" if a new application has been submitted under§ 2518(1) and the original issuing court makes findings under § 2518(3).[412] The application for an extension warrant must include "a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such re-

[407] *Fishman/Mckenna*, Wiretapping and Eavesdropping, 2019, § 14.1.

[408] *Ibid.*

[409] *Ibid.*

[410] *Id.* § 144.

[411] *Ibid.*

[412] § 2518(5) ("Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) (§ 2518(1)) of this section and the court making the findings required by subsection (3) (§ 2518(3)) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days.").

sults"[413]. It is important that this statement justifies the request for the extension. Therefore, such a statement must be written in a way that provides the judges with a full understanding of the implementation of the initial surveillance, which includes a comprehensive summary of the findings[414] or an explanation of why the surveillance was unsuccessful or not sufficient within the period of the original warrant. After receiving an application for an extension, the judge makes a ruling under § 2518(3), namely, whether the probable cause described in the initial application still exists, or whether there is new probable cause, for instance, if it is believed that more incriminating communications will occur in the future. Investigatory alternatives should also be evaluated again, especially if substantial evidence has already been obtained during the initial order and the court needs to decide whether these alternatives are still "unlikely to succeed if tried" or are considered "to be too dangerous".[415]

5. Sealing the Evidence

In accordance with § 2518(8)(a), all communications intercepted under the warrant shall, "if possible, be recorded on tape or wire or other comparable device" and "such recordings shall be made available to the judge issuing such order and sealed under his directions" "immediately upon the expiration of the period of the order, or extensions thereof."[416] This requirement aims at preventing law enforcement officers from editing the intercepted communications, in order to ensure "the reliability and integrity of evidence obtained by means of electronic surveillance".[417] Prosecutors have the responsibility to present the tapes to the issuing judge "immediately upon the expiration of the period of the order".[418]

[413] § 2518(1)(f).

[414] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.32.

[415] § 2518(3)(c).

[416] § 2518(8)(a) ("The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations.").

[417] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.34.

[418] *Fishman/Mckenna*, Wiretapping and Eavesdropping, 2019, § 14.2.

The sealing requirement is "a prerequisite for the use or disclosure" of evidence obtained through interception at trial.[419] The court can therefore exclude evidence on their own initiative if law enforcement officers delayed the delivery of the recording to the court for sealing.[420]

6. Giving Notice of Electronic Surveillance

§ 2518(8)(d) requires that "the persons named in the order or the application" as well as, at the judge's discretion, other intercepted parties are to be given notice "within a reasonable time but not later than ninety days after the filing of an application for an order of approval under § 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof". This requirement dates from the U.S. Supreme Court decision in *Berger*[421], where the lack of notification was held to be unconstitutional. Since individuals must be aware of the existence of surveillance in order to mount a legal response to it, it is necessary to notify the persons concerned of the existence of the surveillance, especially if an application has been denied or no evidence from the surveillance will be used at trial.[422]

§ 2518(8)(d) also requires that notice shall be given within a reasonable time, or within 90 days. This limitation enables the person to recall the contents of the intercepted communications.[423] A postponement after 90 days is allowed by the courts upon good cause[424]; requesting a postponement is not a rare practice.[425] It is rare, however, for the evidence to be suppressed on the grounds of an unauthorized delay exceeding the 90-day maximum period, since the court requires the defendant to demonstrate that he has been subjected to prejudicial treatment, which can be difficult to prove.[426]

---

[419] See § 2518(8)(a) ("The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.").

[420] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.34.

[421] *Berger v. New York*, 388 U.S. 41 (1967).

[422] In such situations, the service of notice is the only way to let the named persons be informed of the existence of the surveillance. To the contrary, the evidence from the surveillance can only be introduced in the trial, when the named persons "has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved" according to § 2518(9).

[423] NWC Report, 1976, 100.

[424] § 2518(8)(d) ("On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.").

[425] NWC Report, 1976, 100

[426] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.47.

V. Exclusionary Rule

Despite the 4th Amendment and *Title III*, it is not unusual for electronic surveillance to be misused by law enforcement officers. For instance, the NWC Report described a scandal involving the Special Investigations Unit of the New York Police Department, when a large number of its officers were charged with practicing illegal surveillance.[427] They had used technological surveillance as "standard practice" in order to obtain probable cause for arrest warrants and conventional search warrants.[428] Without a doubt, the exclusionary rule applies to evidence obtained from surveillance that violates the 4th Amendment and *Title III.* [429]

1. Origin and Purpose of the Exclusionary Rule

According to the exclusionary rule, "evidence seized illegally or obtained as a result of an illegal seizure by a government agent is not directly admissible in a criminal or quasi-criminal proceeding against a person whose expectation of privacy was violated by the illegal seizure."[430] This rule excludes both direct evidence obtained through an illegal search and indirect evidence derived from inadmissible evidence. The latter is also referred to as the "fruit of the poisonous tree".[431] Although this rule is currently one of the most important rules regarding criminal evidence, it existed neither in old common law, nor is it part of the 4th Amendment.[432] For instance, under old common law rules, if evidence was obtained by a search of a home without a warrant, defendants could bring a civil lawsuit or file a criminal complaint against the police officer. The fact that the evidence was obtained in an illegal way did not, however, influence its admissibility in the criminal process. Although law enforcement officers who carried out unconstitutional searches or seizures may have

[427] NWC Report, 1976, 163.

[428] *Ibid.*

[429] See also *LaFave* et al., Criminal Procedure, § 4.6(m).

[430] *C.D.T. v. State*, 653 N.E.2d 1041, 1044–1045 (Ind. App.1995).

[431] This will be discussed Section 3, Chapter V of this Part.

[432] *Burger*, American University L. Rev. 14 (1964), 1, 1 ("Unlike so many of our basic concepts of law this one (the Suppression Doctrine) has little or no linkage with the past in terms of either Roman Law, Napoleonic Law or even the Common Law of England."); *Price*, University of Miami L. Rev. 14 (1959), 57, 57; *Greenleaf*, A Treatise on the Law of Evidence, 12th ed., carefully rev., with large additions, by Isaac F. Redfield, LL.D., Little, Brown, and company 1866, § 254a ("It may be mentioned in this place, that though papers and other subjects of evidence may have been illegally taken from the possession of the party against whom they are offered, or otherwise unlawfully obtained, this is no valid objection to their admissibility, if they are pertinent to the issue. The court will not take notice how they were obtained, whether lawfully or unlawfully, nor will it form an issue, to determine that question."); see also Bishop Atterbury's Trial, 16 How. St. Tr. 323 (H. L. 1723), 495 (The way to get letters would not be considered), *Rosenzweig*, Cornell Law Quarterly 32 (1946–1947), 514, 515–516.

needed to pay compensation or face internal disciplinary procedures,[433] the old rule still placed defendants at a disadvantage due to the misconduct of the law enforcement officers, and the prosecution benefited from the police misconduct. Therefore, it has been argued that person-specific sanctions against misconduct are insufficient and ineffective in reducing such practices.[434] Given this background, an exclusionary rule was introduced to further deter illegal conduct by law enforcement officers and to remove the incentive to disregard the rights of suspects.[435] An exclusionary rule focuses on the legality of the method of obtaining evidence, not on the reliability of the evidence itself. In addition to serving as a deterrent, it has been argued that this rule achieves other purposes. For instance, *U.S.. v. Calandra* stated that this rule "is a judicially created remedy designed to safeguard Fourth Amendment rights"[436] and minimizes "the risk of seriously undermining popular trust in government"[437]. All purposes referred to above are closely interrelated.

The exclusionary rule can be traced back to the 1886 case of *Boyd v. United States*,[438] where the U.S. Supreme Court held certain papers to be inadmissible because they had been obtained in a way that violated the 4th and the 5th Amendments. In this case, a forfeiture proceeding had been initiated against the defendants, relating to certain goods that the prosecution alleged had been fraudulently imported without the payment of duty. The invoices for the goods were demanded and obtained by the government. The Court held that "a compulsory production of a party's private books and papers to be used against himself or his property in a criminal or penal proceeding, or for a forfeiture, is within the spirit and meaning of the [4th] Amendment". In this case, the Court equated the compulsory handing over of private papers with a search covered by the 4th Amendment.[439] The Court emphasized the relationship

[433] *Lippman*, Criminal Procedure, 2020, 385.

[434] *Ibid.*

[435] See *Elkins v. United States*, 364 U.S. 206, 217 (1960) ("The rule (the exclusionary rule) is calculated to prevent, not to repair. Its purpose is to deter – to compel respect for the constitutional guaranty in the only effective available way – by removing the incentive to disregard it."). The deterrence as the major purpose of the exclusionary rule is well recognized by the Courts who phrased this purpose in several cases. See also *Wolf v. Colorado*, 338 U.S. 25, 31 (1949) ("… the exclusion of evidence may be an effective way of deterring unreasonable searches…"); *Terry v. Ohio*, 392 U.S. 1, 12 (1968) ("Ever since its inception, the rule excluding evidence seized in violation of the Fourth Amendment has been recognized as a principal mode of discouraging lawless police conduct. Thus its major thrust is a deterrent one.") (*Citation omitted*).

[436] *U.S. v. Calandra*, 414 U.S. 338, 348 (1974).

[437] *Id.* at 357 (dissenting).

[438] *Boyd v. United States*, 116 U.S. 616 (1886).

[439] *Id.* at 616 and 622 (" It is our opinion, therefore, that a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution in all cases in which a search and seizure would be, because it is a material ingredient, and effects the sole object and purpose of search and seizure.").

between the 4th and the 5th Amendments[440] and held that "the seizure or compulsory production of a man's private papers to be used in evidence against him is equivalent to compelling him to be a witness against himself, …is equally within the prohibition of the Fifth Amendment."[441] By making reference to the 5th Amendment, the Court decided there was a violation of the 4th Amendment and that the illegally obtained papers should be excluded.

The next breakthrough came in 1914 in *Weeks v. U.S.*[442], where private papers were seized from a private dwelling without a search warrant. This time, the Court disregarded concerns about "self-incrimination", as in the *Boyd* case, and instead prioritized the need to send the correct signal to law enforcement officers that illegally obtained evidence would not be admitted at trial.[443] Since it was well established at that time that the Bill of Rights imposed restrictions only upon the Federal Government, the above precedents excluded evidence obtained through the illegal behavior only of Federal officers, not of state officers. This resulted in the so-called "silver-platter doctrine", which allowed evidence gathered illegally by state officers to be used in Federal trials.[444] In *Elkins v. United States*,[445] the Supreme Court for the first time excluded evidence seized by state police officers in violation of Federal constitutional standards from a Federal trial, thereby overruling the "silver-platter doctrine".[446] One year later, the Court in *Mapp v. Ohio*,[447] finally made this rule applicable to all state courts through the due process clause of the 14th Amendment.[448]

---

[440] *Id.* at 616 ("Both amendments relate to the personal security of the citizen. They nearly run into, and mutually throw light upon, each other. When the thing forbidden in the Fifth Amendment, namely, compelling a man to be a witness against himself, is the object of a search and seizure of his private papers, it is an 'unreasonable search and seizure' within the Fourth Amendment.").

[441] *Ibid.*

[442] *Weeks v. United States*, 232 U.S. 383 (1914).

[443] It is argued that this reasoning reflected also the deterrence theory but was not expressly stated. Ibid.

[444] *Lustig v. United States*, 338 U.S. 74, 79 (1949) ("it is not a search by a federal official if evidence secured by state authorities is turned over to the federal authorities on a silver platter.").

[445] *Elkins v. United States*, 364 U.S. 206 (1960).

[446] *Burger*, American University L. Rev. 14 (1964), 1, 7.

[447] *Mapp v. Ohio*, 367 U.S. 643 (1961).

[448] *Id.* at 660 ("Having once recognized that the right to privacy embodied in the Fourth Amendment is enforceable against the States, and that the right to be secure against rude invasions of privacy by state officers is, therefore, constitutional in origin, we can no longer permit that right to remain an empty promise. Because it is enforceable in the same manner and to like effect as other basic rights secured by the Due Process Clause, we can no longer permit it to be revocable at the whim of any police officer who, in the name of law enforcement itself, chooses to suspend its enjoyment.") See also *Gardner* and *Anderson*, Criminal Evidence, 3rd ed., 1995, 197–98. Before 1961, about half of the states have introduced the exclusionary rule. *Ibid.*

2. Admissibility of Wiretap Evidence under the 4th Amendment

The first Supreme Court case that dealt with the admissibility of wiretap evidence was *Olmstead v. U.S.*.[449] As discussed above, the Court decided that wiretapping conducted by law enforcement was not a search or a seizure under the 4th Amendment[450] and that therefore wiretapping was neither illegal nor improper. Since the Court limited the application of the exclusionary rule established in *Weeks* to evidence obtained in violation of the 4th and 5th Amendments, the *Weeks* rule was not applicable to wiretap evidence.[451] As a result, such evidence was admitted in the *Olmstead* case. The Court here stuck to the old common law principle, stating that "the admissibility of evidence is not affected by the illegality of the means by which it was obtained".[452] Furthermore, the Court also hesitated to challenge the long practiced common law rule "without the sanction of congressional enactment".[453]

This problem was resolved in *Katz*, in which interceptions that violate a person's "reasonable expectation of privacy" were regarded as a special type of search and seizure under the 4th Amendment. As a result, the admissibility of evidence from interceptions is now subject to the 4th Amendment.

3. Admissibility under Section 605

Section 605 of the *Federal Communications Act* was passed by Congress in 1934, providing that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person". This provision was first interpreted by the U.S. Supreme Court in *Nardone v. U.S.*[454] in 1937, where testimony of Federal agents as to the contents of communications wiretapped by

[449] *Olmstead v. United States*, 277 U.S. 438 (1928).

[450] *Id.* at 466 ("We think, therefore, that the wiretapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

[451] *Id.* at 467 ("The Weeks Case announced an exception to the common law rule by excluding all evidence in the procuring of which government officers took part by methods forbidden by the Fourth and Fifth Amendments.").

[452] *Ibid.*

[453] *Ibid.* ("Nor can we, without the sanction of congressional enactment, subscribe to the suggestion that the courts have a discretion to exclude evidence, the admission of which is not unconstitutional, because unethically secured. This would be at variance with the common-law doctrine generally supported by authority. There is no case that sustains, nor any recognized textbook that gives color to, such a view. Our general experience shows that much evidence has always been receivable, although not obtained by conformity to the highest ethics.").

[454] *Nardone v. U.S.*, 302 U.S. 379 (1937).

them was held as falling under the term "divulge". The Court stated that their testimony violated Section 605 and therefore was not admissible.[455]

Only two years later, in a case involving the same offenders, the Court decided in *Nardone v. U.S.* [456] (*Nardone II*) that evidence obtained on the basis of information obtained through illegal wiretapping was not admissible.[457] The expression "fruit of the poisonous tree" stems from this judgment. The "fruit of the poisonous tree" or "derivative evidence" rule[458] extends the reach of the exclusionary rule from evidence obtained directly from illegal searches to evidence derived from illegally obtained evidence. In wiretap cases, the derivative evidence refers to evidence derived from evaluating wiretapped communications. The consequence of this theory is that a defendant in a criminal case must be given an opportunity to challenge the evidence against him and to determine whether it is "tainted" by the illegal search.[459]

Both *Nardone* cases, however, focused only on the interpretation of Section 605 without touching upon the Constitution. Since *Katz*, admissibility of evidence from interceptions needs to be decided based on the 4th Amendment and Section 605. Since the contents of a recording from surveillance interceptions are deemed to be reliable, they are strong evidence against a defendant once they have been admitted at trial. Therefore, defense lawyers have a strong incentive to move for suppression of such evidence.

4. Admissibility under *Title III*

Title III superseded Section 605 in 1968. Reflecting former precedent and formulating a "judicially created exclusionary rule"[460], *Title III* contains two provisions to prescribe a statutory exclusionary rule for wire and oral communications, namely,

---

[455] This decision was not interpreted as an overruling of *Olmstead v. United States*, 277 U.S. 438 (1928), because it only dealt with the language of a statute, rather than constitutional rights. See *Beard v. Sanford*, 110 F.2d 527 (C. C. A. 5th, 1940); *Rosenzweig*, Cornell Law Quarterly 32 (1946–1947), 514, 536.

[456] *Nardone v. United States*, 308 U.S. 338 (1939).

[457] *Nardone*, 308 U.S. 338, 341 (1939) ("The burden is, of course, on the accused in the first instance to prove to the trial court's satisfaction that wire-tapping was unlawfully employed. Once that is established – as was plainly done here – the trial judge must give opportunity, however closely confined, to the accused to prove that a substantial portion of the case against him was a fruit of the poisonous tree. This leaves ample opportunity to the Government to convince the trial court that its proof had an independent origin.") This expression was imported from the statement of *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) ("The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all.").

[458] *Gardner/Anderson*, Criminal Evidence, 1995, 200.

[459] *Nardone v. United States*, 308 U.S. 338, 341 (1939).

[460] *LaFave/Israel*, Handbook Criminal Procedure, 1992, 271.

18 U.S. Code § 2515 and § 2518(10)(a).[461] § 2515 prohibits the use of illegally intercepted wire or oral communications as evidence, while § 2518(10)(a) sets forth the procedure and grounds for a suppression motion. Besides these two provisions, § 2510(11) defines the "aggrieved person" as the individual who has standing to file a motion to suppress the evidence.

a) The Scope of the Exclusionary Rule under *Title III*

§ 2515 provides that evidence derived from wire or oral communications obtained in violation of *Title III* is prohibited "in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof".[462] This rule largely reflects the "fruit of the poisonous tree" doctrine previously developed by courts. The wording of this exclusionary rule only applies to wire and oral communications, not to electronic communications because, historically, the latter was considered less private than wire and oral communications. Although this opinion is no longer popular, Congress has not made any amendments to this rule.[463] Therefore, the suppression of evidence based on illegal surveillance of electronic communications can only be sought directly under the Constitution.[464]

In addition, since *Title III* regulates private surveillance, this statutory exclusionary rule applies both to surveillance conducted by private parties and law enforcement agencies, while the judicial exclusionary rule applies only to law enforcement agencies.[465]

---

[461] § 2515 ("Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.").

[462] *Ibid.*

[463] *LaFave* et al., Criminal Procedure, 2020, § 4.6(m).

[464] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.1.

[465] *U.S. v. Crabtree*, 565 F.3d 887, 891 (4th Cir. 2009) ("The Fourth Amendment, of course, constrains state and federal officers only; it has no applicability to private parties. *Title III*, by contrast, explicitly applies to private parties as well as governmental officers. Because the Fourth Amendment and *Title III* differ greatly in scope and purpose, we believe it would be inappropriate to treat the judicially created Fourth Amendment exclusionary rule as impliedly setting the boundary for the broader, statutorily created exclusionary rule of § 2515.").

b) Standing to Demand Suppression

The issue of standing determines who is "a proper party to assert the claim of illegality and seek the remedy of exclusion".[466] Standing to "move to suppress the contents of any wire or oral communication intercepted pursuant to" *Title III* is granted by § 2518(10)(a) to "any aggrieved person in a trial, hearing or proceeding".[467] This means that in order to seek suppression of evidence, a person must be (1) aggrieved by the interception; and (2) be a party of a "trial, hearing, or proceeding".[468] § 2510(11) defines an "aggrieved person" as "a person who was a party to any intercepted wire, oral or electronic communication or a person against whom the interception was directed".

aa) Being Party to Communications

This expression in § 2510(11) corresponds with the standing requirement under the 4th Amendment. In *Alderman v. United States*, the U.S. Supreme Court limited standing to "those whose rights were violated by the search itself, not … those who are aggrieved solely by the introduction of damaging evidence."[469] Professor Wayne LaFave termed this approach the "personal rights" approach[470]; it means that only the person whose constitutional rights were violated or intruded upon by a search has the right to apply for suppression of the evidence.[471] In order to be qualified as an aggrieved person, the party "must have been a victim of a search or seizure", that is, the search must have been directed against that person.[472] Under this approach, the right to privacy of those who were parties to the wire or oral communications is also infringed upon by the interception. Thus, without doubt, such parties have standing to move to suppress such communications as evidence.

bb) Possessory Interest

The U.S. Supreme Court in *Alderman v. United States* also granted standing for the suppression of an intercepted communication to the person on whose premises the

[466] *LaFave* et al., Criminal Procedure, 2020, § 9.1(a).

[467] § 2518(10)(a).

[468] *Fishman/Mckenna*, Wiretapping and Eavesdropping, 2019, § 35.21.

[469] *Alderman v. United States*, 394 U.S. 165, 171 – 172 (1968) ("The established principle is that suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence."; *People v. Varnum*, 66 Cal. 2d 808 (1967) (The defendant lacks standing to move to suppress the evidence which is fruits of Miranda violation.).

[470] *LaFave* et al., Criminal Procedure, 2020, § 9.1(a).

[471] *Ibid.*

[472] *Jones v. United States*, 362 U.S. 257, 261 (1960) ("In order to qualify as a 'person aggrieved by an unlawful search and seizure' one must have been a victim of a search or seizure, one against whom the search was directed").

interception occurred, even if he did not take part in this communication.[473] This interpretation differs from the definition in § 2510(11) and expands standing to non-parties with a mere "possessory interest".[474] The Court argued that illegal interception violates not only the right to privacy of the parties to the communication but also the property rights of the person in whose property the communication takes place.[475] Standing based upon the "possessory interest" was affirmed in *U.S. v. Gonzalez, Inc.*, where the owners of a business company were entitled to move to suppress intercepted communications occurring on their premises, although they were not party to some of the communications.[476]

cc) The Person against Whom the Interception Was Directed

The meaning of this expression, incorporated from *Jones v. U.S.*,[477] originally was not clear, since it could be literally interpreted as referring to the target of the surveillance.[478] A proposal submitted by Senator Philip Hart, which sought to give "standing to any person against whom eavesdropping evidence was sought to be used",[479] however, was defeated.[480] This reflected the opinion of the legislature that a defendant cannot assert standing just because he is "'implicated' by the evidence",[481] he is the "ultimate target of the investigation", or his arrest is the fruit of the interception of another person.[482] Nevertheless, in some cases, courts granted standing to persons implicated by illegally intercepted evidence who were neither a party to the communication nor had a possessory interest, arguing that the more restrictive approach to the standing requirement would "undermine the deterrent effect of the

[473] *Alderman v. United States*, 394 U.S. 165 (1968).

[474] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.18. Some scholars include the person who has "possessory interest" within the group of "a person against whom the interception was directed". *Fishman/McKenna*, Wiretapping and Eavesdropping, 2019, § 35.10.

[475] This "possessory interest" is not necessary established on the basis of ownership; it is rather that "he has the right to exclude others from dealing with the property." *United States v. Perea*, 986 F.2d 633, 639–640 (2d Cir. 1993).

[476] *U.S. v. Gonzalez, Inc.*, 412 F.3d 1102, 1116–1117 (9th Cir. 2005).

[477] *Jones v. United States*, 362 U.S. 257, 261 (1960) ("…one against whom the search was directed").

[478] *LaFave* et al., Handbook Criminal Procedure, 1992, 273.

[479] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.19.

[480] 114 Cong. Rec. 12508 (1968).

[481] *U.S. v. Eiland*, 398 F. Supp. 2d 160, 167 (D.D.C. 2005) ("Some defendants … claim that merely being "implicated" by the evidence gives rise to standing. They cite no binding precedent for this assertion, and this Court finds their argument specious in light of existing case law and the principles that the standing requirement seeks to protect. Therefore, this Court finds that a defendant may challenge only that evidence resulting from surveillance of his property or of which he was a target or interceptee.") (*Citation omitted*).

[482] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.16.

exclusionary rule".[483] For instance, a lower Federal court decided that a defendant had standing to challenge the legality of a former surveillance order during which his communications had not been intercepted, on the grounds that the subsequent order where his communications had been intercepted was the result of the former order.[484] This rationale, however, has not been widely accepted.[485]

c) Grounds for Excluding Evidence

Title III provides grounds for the suppression of evidence derived from illegal interceptions.[486] The related rules consist of a general provision concerning the grounds for suppression, i. e., § 2518(10)(a), and provisions concerning violations of specified requirements in *Title III*, such as § 2518(8)(a) and § 2518(9).

aa) "Unlawfully Intercepted" Communications

According to § 2515, "unlawfully intercepted" communications can be understood as those obtained "in violation of" *Title III.* One example is *U.S. v. Giordano*,[487] where the initial order was authorized by the Attorney General's Executive Assistant who had no authority under § 2516(1), whereas the extension application had been approved by the Attorney General himself. The Court granted the motion to suppress the communications intercepted pursuant to the extension order because they were derived from the interception pursuant to the invalid initial order. In this case, the Court rejected the Government's contention that "unlawfully intercepted" communications in § 2518(10)(a)(i) referred only to those obtained in violation of the Constitution. The Court interpreted the intention of Congress to include communications "unlawfully intercepted" in violation of *Title III* requirements.[488]

---

[483] *Id.* § 6.20. See also *People v. Brown*, 364 N.Y.S.2d 364, 374 (Sup 1975); *U.S. v. Gibson*, 500 F.2d 854, 855 (4th Cir. 1974).

[484] *U.S. v. Marcello*, 508 F. Supp. 586, 601 – 602 n.6 (E.D. La. 1981).

[485] See *U.S. v. Civella*, 648 F.2d 1167, 1171 – 1172 (8th Cir. 1981) (The defendant is held to be lack of standing to move to suppress the intercepted communications from the first two orders which were the probable cause for the subsequent order upon which he was intercepted); *U.S. v. Cruz*, 594 F.2d 268, 273 – 274 (1st Cir. 1979) (The defendant has no standing to move to suppress the intercepted communications which were probable cause for the search warrant of his home.). *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.20.

[486] *Fishman*/*McKenna*, Wiretapping and Eavesdropping, 2019, § 34.1.

[487] *U.S. v. Giordano*, 416 U.S. 505 (1974).

[488] *Id.* at 527 ("The words 'unlawfully intercepted' are themselves not limited to constitutional violations, and we think Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.").

(1) "Central Role" Test

To determine which violations of *Title III* can lead to exclusion, the "central role" test was developed in *U.S. v. Giordano*[489]. All evidence derived from a warrant that violates a "central" provision is subject to suppression.[490] In *Giordano*, the U.S. Supreme Court ruled that suppression can be granted under *Title III* only if the violated statutory provision "was intended to play a central role in the statutory scheme".[491] In this case, the Court held that the requirement that limits the authorization of applications to senior officers in the U.S. Attorney's Office plays a "central role" in the statutory scheme because it "directly and substantially implement[s] the congressional intention to limit the use of intercept procedures," and is designed "to limit resort to wiretapping".[492]

Under the scheme established by *Giordano*, courts must first decide whether there was a violation of *Title III* and then determine whether the violated provision plays a "central role", namely, whether the provision "directly and substantially implement[s] the congressional intention to limit the use of intercept procedures."[493] For instance, in accordance with these criteria, the Court in *Giordano* determined that the requirements limiting the crimes that can be investigated via interception (§ 2516) and those concerning probable cause (§ 2518(3) and (5)) play a "central role".[494] In addition, the duration directive, termination directive and the minimization requirement provided for in § 2518(5) are also "central" provisions. This means that evidence obtained in violation of the duration directive, namely, evidence that has been obtained after the order has ended, will be suppressed. Excessive interception, however, does not invalidate the whole order, and the evidence obtained within the approved period is still admissible.[495]

Due to the unclear criteria of the minimization requirement[496], it is more difficult to decide on the exclusion of evidence in the case of a violation of the minimization requirement.[497] For instance, the good faith of law enforcement officers can have an

[489] *U.S. v. Giordano*, 416 U.S. 505 (1974).

[490] *Id.* at 528.

[491] *Ibid.* ("We are confident that the provision for pre-application approval was intended to play a central role in the statutory scheme and that suppression must follow when it is shown that this statutory requirement has been ignored.").

[492] *Id.* at 527.

[493] *Ibid.* See also *Fishman*, American University L. Rev. 28 (1979), 315, 323.

[494] *Ibid.* ("We have already determined that Congress intended not only to limit resort to wiretapping to certain crimes and situations where probable cause is present but also to condition the use of intercept procedures upon the judgment of a senior official in the Department of Justice that the situation is one of those warranting their use.").

[495] *People v. Meranto*, 86 A.D.2d 776 (N.Y. App. Div. 1982).

[496] The criteria upon which the minimization requirement is evaluated have been discussed above, see Section 21.c)cc), Chapter IV, Part I.

[497] Some scholars categorize both duration and termination directives as part of minimization requirement. See *Fishman*, American University L. Rev. 28 (1979), 315, 331. In the

impact on exclusion for violations of the minimization requirement. As discussed in *Scott v. U.S.*,[498] bad faith of law enforcement officers is not required for a finding that § 2518(5) has been violated,[499] although officers who intentionally intercept, disclose or use wire, oral and electronic communications in violation of *Title III* can be sanctioned criminally[500] or administratively[501]. Good faith, however, is considered to play a role in deciding to what extent the suppression will be granted, i. e. partially or completely.[502] If law enforcement officers violated the minimization requirement in good faith, suppression will be granted only regarding the conversations that should have been minimized.[503] This approach has attracted criticism because it does not deter officers from excessive interception, due to the fact that officers can obtain incriminating conversations without fear that all of the evidence will be suppressed.[504] Some courts even held that the good faith exception, as stated by the Supreme Court in *U.S. v. Leon*[505], is inapplicable in cases involving surveillance evidence because the statutory exclusionary rule § 2515 does not provide for such an exception.[506] Whenever a substantial violation of the minimization requirement is proved, courts should grant complete suppression of the obtained evidence.[507] A substantial violation means that "a pattern of unlawful interception is established",[508]

---

current context, the minimization requirement limits to the substantial behavior during the execution of the order, excluding the element of when the interception should be terminated.

[498] *Scott v. U.S.*, 436 U.S. 128 (1978).

[499] *Id.* at 136–139 ("Petitioners…argue… the statute regulating wiretaps requires the agents to make good-faith efforts at minimization, and the failure to make such efforts is itself a violation of the statute which requires suppression.[T]his argument is flawed for several reasons. In the first place, in the very section in which it directs minimization to Congress, its use of the word 'conducted,' makes it clear that the focus is to be on the agents' actions not on their motives. Any lingering doubt is dispelled by the legislative history which, as we have recognized before in another context, declares that § 2515 was not intended 'generally to press the scope of the suppression role beyond present search and seizure law.'").

[500] 18 U.S.C. § 2511(1)(4) and (5).

[501] 18 U.S.C. § 2520(f).

[502] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.21.

[503] For example, *U.S. v. Charles*, 213 F.3d 10, 21–22 (1st Cir. 2000) ("The district court ruled that the interception of the July 29 Charles/Kelley phone call was in clear violation of the amended minimization order, entitling appellant Charles to a suppression remedy under § 2518(1)(a)(iii). The district court, however, declined to invalidate the entire wiretap. Instead, the court ruled that the appropriate remedy was the limited suppression of the Charles/Kelley call because the totality of the circumstances demonstrates that the state police's minimization efforts were reasonably managed. The district court's ruling is amply supported by both the law and the record.") (*Internal citation omitted).*

[504] *Carr* et al., The Law of Electronic Surveillance, 2020, § 5.21.

[505] *United States v. Leon*, 468 U.S. 897 (1984).

[506] For example, *U.S. v. Spadaccino*, 800 F.2d 292, 296 (2d Cir. 1986).

[507] *Ibid.*

[508] *U.S. v. Dorfman*, 542 F. Supp. 345, 394–395 (N.D. Ill. 1982) ("[w]e do not simply focus on the individual conversation and determine whether it contains any incriminating statements; rather, where a pattern of unlawful interception is established we examine the challenged in-

or that no effort has been made to minimize the interception to pertinent communications.[509] All the conversations intercepted in this way, even if incriminating and pertinent, should be excluded.

(2) Non-Central Provisions

The courts also determined that some provisions in *Title III* are not central, hence their violation does not mandate the suppression of the intercepted communications. In *United States v. Chavez*[510] the authorizing official, the U.S. Attorney General, was misidentified as an Assistant Attorney General by the Justice Department. The Court held that the application and the warrant issued under *Title III* were nevertheless valid and thus the evidence obtained was admissible since § 2518(1)(a) and (4)(d) (concerning the identification of the authorizing official) "does not establish a substantive role to be played in the regulatory system".[511]

The identity of the targets was identified by courts as a non-central provision. In *U.S. v. Donovan*,[512] the application did not include the names of all persons to be intercepted. The U.S. Supreme Court decided that there was a violation of *Title III*, however, the evidence derived from the warrant was held to be admissible, because the application provided sufficient information for the issuing judge to approve the application even without the correct names.[513]

---

terceptions to determine whether they fall within that pattern. If the Government continues to intercept, for example, a person not named in the authorization order after his or her identity has been established and a pattern of innocent conversation takes place, it would be of no moment that eventually that individual was heard discussing incriminating matter; the conversation would still be subject to suppression because it would have been 'unlawful' for the monitors to be overhearing the conversation in the first place.").

[509] *State v. Thompson*, 464 A.2d 799, 812–813 (Conn. 1983).

[510] *U.S. v. Chavez*, 416 U.S. 562 (1974).

[511] *Id.* at 578. In this case, four members of the Court delivered their dissenting opinions and argued that the identification requirement was central.

[512] *U.S. v. Donovan*, 429 U.S. 413 (1977).

[513] *Id.* at 436 ("Here, however, the statutorily imposed preconditions to judicial authorization were satisfied, and the issuing judge was simply unaware that additional persons might be overheard engaging in incriminating conversations. In no meaningful sense can it be said that the presence of that information as to additional targets would have precluded judicial authorization of the intercept. Rather, this case resembles Chavez, where we held that a wiretap was not unlawful simply because the issuing judge was incorrectly informed as to which designated official had authorized the application. The Chavez intercept was lawful because the Justice Department had performed its task of prior approval, and the instant intercept is lawful because the application provided sufficient information to enable the issuing judge to determine that the statutory preconditions were satisfied.") (Footnote omitted) The Court, however, stated that the result might be different if the missing had been made intentionally in order to mislead the judge. *Id.*, at 436, Fn. 23 ("There is no suggestion in this case that the Government agents knowingly failed to identify respondents Donovan, Robbins, and Buzzacco for the purpose of keeping relevant information from the District Court that might have prompted the court to conclude that probable cause was lacking. If such a showing had been made, we would have a

bb) "Insufficient on its Face" (§ 2518(10)(a)(ii))

The expression "insufficient on its face" in § 2518(10)(a)(ii) concerns the validity of the warrant. "Insufficient on its face" means that the warrant does not include all the contents required in § 2518(3)(4) and (5). The evaluation of whether a warrant is "insufficient on its face" follows the "central role" test: Suppression is mandatory only if the facial insufficiency of the warrant leads to the violation of a "central provision" of the statute. In *United States v. Chavez*[514] and *U.S. v. Donovan*,[515] the U.S. Supreme Court denied a motion of suppression because the order itself included the required information "on its face", despite the misidentification of officers and the missing names of the potential interceptees.[516] The Court also decided that a misleading description of the communications should not lead to suppression.[517]

cc) Not "in Conformity with the Order" (§ 2518(10)(a)(iii))

This item focuses on the practical details of the implementation process. "In conformity with the order" requires that the implementation must be in compliance with the warrant. For instance, communications intercepted after 19.30 o'clock should be suppressed if the order prohibits such interceptions[518] and conversations held in a bedroom should be excluded if the bedroom is not listed among the locations allowed to be intercepted by the warrant.[519] The "conformity" here mainly concentrates on the process of implementation and ensures that it conforms to the warrant. Chance findings achieved through surveillance which might not have been predicted by the warrant are regarded as "in conformity with the order". For instance, if offenses not named in the warrant are discovered during surveillance, they do not fall under § 2518(10)(a)(iii) but under § 2517(5).

---

different case.") In a roving interception case, it is required that at least one person should be identified. This requirement is regarded as "central". *Fishman/McKenna*, Wiretapping and Eavesdropping, 2019, § 34.14.

[514] *U.S. v. Chavez*, 416 U.S. 562 (1974).

[515] *U.S. v. Donovan*, 429 U.S. 413 (1977).

[516] For instance, *id.* at 432 ("There is no basis on the facts of this case to suggest that the authorization orders are facially insufficient.") and *U.S. v. Chavez*, 416 U.S. 562, 574 (1974) ("That this has subsequently been shown to be incorrect does not detract from the facial sufficiency of the order.").

[517] *U.S. v. Cunningham*, 113 F.3d 289, 294 (1st Cir. 1997). More details can be found *Fishman/McKenna*, Wiretapping and Eavesdropping, 2019, § 34.17, where several other provisions in *Title III* whose violations did not lead to suppression are discussed. See also *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.43.

[518] *U.S. v. Principie*, 531 F.2d 1132, 1140 (2d Cir. 1976).

[519] *U.S. v. Lucht*, 18 F.3d 541, 547 (8th Cir. 1994).

dd) Violation of Regulations regarding the Post-Implementation Phase

Provisions in *Title III* concerning post-implementation requirements refer to the delivery and sealing of evidence (§ 2518(8)(a)), the notification of persons named in the order or the application (§ 2518(8)(d)), the disclosure of evidence relating to other crimes (§ 2517(5)) and to pretrial notice (§ 2518(9)). § 2517(5), § 2518(8)(a) and § 2518(9)) contain exclusionary rules. § 2518(10)(a) leaves open the question of whether suppression is required if other post-implementation provisions have been violated. One Federal Court held that violations of such post-implementation provisions can lead to suppression under § 2518(10)(a)(i).[520]

In order to determine under what circumstances legally intercepted evidence should be excluded for violation of post-implementation provisions, the Court in *United States v. Chun*[521] developed a three-step test: (1) first, following the "central role" approach established by Chavez[522] and Giordano[523], "whether the particular procedure is a central or functional safeguard in *Title III*'s scheme to prevent abuses";[524] (2) "whether the purpose which the particular procedure was designed to accomplish has been satisfied in spite of the error";[525] and (3) "whether the statutory requirement was deliberately ignored; and, if so, whether there was any tactical advantage to be gained thereby."[526] Three elements are considered in this test, i. e., the importance of the violated provision ("central role" test), the purpose of the provision, and the good faith of law enforcement. The test sets a higher threshold for exclusion than exclusionary rules concerning implementation rules. For example, if a law enforcement officer violates the minimization requirement in good faith, the resulting evidence is to be partially excluded. By contrast, only a deliberate violation of post-implementation rules may lead to suppression.

Moreover, the Court interpreted this three-step test in a restrictive way and hesitates to exclude evidence obtained on the basis of a valid warrant. Not long after deciding *Chun*[527], the U.S. Supreme Court in *U.S. v. Donovan*[528] denied a suppression

[520] *U.S. v. Lawson*, 545 F.2d 557, 564 (7th Cir. 1975) ("we hold that the post-interception violations must also be scrutinized to determine if the failures to satisfy the statutory requirements directly and substantially affect the Congressional intention to limit the use of intercept procedures and to comply with Fourth Amendment principles."); see also *United States v. Chun*, 503 F.2d 533 (9th Cir. 1974) and *United States v. Falcone*, 505 F.2d 478 (3d Cir. 1974).

[521] *United States v. Chun*, 503 F.2d 533 (9th Cir. 1974).

[522] *U.S. v. Chavez*, 416 U.S. 562 (1974).

[523] *United States v. Giordano*, 416 U.S. 505 (1974).

[524] *United States v. Chun*, 503 F.2d 533, 542 (9th Cir. 1974).

[525] *Ibid.*

[526] *Ibid.* These three factors were also cited in *U.S. v. Lawson*, 545 F.2d 557 (7th Cir. 1975) and *United States v. Falcone*, 505 F.2d 478 (3d Cir. 1974).

[527] *United States v. Chun*, 503 F.2d 533 (9th Cir. 1974).

[528] *U.S. v. Donovan*, 429 U.S. 413 (1977).

motion based on the lack of a notification service, § 2518(8)(d). The Court stated that "nothing in the structure of the Act or this legislative history" indicated that the inadvertent failure of law enforcement officers to provide subjects with notification of the surveillance could make the intercepted conversations "unlawful", since the violation occurred after the conversations had been lawfully intercepted under a valid order.[529] The noncompliance with post-implementation provisions by itself is seldom held to affect the admissibility of the intercepted communications.[530] Even where a provision demands exclusion, such as § 2518(8)(a), the courts interpret the expression "a satisfactory explanation for the absence" as meaning that suppression will only be granted if the provision has been violated deliberately, otherwise there will be "a satisfactory explanation" for unsealing.[531] The same is true of the pretrial notice[532] and disclosure requirements[533].

In sum, courts adopt a more restrictive approach toward applying the exclusionary rule for violations that take place after the implementation than during the implementation. A possible explanation is that the intrusion caused by the former is less serious than the latter.

ee) Evidence Derived from Illegal Private Interceptions

As stated above, *Title III* regulates interception activities conducted by both private persons and law enforcement officers. § 2515 provides that evidence derived from the contents of any wire or oral communication intercepted in violation of *Title III* must be excluded. Evidence derived from communications intercepted by private persons should thus also be subject to § 2515. Therefore, even if law en-

[529] *Id.* at 438–439 ("Nothing in the structure of the Act or this legislative history suggests that incriminating conversations are 'unlawfully intercepted' whenever parties to those conversations do not receive discretionary inventory notice as a result of the Government's failure to inform the District Court of their identities. At the time inventory notice was served on the other identifiable persons, the intercept had been completed and the conversations had been 'seized' under a valid intercept order. The fact that discretionary notice reached 39 rather than 41 identifiable persons does not in itself mean that the conversations were unlawfully intercepted. [T]he legislative history indicates that post-intercept notice was designed instead to assure the community that the wiretap technique is reasonably employed. But even recognizing that Congress placed considerable emphasis on that aspect of the overall statutory scheme, we do not think that post-intercept notice was intended to serve as an independent restraint on resort to the wiretap procedure.") (*Footnotes omitted*).

[530] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.43.

[531] For example, *Cabble v. State*, 114 So. 3d 855, 866 (Ala. Crim. App. 2012) (no order to unsealing could be produced); *U.S. v. Lawson*, 545 F.2d 557 (7th Cir. 1975).

[532] *Piggott v. U.S.*, WL 77001 (S.D. N.Y. 2003) (The motion of suppression was rejected where the defendant did not receive copies of the application and order within 10 days before trial resulted from a technical failure).

[533] *U.S. v. Cardall*, 773 F.2d 1128, 1134 (10th Cir. 1985) (subsequent application was not submitted in time); *U.S. v. Johnson*, 696 F.2d 115, 125 (D.C. Cir. 1982) (subsequent application was defective).

forcement officers were not involved in the illegal interception and were informed about the contents of the communications only afterwards, neither the contents nor evidence derived therefrom is admissible. The exclusionary rule under the 4th Amendment, however, applies only to governmental activities.[534] Moreover, Congress stated that § 2515 "largely reflects existing law"[535] and does not "press the scope of the suppression rule beyond present search and seizure law".[536] There seems to be a conflict between § 2515 and its legislative history, causing a division in the opinion of courts about the use of communications illegally intercepted by private persons.

In *United States v. Murdock*,[537] the United States Court of Appeals for the Sixth Circuit introduced the so-called "clean hands" exception to § 2515, allowing the prosecutor to introduce communications illegally obtained by the defendant's wife because "the government played no part in the unlawful interception" and thus had "clean hands".[538]

This holding overruled *United States v. Vest*,[539] where the "clean hands" exception had been explicitly rejected by the First Circuit.[540] The Fourth Circuit in *United States v. Crabtree*[541] criticized *Murdock*[542] and followed *United States v. Vest*[543], stating that § 2515 "prohibits the introduction of improperly intercepted communications without regard to whether the government was involved in the interception".[544] Today, the mainstream view does not recognize a "clean hands" exception to § 2515 and favors suppression of evidence illegally obtained by private persons.[545]

---

[534] *Burdeau v. McDowell*, 256 U.S. 465 (1921).

[535] S.Report 1097, 2185 ("It largely reflects existing law. It applies to suppress evidence directly or indirectly obtained in violation of the chapter. There is, however, no intention to change the attenuation rule. Nor generally to press the scope of the suppression rule beyond present search and seizure law.") (Internal citation omitted).

[536] *Ibid.*

[537] *United States v. Murdock*, 63 F.3d 1391 (6th Cir. 1995).

[538] *United States v. Murdock*, 63 F.3d 1391, 1403–1404 (6th Cir. 1995) ("In this case, the government played no part in the unlawful interception … Under the circumstances of this case, we find that any privacy interest which the defendant may have had is protected solely by his right to bring a civil action against his former wife. However, he does not enjoy the additional right to the suppression of the interceptions where, as here, the government took no part in the interceptions. In our view, it is appropriate under the legislative history and the case law to apply a 'clean hands' exception to Section 2515.").

[539] *United States v. Vest*, 813 F.2d 477 (1st Cir. 1987).

[540] *Id.* at 481 ("We decline to read into section 2515 an exception permitting the introduction in evidence of an illegally-intercepted communication by an innocent recipient thereof.").

[541] *U.S. v. Crabtree*, 565 F.3d 887 (4th Cir. 2009).

[542] *Id.* at 891 ("Nothing in the Sixth Circuit's analysis of the issue convinces us that it would be proper to read a clean-hands exception into § 2515's exclusionary rule.").

[543] *United States v. Vest*, 813 F.2d 477 (1st Cir. 1987).

[544] *U.S. v. Crabtree*, 565 F.3d 887, 892 (4th Cir. 2009).

[545] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.48.

5. Comments on the Exclusionary Rule

The 4th Amendment prohibits unreasonable searches and seizures but keeps silent on the consequences of such infringement upon the right to privacy. To deter unreasonable searches and seizures and to protect the integrity of the judicial process,[546] the Supreme Court developed the exclusionary rule through a series of judgments. In the *Weeks* case, the Court ruled that evidence seized in violation of the 4th Amendment should be excluded in Federal courts. In *Mapp*, the Court made this rule applicable to state courts. In *Silverthorne Lumber Co. v. United States*[547] and *Nardone*[548], the Court decided that this rule excludes not only evidence directly obtained through illegal searches but also evidence derived from such evidence (the "fruit of the poisonous tree"). By balancing the deterrent value of the exclusionary rule and the cost of excluding the evidence, the Supreme Court established several exceptions to the exclusionary rule, such as a good faith exception.[549] In sum, the exclusionary rule in the U.S. is a judge-made remedy rather than a remedy inherent in the 4th Amendment.

The impact of the deterrent effect of the exclusionary rule is controversial. Some writers argue that this rule does not significantly deter police from abusing their powers,[550] while others evaluate its effect more positively.[551]

The U.S. Supreme Court held that electronic surveillance constitutes a search under the 4th Amendment. Therefore, the exclusionary rule is applicable to evidence obtained through such surveillance. Moreover, *Title III* constitutes a statutory exclusionary rule, especially designed for surveillance.

When police conduct interceptions without a warrant, courts should first determine whether the police behavior constitutes a search under the "reasonable expectation of privacy" doctrine and whether it belongs to one of the exceptional situations where warrants are not required, such as consent surveillance or plain hearing. If a warrant was issued, the courts need to decide whether the interception nevertheless was "unlawful", for example, because the warrant was "insufficient on its face",[552] or because the implementation did not conform with the warrant. If there was a violation, courts must decide whether the violated provision is a "central provision". Only violation of a "central provision" mandates suppression. If only post-implementation provisions were violated, courts set a higher threshold for

[546] *Lippman*, Criminal Procedure, 2020, 386, 424.

[547] *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920).

[548] *Nardone v. United States*, 308 U.S. 338 (1939).

[549] *Lippman*, Criminal Procedure, 2020, 424; *Jirard*, Criminal Law & Procedure, 2019, 240–241.

[550] *Alschuler*, University of Chicago L. Rev. 75 (2008), 1365, 1374; *Nardulli*, American Bar Foundation Research Journal 8 (1983), 585. More about the empirical studies on deterrence doctrine can be found in Part IV.

[551] *Belknap*, The Supreme Court and Criminal Procedure, 2011, 76.

[552] See Section 4. c) bb), Chapter V, Part I.

excluding evidence from trial and require that the violation was committed deliberately. If evidence was obtained illegally by private persons, the majority view does not recognize a "clean hands" exception to § 2515. Therefore, the evidence illegally obtained by private persons should also be suppressed.

VI. Empirical Studies

The Administrative Office of the United States Courts (AO) is required by 18 U.S. Code § 2519(3) to report statistics annually to Congress on the number of Federal and state applications to intercept wire, oral, or electronic communications, and the number of orders and extensions granted or denied during the preceding calendar year. These reports, including statistics, can be found on the official website of the AO.[553] In May 2020, the reports from 1997 to 2018 could be found on this website. Although these reports are called "wiretap reports", the statistics include interceptions of wire, oral and electronic communications. One warrant can authorize more than one type of surveillance.[554] All statistics analyzed in this Chapter come from these reports.

1. Number of Surveillance Applications and Issued Warrants

According to Table Wire A1 – Appendix Tables Wiretap (December 31, 2018),[555] warrants are normally specific to a whole case or investigative activity. For instance, if the police are investigating a narcotics case, only one warrant will probably be applied for and issued, and it will include the names of all suspects and facilities to be intercepted. If suspicion extends to other less serious crimes, they can also be listed in the same warrant.[556] This means that applicants can decide on the persons, locations and offenses to be included in an application.

[553] https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports, visited at 03.05.2020.

[554] See Table Wire 6 – Wiretap Wiretap (December 31, 2018). The table can be downloaded at https://www.uscourts.gov/statistics/table/wire-6/wiretap/2018/12/31, visited at 03.05.2020.

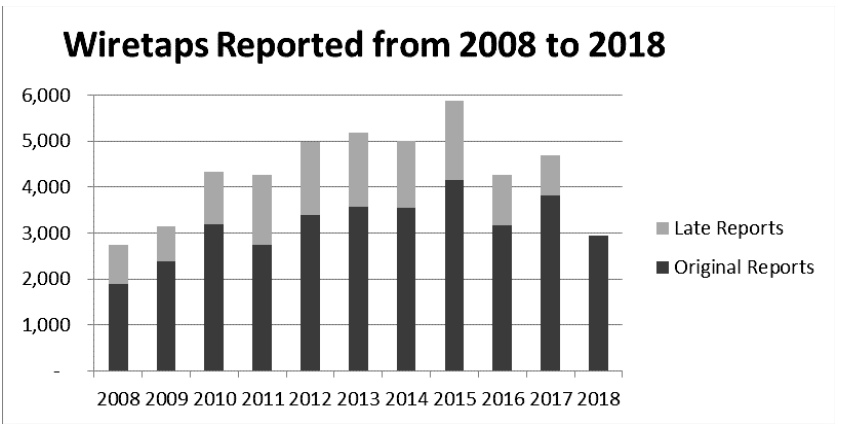
[555] The table can be downloaded at https://www.uscourts.gov/statistics/table/wire-a1/wiretap/2018/12/31, visited at 03.05.2020.

[556] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 06.05.2020.

Table 1
The Number of Applications, Authorized Warrants and Implemented Warrants from 2008 to 2018

	Intercept Applications Requested	**Intercept Applications Authorized (Whole U.S./Federal)**
2008	1891	1891/386
2009	2376	2376/663
2010	3195	3194/1207
2011	2734	2732/792
2012	3397	3395/1354
2013	3577	3576/1476
2014	3555	3554/1297
2015	4148	4148/1403
2016	3170	3168/1551
2017	3813	3813/2013
2018	2939	2937/1457

Comparing Columns 2 and 3 (total) in Table 1, almost all applications requested were approved by judges, with only 10 applications rejected from 2008 to 2018 in the U.S.



Graph 1: Wiretaps Reported in the United States from 2009 to 2018[557]

Graph 1 shows an increase in the numbers of issued warrants in all (State and Federal) U.S. jurisdictions from 2008 to 2015, with the number of issued warrants in

[557] This table can be found at the AO website: https://www.uscourts.gov/statistics-reports/wiretap-report-2018. Visited at 03. 05. 2020. The late reports for the number of wiretaps in 2018 have not been released.

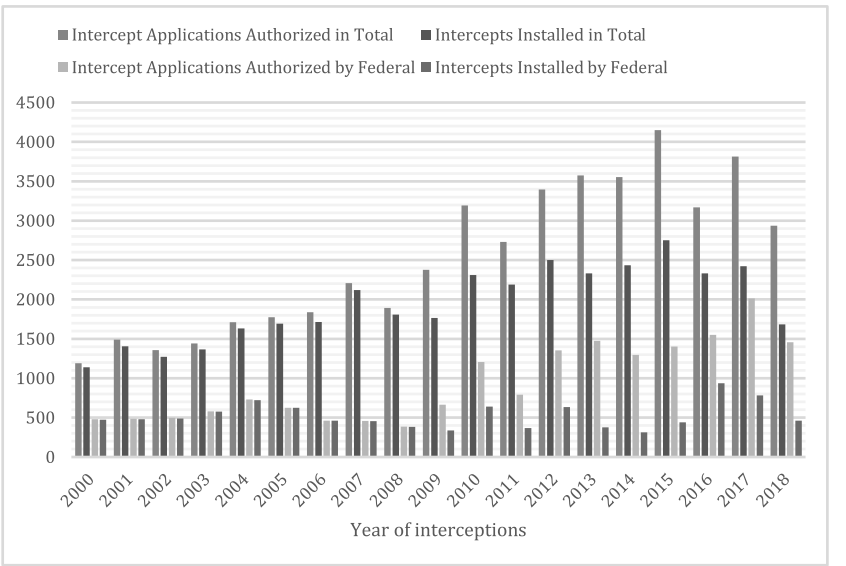
2015 being twice as high as in 2008. By local jurisdictions, applications in California alone constituted 41 % of all applications approved by state judges in 2015.[558] California und New York consistently have the most authorized warrants among states.

2. Rate of Installed Intercepts

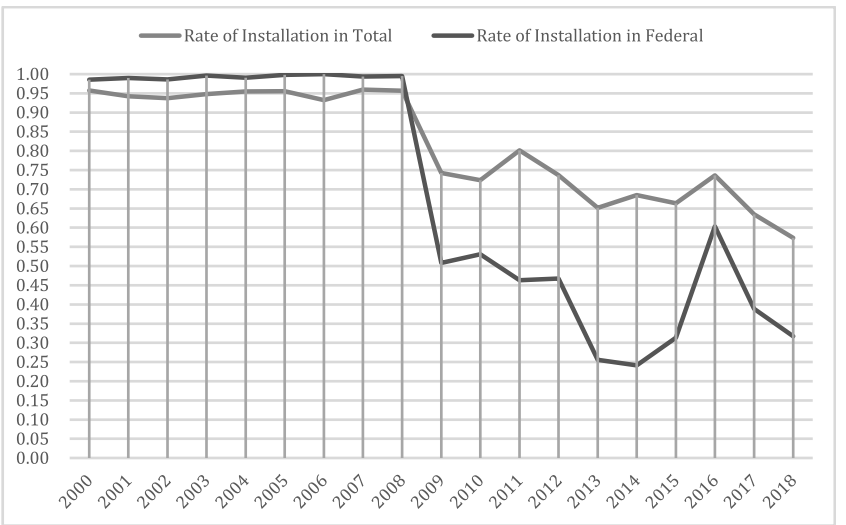
Table 2
The Number and Rate of Installations from 2000 to 2018

	Intercepts' Applications Authorized in Total	**Intercepts Installed in Total**	**Intercepts' Applications Authorized by Federal**	**Intercepts Installed by Federal**	**Rate of Installation in Total**	**Rate of Installation in Federal**
2000	1190	1139	479	472	0.96	0.99
2001	1491	1405	486	481	0.94	0.99
2002	1358	1273	497	490	0.94	0.99
2003	1442	1367	578	576	0.95	1.00
2004	1710	1633	730	723	0.95	0.99
2005	1773	1694	625	624	0.96	1.00
2006	1839	1714	461	461	0.93	1.00
2007	2208	2119	457	454	0.96	0.99
2008	1891	1809	386	384	0.96	0.99
2009	2376	1764	663	337	0.74	0.51
2010	3194	2311	1207	641	0.72	0.53
2011	2732	2189	792	367	0.80	0.46
2012	3395	2501	1354	633	0.74	0.47
2013	3576	2331	1476	377	0.65	0.26
2014	3554	2433	1297	313	0.68	0.24
2015	4148	2753	1403	440	0.66	0.31
2016	3168	2332	1551	936	0.74	0.60
2017	3813	2421	2013	782	0.63	0.39
2018	2937	1684	1457	462	0.57	0.32

[558] https://www.uscourts.gov/statistics-reports/wiretap-report-2015, visited at 08. 05. 2020.



Graph 2: Intercept Applications Authorized and Installed from 2008 to 2018



Graph 3: The Rate of Installations from 2008 to 2018

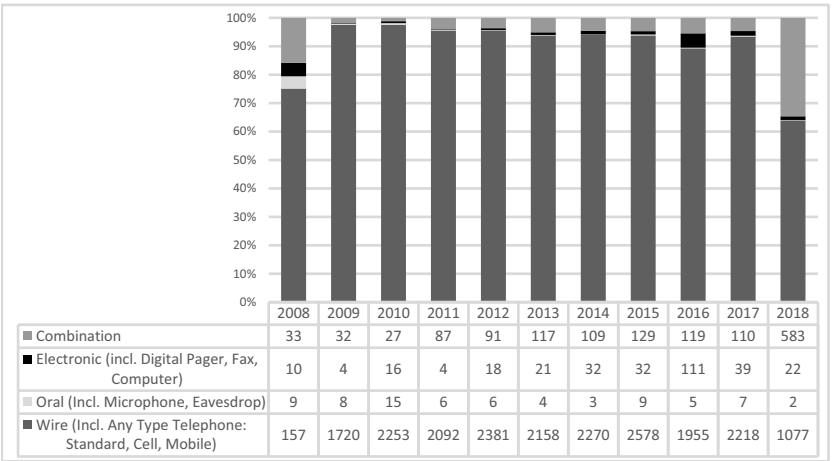
Due to the fact that the practice of implementing warrants underwent an obvious shift since 2009, statistics from 2000 to 2018 are presented here in order to demonstrate this change more clearly. Both Graph 2 and Graph 3 show that before 2009 there was a high rate of implementation of issued warrants. This rate was no less than 0.93 in the whole of the U.S. and was either 0.99 or 1.00 at the Federal level. Almost all issued warrants were implemented before 2009. However, the implementation rate dropped dramatically since 2009.

Graph 2 shows that the number of issued warrants increased since 2009, but the number of implemented warrants remained stable.[559] Although it rose again in certain years, such as 2016, the rate never managed to reach 0.9 again. This means that since 2009, a large number of issued warrants were actually not implemented. The correlation between the numbers of issued warrants and of intercepts implemented at the Federal level and across the U.S. was $r \approx 1.00$ prior to 2009 but fell to $r = 0.60$ at the Federal level and $r = 0.84$ across the U.S. One possible explanation is that the number of installed intercepts is influenced by other factors. The limited human and financial resources of law enforcement might in part explain the discrepancy between the number of issued and implemented warrants.[560]

[559] The standard deviation (SD) of the number of issued warrants across the whole of U.S. from 2009 to 2018 is 496.8, while the SD of the number of installed intercepts is 308.4. At Federal level, the SDs are 361.7 and 199.6 correspondingly. In both situations, the number of issued warrants is more dispersed than the number of installations.

[560] See Section 1. e) cc), Chapter IV, Part I. The statistics on costs are discussed in Section 6, Chapter VI, Part I.

3. Types of Surveillance Used



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Combination	33	32	27	87	91	117	109	129	119	110	583
Electronic (incl. Digital Pager, Fax, Computer)	10	4	16	4	18	21	32	32	111	39	22
Oral (Incl. Microphone, Eavesdrop)	9	8	15	6	6	4	3	9	5	7	2
Wire (Incl. Any Type Telephone: Standard, Cell, Mobile)	157	1720	2253	2092	2381	2158	2270	2578	1955	2218	1077

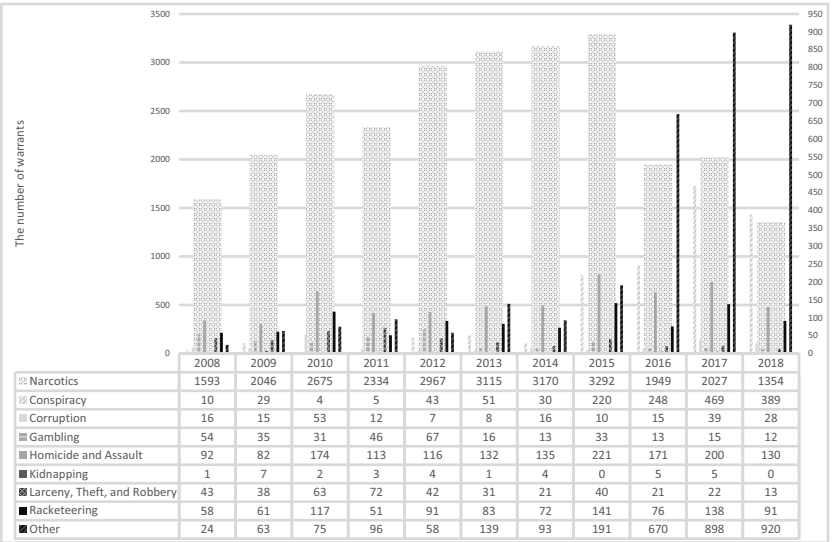
Graph 4: Use of Different Forms of Surveillance[561]

Graph 4 demonstrates that wiretapping is used more widely than other types of surveillance, while oral surveillance is undertaken only in exceptional cases. A majority of cases involve cellular telephones. In 2018, a total of 96 % of all authorized wiretaps concerned portable devices, including cell phone communications, text messages and software applications.[562]

[561] Statistics resource: https://www.uscourts.gov/statistics-reports/analysis-reports/wire-tap-reports. Visited at 05. 05. 2020.

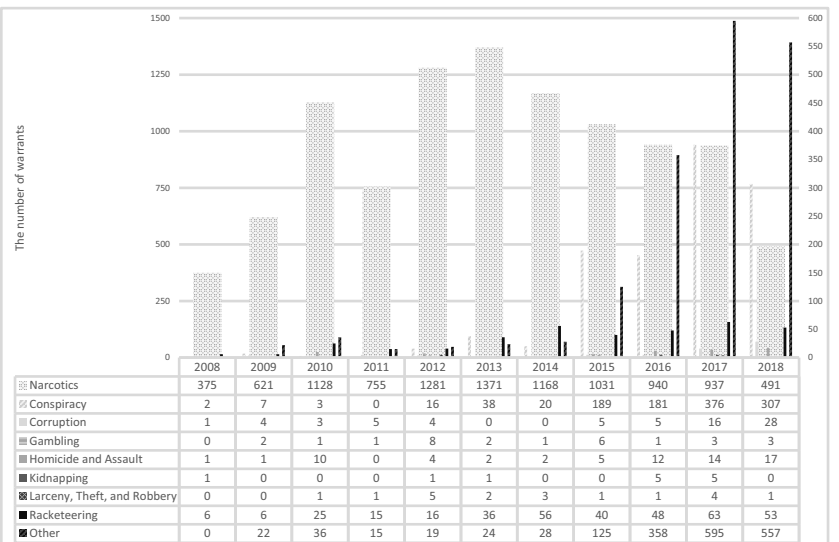
[562] https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports, visited at 05. 05. 2020.

4. Major Offenses Named in Warrants



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Narcotics	1593	2046	2675	2334	2967	3115	3170	3292	1949	2027	1354
Conspiracy	10	29	4	5	43	51	30	220	248	469	389
Corruption	16	15	53	12	7	8	16	10	15	39	28
Gambling	54	35	31	46	67	16	13	33	13	15	12
Homicide and Assault	92	82	174	113	116	132	135	221	171	200	130
Kidnapping	1	7	2	3	4	1	4	0	5	5	0
Larceny, Theft, and Robbery	43	38	63	72	42	31	21	40	21	22	13
Racketeering	58	61	117	51	91	83	72	141	76	138	91
Other	24	63	75	96	58	139	93	191	670	898	920

Graph 5: Major Offenses Named in Warrants across the U.S. from 2008 to 2018



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Narcotics	375	621	1128	755	1281	1371	1168	1031	940	937	491
Conspiracy	2	7	3	0	16	38	20	189	181	376	307
Corruption	1	4	3	5	4	0	0	5	5	16	28
Gambling	0	2	1	1	8	2	1	6	1	3	3
Homicide and Assault	1	1	10	0	4	2	2	5	12	14	17
Kidnapping	1	0	0	0	1	1	0	0	5	5	0
Larceny, Theft, and Robbery	0	0	1	1	5	2	3	1	1	4	1
Racketeering	6	6	25	15	16	36	56	40	48	63	53
Other	0	22	36	15	19	24	28	125	358	595	557

Graph 6: Major Offenses Named in Warrants Issued by Federal Courts from 2008 to 2018

Graph 5 and Graph 6 show that drug offenses were the most prevalent offenses investigated by surveillance from 2008 to 2018 across the whole of the U.S., and from 2008 to 2017 at the Federal level.[563] Taking the year 2018 as an example, 46 % of all surveillance warrants issued across the whole of the U.S. cited narcotics as the most serious offense under investigation. Warrants citing narcotics combined with other offenses, which includes offenses related to drugs, accounted for 77 % of all issued warrants. As the second-most frequently cited crime, conspiracy was named in 13 % of warrants. This was followed by homicide and assault, which were cited in around 4 % of warrants in 2018.[564]

5. Duration and Extension

Table 3
Duration and Extension of Warrants across the Whole of the U.S.

	Number of Installed Warrants	Number of Extensions	Number of Extensions per Warrant	Avg. Length (in Days)		Total Number of Days in Operation	Avg. Days Operation per Warrant
				Original Authorization	Extensions		
2008	1809	1266	0.70	29	29	73,509	40.6
2009	1764	1627	0.92	29	28	73,799	41.8
2010	2311	1925	0.83	29	29	93,078	40.3
2011	2189	1777	0.81	29	29	91,240	41.7
2012	2501	1932	0.77	30	29	98,562	39.4
2013	2331	2129	0.91	30	30	92,788	39.8
2014	2433	1532	0.63	30	30	81,892	33.7
2015	2753	3297	1.20	30	30	118,583	43.1
2016	2332	2096	0.90	30	30	102,108	43.8
2017	2421	2369	0.98	30	30	98,749	40.8
2018	1684	1355	0.80	30	30	62,681	37.2
Total	24,528	21,305	0.87	-	-	986,989	40.2

[563] Only the most serious criminal offense listed on a warrant is included in these statistics.

[564] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 06. 05. 2020.

Table 4
The Duration and Extension of Warrants at the Federal Level

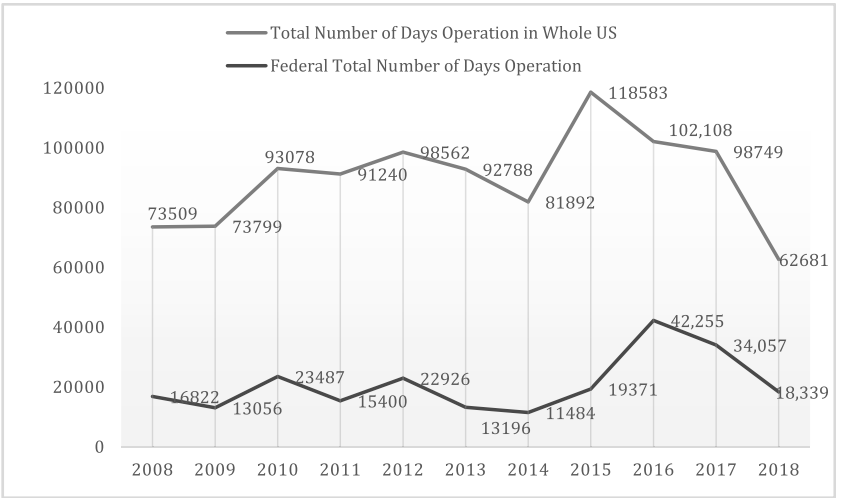
	Number of Installed Warrants	Number of Extensions	Number of Extensions per Warrant	Avg. Length (in Days)		Total Number of Days in Operation	Avg. Days Operation per Warrant
				Original Authorization	Extensions		
2008	384	271	0.71	30	30	16,822	43.8
2009	337	387	1.15	30	30	13,056	38.7
2010	641	543	0.85	30	30	23,487	36.6
2011	367	403	1.10	30	30	15,400	42.0
2012	633	521	0.82	30	30	22,926	36.2
2013	377	668	1.77	30	30	13,196	35.0
2014	313	493	1.58	30	30	11,484	36.7
2015	440	784	1.78	30	30	19,371	44.0
2016	936	1007	1.08	30	30	42,255	45.1
2017	782	1075	1.37	30	30	34,057	43.6
2018	462	584	1.26	30	30	18,339	39.7
Total	5,672	6,736	1.19	-	-	230,393	40.6

Federal and state law limits the period of surveillance under an original order to 30 days. This period, however, can be prolonged by one or more extensions, which require a new authorization from a judge.[565] Table 3 and Table 4 show that in most years warrants, including extensions, were authorized for 30 days. According to the Wiretap Report for 2018, the longest Federal intercepts that took place in 2018 were implemented in a bribery investigation. A warrant with eight extensions, a 270-day wiretap, was issued by the Northern District of Illinois (IL-N).[566]

Table 3 and Table 4 show a clear decrease in the number of extensions in 2018 compared to 2017. This reduction might in part be the consequence of the introduction of new technology that facilitates the matching of extensions arising from the same intercept order which prevents extensions from being counted multiple times.[567]

According to the statistics for the years 2008 to 2018, Federal courts issued more extensions than state courts (1.19: 0.87 extensions per warrant). The average number of days that the surveillance was in operation per warrant was roughly the same across both the Federal and state courts, approximately 40 days per warrant.

[565] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 07.05.2020.
[566] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 07.05.2020.
[567] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 07.05.2020.



Graph 7: The Number of Days in Operation

Graph 7 shows the overall length of operations of surveillance between 2015 to 2018 at the Federal level and across the U.S. The unusual length of operations in 2015 is related to the high number of warrants issued in that year. In addition, Queens County, New York, contributed to this high number with a racketeering investigation in which one original warrant was extended 30 times to implement a 913-day wiretap.

6. Cost

As mentioned above, implementing a surveillance warrant in the U.S. is expensive and is described as a "manpower killer".[568] Therefore, the cost of implementing a warrant plays an important role in applications and the number of warrants actually implemented.

The cost depends on the length of the intercept and the number of days in operation. According to the Wiretap Report for 2018, the most expensive state wiretap occurred in the State of New York, where costs for a 365-day wiretap totaled $3,331,169. The most expensive Federal wiretap completed in 2018 was in the Eastern District of California with a 90-day wiretap for a murder investigation, which cost $1,192,390.[569] The implementation of Federal warrants costs more on average than implementing state warrants.

[568] See Section 2. c) cc), Chapter IV, Part I.

[569] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 08. 05. 2020.

The correlation between the number of implemented warrants and the average cost per warrant for the whole of the U.S. is -0.2. This negative correlation means that the more warrants were installed, the lower was the average cost per warrant. This suggests that the total cost per year has an influence upon how many warrants are implemented. This conclusion is also supported by the average number of intercepts per warrant and the number of implemented warrants, as shown in Table 5 Rate of Incriminating Intercepts per Installed Warrant. The correlation between the average number of intercepts per implemented warrant and the number of implemented warrants is -0.4, which means that the more warrants were implemented, the fewer intercepts per warrant occurred. Since the approximate total cost per year varies greatly between 2008 and 2018, however, this influence is limited. This influence is even more limited at the Federal level.

7. Efficiency of Surveillance

Surveillance is an intrusion into privacy and at the same time an expensive investigatory method. Its use is worthwhile only if it helps to discover crime[570] and provides incriminating evidence. The NWC Report defined the efficiency of surveillance by "whether court-ordered surveillance in fact uncovered criminal …activities which were sufficiently significant to justify the costs involved".[571] The efficiency of surveillance, however, can be evaluated using various criteria. The Wiretap Reports present statistics on incriminating information, numbers of persons arrested and of those convicted based on intercepts. They reflect the efficiency of surveillance from different perspectives.

[570] NWC Report, at 125.

[571] *Id.* at 135. If it is defined in a broader way, its ability to prevent of future crime should also be included. It is difficult, however, to evaluate the effectiveness of electronic surveillance from this perspective, since there are no statistics of crimes, which are yet to be committed.

a) Rates of Incriminating Information

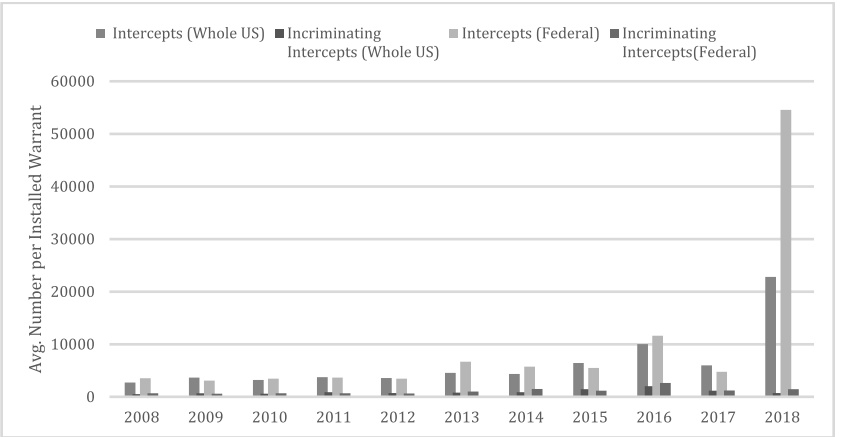
Table 5
Rate of Incriminating Intercepts per installed warrant

	Average Number per Order when installed					
	Intercepts (Whole U.S.)	Intercepts Providing Incriminating Information (Whole U.S.)	Rate of Incriminating Intercepts	Intercepts (Federal)	Intercepts Providing Incriminating Information (Federal)	Rate of Incriminating Intercepts
2008	2,707	514	0.19	3,547	674	0.19
2009	3,673	688	0.19	3,077	573	0.19
2010	3,199	603	0.19	3,463	655	0.19
2011	3,716	868	0.23	3,648	654	0.18
2012	3,584	703	0.20	3,440	642	0.19
2013	4,558	811	0.18	6,673	992	0.15
2014	4,348	886	0.20	5,724	1,491	0.26
2015	6,422	1,454	0.23	5,504	1,180	0.21
2016	10,021	2,034	0.20	11,598	2,652	0.23
2017	5,989	1,178	0.20	4,752	1,199	0.25
2018	22,788	720	0.03	54,555	1,467	0.03

Leaving aside the unusually low rate of intercepts generating incriminating information in 2018, the rate is around 0.2 from 2008 to 2017. The total rate of incriminating intercepts from 2008 to 2017 is 0.20 across the whole of the U.S. and 0.21 at the Federal level.[572] If the statistics in 2018 are included, this rate decreases to 0.16 and 0.13 respectively.

The unusually low rate in 2018 is more obvious in Graph 8. The Wiretap Report in 2018 reported that 9,208,906 messages over 120 days were intercepted during a narcotics investigation in the Southern District of Texas. Given such an unusual situation, one should disregard the statistics from 2018, as this will give a more reliable picture of normal practice. This means that normally 20 % of intercepted communications generate incriminating information.

[572] The total rate of incriminating intercepts from 2008 to 2017 = The total number of incriminating intercepts from 2008 to 2017/the total number of intercepts from 2008 to 2017.



Graph 8: Avg. Number of Intercepts and Incriminating Intercepts per Implemented Warrant across the Whole of the U.S. and at Federal Level

b) Number of Arrests and Convictions

It is common for surveillance warrants to involve large-scale criminal investigations that last longer than one year. The subsequent trials may also take years. Arrests and convictions resulting from a surveillance warrant often do not occur within the same year in which the intercepts were first reported.[573] Therefore the number of people recorded as being arrested and convicted each year is not a true reflection of the efficiency of intercepts.

Under 18 U.S.C. § 2519(2), supplemental reports must be submitted to record additional data from intercepts reported in prior years. In general, however, supplementary reports do not alter the overall picture of the type of surveillance used, the percentage of major offenses named in the warrant, or the average cost per warrant, because they do not greatly amend the data concerning these issues. The large volume of statistics involved in the analysis also has the effect of ironing out any minor discrepancies caused by missing data. The data regarding the number of people arrested and convicted in the original reports, however, is far from complete. For instance, the supplementary report for 2018 reported a total of 7,932 arrests. There were 2,295 convictions in 2018 reported subsequently and based on intercepts conducted earlier.

Table 6 reflects statistics contained in the Wiretap Report of 2018. It contains the number of persons arrested and convicted in the original reports and those reported in later years. According to the original statistics in the Wiretap Report of 2018, only the

[573] https://www.uscourts.gov/statistics-reports/wiretap-report-2018, visited at 10. 05. 2020.

data for the years 2008 and 2009 do not show an increase in the number of people arrested and convicted as a consequence of intercepts. This shows that some cases took ten years to reach a final conviction. Therefore, only the data prior to 2009 has a high degree of accuracy. Table 6 shows the statistics from 2000 to 2009.

The number of authorized warrants and the number of persons arrested have a strong correlation (r=0.87). The number of persons arrested and convicted also has a strong correlation (r=0.90). This implies that the more warrants were authorized, the more persons were arrested as a consequence of intercepts. The more persons were arrested, the more persons were convicted.

Table 6
Number of Persons Arrested and Convicted Resulting from Intercepts Installed

Year of Intercepts	Number of Authorized Warrants	Total Number of Intercepted Persons	Number of Persons Arrested Till 2018	Percent of Persons Arrested among Persons Intercepted (%)	Number of Persons Convicted Till 2018	Percent of Persons Convicted among Persons Arrested (%)	Avg. Number of Persons Arrested per Authorized Warrant	Avg. Number of Persons Convicted per Authorized Warrant
2000	1190	2,380,000	6009	0.25	3062	51.0	5.05	2.57
2001	1491	2,983,491	5607	0.19	2947	52.6	3.76	1.98
2002	1358	2,718,716	4651	0.17	2321	49.9	3.42	1.71
2003	1442	2,888,326	5705	0.20	2523	44.2	3.96	1.75
2004	1710	3,426,840	6734	0.20	2841	42.2	3.94	1.66
2005	1773	3,554,865	7382	0.21	3643	49.3	4.16	2.05
2006	1839	3,689,034	7257	0.20	3256	44.9	3.95	1.77
2007	2208	4,431,456	8310	0.19	3630	43.7	3.76	1.64
2008	1891	3,797,128	7,913	0.21	3,622	45.8	4.18	1.92
2009	2376	4,773,384	7,952	0.17	3,369	42.4	3.35	1.42
Total	17,278	34,643,240	67,520	0.19	31,214	46.2	3.91	1.81

VII. Conclusions

The "reasonable expectation of privacy" is the fundamental criterion developed by the U.S. Supreme Court to determine the reach of the 4th Amendment. Since the *Katz* decision, interceptions of wire and oral communications are regarded as a form of search and seizure; they are consequently subject to the "reasonable expectation of privacy" test, which determines whether a warrant is required for certain interceptions. This criterion has replaced the traditional trespass theory, which was based

on property rights and had limited infringements on the 4th Amendment to physical trespass. The "reasonable expectation of privacy" test consists of a two-pronged requirement based on subjective and objective perspectives, i. e., "an actual (subjective) expectation of privacy" and the determination of what "society is prepared to recognize as 'reasonable'".[574] This doctrine, however, is not devoid of problems. The key problem is to determine what kind of expectation of privacy is justified and should be protected. Post-*Katz* cases show that courts tend to mix up the individual's subjective expectation with society's reasonable belief. Moreover, some courts have required defendants to take all possible measures to prevent surveillance by any type of technology and to prevent any exposure to the public to demonstrate their expectation of privacy. This leaves citizens helpless in the fight against invasions of privacy by technologically advanced state agencies. As a result, the protection afforded by the "reasonable expectation of privacy" shrinks along with the development of technology. Ultimately, citizens will lose this "war" because the more advanced technology is always in the hands of public agencies. Furthermore, the U.S. Supreme Court introduced the "society" element to evaluate the justification of the expectation of privacy. This requires courts to determine citizens' opinions. This is, however, an almost impossible task. Empirical studies have shown that the determinations made by courts sometimes differ markedly from what most citizens actually think.[575] It is also questionable whether it is proper to require courts to follow majority opinion. Courts that do so might fail in their task to prevent the tyranny of the majority.

In the *Kyllo* case,[576] the formula "minimal expectation of privacy" has been suggested as a possible alternative that might resolve problems of the "reasonable expectation of privacy" doctrine. The Supreme Court thereby tried to block the continuing invasion of technology upon privacy, but its effect is limited. A "minimal expectation of privacy" could create a clearly defined sphere where people could enjoy their privacy regardless of what technological surveillance may be available. This approach would protect people from warrantless surveillance under the "reasonable expectation of privacy" doctrine. If the police obtain a judicial warrant, however, they can install surveillance anywhere as directed in the warrant. Since almost all applications are approved by courts, it would not be difficult for police to obtain a warrant. Given this situation, "the minimal expectation of privacy" rule offers only very limited additional protection to the privacy of individuals.

Title III incorporates the "reasonable expectation of privacy" doctrine. In addition, this statute provides detailed procedural rules for applying for and issuing a judicial warrant, the contents of a warrant, the post-implementation activities, etc. These rules were set up to reduce the abuse of surveillance powers by improving the transparency of surveillance activities. The warrant requirement guarantees prior

[574] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[575] See Section 4. b) bb), Chapter I, Part I.

[576] *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

judicial control unless an exception applies. The comprehensive requirements for the contents of a warrant, such as probable cause and the duration directive, make it possible for defense lawyers to seek suppression of any evidence obtained in violation of the warrant. The notice requirement serves the same purpose. The minimization requirement and the progress report system aim at keeping the interception of conversations to a minimal level. In practice, however, some requirements provided for in *Title III* are not complied with and are only reviewed formally, not substantially. For instance, the last resort requirement can be fulfilled by a simple declaration that other investigative measures are likely to be unsuccessful or too dangerous. As a result, almost all applications have been approved in past years. The effect of judicial control on surveillance provided for in *Title III* is therefore questionable; however, the detailed statutory requirements may well have a preventive effect on prosecutors and make them refrain from applying for warrants unless they think that all requirements can be met. Congress, in any event, when passing *Title III* made a reasonable effort at balancing the individual's right to privacy with the need to combat crime.

Another important issue is the admissibility of evidence from surveillance. The general exclusionary rules are applicable to illegally obtained surveillance evidence. In a series of landmark cases, such as *Weeks, Mapp* and *Wolf v. Colorado*, the U.S. Supreme Court developed the exclusionary rule and the famous "fruit of the poisonous tree" doctrine.[577] This doctrine requires the exclusion of evidence derived from illegally obtained direct evidence. In accordance with these rules, if a communication was intercepted illegally, this communication is in principle not admissible in court, nor is any further evidence derived from this communication admissible. This judge-made exclusionary rule is designed to deter unreasonable searches and seizures; however, opponents argue that the exclusionary rule goes too far in protecting offenders and disregards the interests of victims and society.[578]

In addition to this general rule, *Title III* contains its own exclusionary rule, which prohibits the use of evidence obtained by illegally intercepted wire or oral communications and sets forth the procedure and grounds for a suppression motion. 18 U.S. Code § 2515 excludes the contents of illegally intercepted communications and evidence derived from these communications. In determining the consequences of a failure to comply with *Title III*, courts make a distinction between central and non-central provisions in *Title III*. Only a violation of a central provision leads to exclusion. In case law, the crime catalogue, the probable cause requirement, the duration directive, the termination directive, and the minimization requirements have all been deemed to be "central" provisions. If a central provision has been violated, the consequence normally is total exclusion of the communication in question, yet sometimes only those parts of the communication that are affected by the violation

[577] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, Chapter 6; *Cammack*, in: Thaman (ed.), Exclusionary Rules in Comparative Law, 2013, 8 – 13.

[578] *Lippman*, Criminal Procedure, 2020, 386.

are excluded. For example, if the police in good faith failed to minimize surveillance, only those conversations that should not have been recorded will be excluded; the same applies if surveillance extended to persons or locations not covered by the warrant.[579]

Concerning communications intercepted by private persons, some courts have suggested a "clean hands" exception to the exclusionary rule; when law enforcement officers played no role in the illegal interception conducted by private parties, suppression was not necessary. This exception, however, has not been adopted by a majority of courts and legal writers.[580]

In sum, electronic surveillance by law enforcement officers is regulated both at the constitutional level by the 4th Amendment interpreted through the "reasonable expectation of privacy" doctrine and at the statutory level by *Title III*. The former determines what surveillance constitutes search and seizure while the latter provides procedural guarantees for surveillance practice.

The fact that AO releases comprehensive annual statistics on electronic surveillance allows this study to have an overall view of the practice of surveillance in the U.S. According to these statistics, drug-related offenses are cited most frequently as the triggering offenses in surveillance warrants, and surveillance of wire communications is used more often than that of oral communications. As to the efficiency of surveillance measures for producing incriminating information and evidence, 20 % of all intercepted communications were incriminating. In addition, from 2000 to 2009, one authorized warrant led to an average of 3.91 persons being arrested and 1.81 persons being convicted. If these statistics are merely evaluated according to the effect of surveillance on fighting crime, surveillance can be regarded as productive since each warrant can lead to arrest and conviction. Due to the lack of a standard, however, it is hard to draw a conclusion on whether surveillance is efficient when its results are balanced against its costs and the infringement upon privacy.

The U.S. legislature made an effort at protecting privacy by establishing procedural requirements on surveillance, such as the requirements on warrants, on minimization, sealing, giving notice, etc. These measures deter law enforcement officers from massive abuse of surveillance and increase the transparence of surveillance. However, one problem of the U.S. system is that surveillance can also be implemented without a warrant if there is no "reasonable expectation of privacy".

[579] For example, *U.S. v. Renzi*, 692 F. Supp. 2d 1136 (D. Ariz. 2010).

[580] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.44.

Part II

Technological Surveillance in the Federal Republic of Germany

Since offenders make much use of new technologies, the traditional way to investigate crimes does not work any longer. Moreover, criminal organizations and terrorism are regarded as a new threat to public security. As a result, despite the infringement upon privacy caused by technological surveillance measures, *the German Criminal Procedure Code* (hereafter referred to as StPO) legitimates several surveillance measures, among them telecommunication surveillance, telecommunication traffic data, and acoustic communication surveillance, which includes the interception of oral communications conducted at home, i. e., "großer Lauschangriff," and in public areas. These measures will be discussed in the following chapters.

I. Telecommunication

1. Constitutional Protection – Art. 10 German Basic Law

The term "Privatsphäre" ("private sphere") cannot be found in the text of the German Basic Law (Grundgesetz, hereafter referred to as GG). The right to privacy, however, has been inferred from several provisions of GG. This right is interpreted as an integral part of "Menschenwürde" ("human dignity") in Art. 1 GG and "Recht auf die freie Entfaltung seiner Persönlichkeit" ("the right to the free development of the personality") in Art. 2 GG; moreover, it is also covered by special provisions in certain areas, especially Art. 10 on protecting the privacy of communications and Art. 13 on protecting the home. The most relevant constitutional article for telecommunication is Art. 10 GG regarding the protection of the privacy of letters, the mail, and distance-communication.[581] Moreover, the Federal Constitutional Court (Bundesverfassungsgericht, hereafter referred to as BVerfG) has recognized Art. 1 I

[581] § 10 GG: "(1) The secrecy of letters, posts and distant communications is inviolable. (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

GG, the absolute protection of human dignity,[582] and Art. 2 I GG, the right to free development of the personality,[583] as the constitutional basis of the telecommunication protection.[584]

a) History

Art. 10 I GG protects different forms of communication. Among them, the protection of the privacy of letters has the longest history dating back to Roman law. The privacy of letters and mails began to gain importance during the French revolution when the privacy of mails was protected from surveillance by the government.[585] In Germany, the *Verfassung des Kurfürstentums Hessen* in 1831 was the first constitution to recognize the privacy of letters and mails.[586] Its § 38 provided: "The privacy of letters shall not be violated. The intentional direct or indirect infringement upon such privacy by mail-management shall be punished under criminal law". § 142(1) *Frankfurter Paulskirchenverfassung* in 1849 issued by the National Assembly provided: "The privacy of letters is guaranteed." Furthermore, § 33(1) *Verfassungsurkunde für den Preußischen Staat* in 1850stated: "The privacy of letters is inviolable." Different from § 38 *Verfassung des Kurfürstentums Hessen*, both § 142(2) *Frankfurter Paulskirchenverfassung* and § 33(2) *Verfassungsurkunde für den Preußischen Staat* added exceptions: "The necessary limitations for criminal investigations and in case of war shall be regulated through legislation." The constitution documents of the later part of the 19th century, i. e., *Verfassung des Norddeutschen Bundes* of 1867 and *Verfassung des Deutschen Reiches* of 1871, however, did not contain chapters about fundamental rights, so there was no guarantee of the privacy of letters or mail provided by these constitutions. At that time, the privacy of letters and mail was protected by separate legislation. As a reflection of the development of telegram technology in 19th century, there were rules in these two constitutional documents about the management of the telegram system. The first law about telegrams, *Gesetz über das Telegrafenwesen*[587], was passed in 1892. § 8 of this

[582] § 1(1) of GG: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority."

[583] § 2(1) GG: "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law."

[584] *Weigend*, Using the Results of Audio-surveillance as Penal Evidence in the Federal Republic of Germany, Stanford Journal of International Law 24 (1988), 21, 23.

[585] The legal text can be found in Loi des 10 – 14 août 1790, Collection complète des Lois, Décrets, Ordonnances, Réglements, avis du Conseil d'État de 1788 à 1830 inclusivement, par ordre chronologique) par J.B. Duvergier, Tome 1er, 2e éd., 1834, 277. The development of the privacy of letters can be found in: Chauveau/Hélie, Théorie du Code Pénal, Band 2, 1837, S. 211.

[586] *Sievers*, Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, 2003, S. 103.

[587] Deutsches Reichsgesetzblatt Band 1892, Nr. 21, S. 467 – 470.

legislation offered parallel protection to the secrecy of telegrams as to letters and mail.[588]

The second part of *Weimarer Reichsverfassung (WRV)* of 1919 listed the fundamental rights of individuals. Given the development of telephones in the 20th century, Art. 117 WRV expanded its protection to conversations by telephone: "The privacy of letters, as well as mail, telegram and telephone conversations is inviolable. Exceptions are only allowed by legislation of the *Reich*".[589] The enumeration of communication methods showed the attempt to protect all kinds of communication. This way of formulating the protection influenced the current Art. 10 GG.[590]

Art. 117 WRV was suspended by Art. 1 of *Verordnung des Reichspräsidenten zum Schutz von Volk und Staat* (*Order of the Empire's President to Protect the People and the State*; RGBl. I 1933, S. 83) issued by the National-Socialist government in Feb. 1933. Art. 1 provided: "Article 117 of Verfassung des Deutschen Reichs is suspended until further notice. The intervention on the secrecy of letters, mail, telegrams and telephone conversations is allowed within certain legal limits." Taking advantage of this Article, Gestapo and police adopted massive and systematic interceptions on telephones and telegrams of political opponents.[591]

Shortly after the Second World War, deputies from the Western occupied zones began to work on a constitutional document for West Germany. As a result, the so-called *Herrenchiemseer Entwurf (the Draft of Herrenchiemsee)* was published in August 1948. Art. 11 of this document provided: "(1) The privacy of letters, mail and telephone is inviolable. (2) Exceptions are allowed only upon judicial proceedings in situations and forms provided by law."[592] The drafters of the GG in 1949 decided to simplify this article to only one paragraph: "The privacy of letters as well as of the mail and telecommunication is inviolable. Restrictions may be ordered only pursuant to a law."

The current formulation of Art. 10 GG dates from June 1968. At the same time, *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*[593] (*Law on the Limitation of the Privacy of Letters, Mail and Telecommunication*; hereafter referred to as G10) entered into force. The explanation in the draft of G10 made it

[588] *Aubert*, Fernmelderecht, 2. Aufl. 1962, S. 45.

[589] *Huber*, Dokumente zur deutschen Verfassungsgeschichte, Band III, 1990, 146.

[590] Vgl. *Durner*, in: Maunz/Dürig, GG, 2020, Art. 10, Rn. 14.

[591] *Pagenkopf*, in: Sachs, GG, 9. Aufl., 2021, Art. 10, Rn. 2; *Durner*, in: Maunz/Dürig, GG, 2020, Art. 10, Rn. 15.

[592] "(1) Das Brief-, Post- und Fernmeldegeheimnis ist unverletzlich. (2) Ausnahmen sind nur in einem Gerichtsverfahren in den vom Gesetz vorgeschriebenen Fällen und Formen zulässig." Compared to Art. 117 WRV, this article used "Fernmelde" (distance-communication), instead of "Telegraphen- und Fernsprech". *Pagenkopf*, in: Sachs, GG, 9. Aufl., 2021, Art. 10, Rn. 2.

[593] BGBl. I S. 1254, 2298; 2007 I S. 154.

clear that there were two main purposes of the modification to Art. 10 GG.[594] First, the former Art. 10 GG and the related articles in StPO allowed telecommunication surveillance only for the purpose of investigating committed crimes. This was, however, not sufficient to protect security and freedom from danger. Secondly, after the Second World War, the Allied Forces intercepted mail and telecommunications to protect the security of West Germany. *Deutschlandvertrag*, signed in 1952, declared that the Allied Forces should hand over the duty of safeguarding West Germany to the Federal Republic of Germany when a competent agency for surveillance was established. G10 and the new Art. 10 GG established such an agency. Art. 1 of G10 explained its function in protecting security: "To prevent from danger threatening the basic order or the existence of free democracy, or to the security of the Republic or one state … it is legitimate to place telecommunications under surveillance and to record them."

b) The Personality Right ("Allgemeines Persönlichkeitsrecht")

aa) The Right to a Private Sphere and the "Core Area of Privacy"

Art. 2 I GG protects not only the freedom but also the development of the personality.[595] Moreover, the BVerfG has defined a general personality right ("allgemeines Persönlichkeitsrecht") by combining Art. 2 I and Art. 1 I GG.[596] Although the right to privacy does not appear in the text of GG, the BVerfG has made it clear that the general personality right serves to protect individuals from state infringement and creates a private area for them where they are left alone and can make their own decisions.[597]

As early as in 1957, the BVerfG stated that the constitution preserves an area of private life ("eine Sphäre privater Lebensgestaltung") for every citizen, i. e., the core untouchable area of human freedom.[598] In the so-called "Tonband-Beschluss", the BVerfG divided the private area into two spheres: one is the core area of privacy, i. e., "Kernbereich privater Lebensgestaltung"; and the other is the private area which can be invaded by the public authority under certain preconditions.[599] In a case con-

[594] BT-Drucks. V/1880, 6.

[595] *Rixen*, in: Sachs, GG, 9. Aufl., 2021, Art. 2, Rn. 59.

[596] BVerfGE 54, 148, 153; 27, 1. 6.

[597] BVerfGE 27, 1. 6; 34, 269, 282.

[598] BVerfGE 6, 32, 41 ("Hieraus ergibt sich, daß dem einzelnen Bürger eine Sphäre privater Lebensgestaltung verfassungskräftig vorbehalten ist, also ein letzter unantastbarer Bereich menschlicher Freiheit besteht, der der Einwirkung der gesamten öffentlichen Gewalt entzogen ist.") The case itself focused on the behavior freedom ("Handlungsfreiheit").

[599] BVerfGE 34, 238, 245, 248 ("Wann eine heimliche Tonbandaufnahme den schlechthin unantastbaren Bereich privater Lebensgestaltung berührt und wann sie lediglich den unter bestimmten Voraussetzungen dem staatlichen Zugriff offenstehenden Bereich des privaten Lebens betrifft, läßt sich nur schwer abstrakt umschreiben."). Another category is also defined by the BVerfG, but falls out of the private area, more belongs to the public information, such as

cerning a diary, the BVerfG developed a three-factors test to decide whether certain circumstances or information belong to the core area of privacy: (1) whether the person has the will to keep the information secret; (2) whether the information is highly personal, and (3) whether and to what extent the information interferes with the personal sphere of other persons or with the interests of society.[600] The BVerfG noted that human beings necessarily entertain social relations, even in the core area of personality. Therefore, the question whether a circumstance belongs to the "core area of privacy" does not depend upon whether a social relation exists but in what form and to what degree the spheres of others are affected.[601] If the recording has a direct relation with a crime, such as the description of a criminal plan or a crime committed, it will not be part of the "core area of privacy".[602]

The concept of "core area of privacy" was further extensively discussed in a judgment concerning the acoustic surveillance of a home, which generally is part of the "core area of privacy".[603] According to this decision, any person's ability to freely express his inner processes, such as emotions, feelings, thoughts, opinions, highly personal experience, as well as the expression of his sexuality, without fear of surveillance by public authority is essential for the free development of the person-

---

an announce in the train station. 34, 238, 247 ("Zwar gibt es Fallgruppen, in denen auch eine ohne Wissen des Sprechenden hergestellte Tonbandaufnahme von vornherein aus dem Schutzbereich des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG herausfällt, weil in diesen Fällen nach allgemeiner Auffassung von einem Recht am eigenen Wort nicht mehr die Rede sein kann. Soweit es z. B. im geschäftlichen Verkehr üblich geworden ist, fernmündliche Durchsagen, Bestellungen oder Börsennachrichten mittels eines Tonabnehmers festzuhalten, ist in aller Regel das Recht auf freie Entfaltung der Persönlichkeit des Sprechers noch nicht betroffen. Bei derartigen Mitteilungen steht der objektive Gehalt des Gesagten so sehr im Vordergrund, daß die Persönlichkeit des Sprechenden nahezu vollends dahinter zurücktritt und das gesprochene Wort damit seinen privaten Charakter einbüßt.").

[600] BVerfGE 80, 367, 374 ("a) Es kommt zunächst darauf an, ob der Betroffene einen Lebenssachverhalt geheimhalten will oder nicht. Denn dort, wo der Betroffene auf Geheimhaltung selbst keinen Wert legt, ist der Kernbereich schon wegen dieses Umstands in aller Regel nicht berührt. Andererseits läßt sich der Kernbereich des Persönlichkeitsrechts nicht in der Weise bestimmen, daß es allein auf den Willen des Betroffenen zur Geheimhaltung ankommt. b) Ob ein Sachverhalt dem Kernbereich zugeordnet werden kann, hängt ferner davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakters ist und in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder die Belange der Gemeinschaft berührt."). This is also confronted with criticism, stating that the absolute protection of the "core area of privacy" will be derogated when its determination depends on whether the rights of the other person have been infringed upon or not. *Baldus*, JZ 2008, 219, 225.

[601] BVerfGE 80, 367, 374.

[602] BVerfGE 80, 367, 375 ("Vielmehr hängt die Verwertbarkeit von Charakter und Bedeutung des Inhalts ab. Enthalten solche Aufzeichnungen etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten, stehen sie also in einem unmittelbaren Bezug zu konkreten strafbaren Handlungen, so gehören sie dem unantastbaren Bereich privater Lebensgestaltung nicht an.").

[603] BVerfGE 109, 279, 313, 314. This case is also called as "Lauschangriffentscheidung". *Roggan*, StV 2011, 762, 763.

ality.[604] Due to its impact on society, however, a conversation including concrete information on criminal activities, such as the plan or report of a crime, does not belong to the "core area of privacy" regardless of the relation between the partners to the conversation,[605] and thus can be intercepted by the state.

German Federal Court (Bundesgerichtshof, hereafter referred to as BGH) accepted an absolute protection and the concept of the "core area of privacy" much later than the BVerfG. In two earlier cases concerning recordings with diary characteristics, the court used the term "private area" ("privater Lebensbereich").[606] Regardless of the similarity of the definitions of the two terms, the BGH stated that the protection of the private area must cease when crimes seriously infringe upon important legal interests, such as the right to life or the legal order.[607] The BGH did not grant such recordings an absolute protection, but balanced the privacy interest against the public interest.[608] Given the minor seriousness of the crime at hand, the BGH held that the recording in question was not admissible and the contents were also not allowed to be presented as evidence in another way, such as through interrogation of witnesses.[609]

In the second case, the BGH stated that the admission of the diaries can be justified by the seriousness of the crime, i. e., murder.[610] As a result, the diaries were allowed to prove the motivation of the defendant.[611] After his conviction, the defendant filed a

[604] BVerfGE 109, 279, 313 ("Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität.").

[605] BVerfGE 113, 349, 391 ("Nicht zu diesem Kernbereich gehören Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten."); BVerfGE 109, 279, 319.

[606] BGHSt 19, 325 and 34 238. In the first case, the BGH emphasized that one has right to keep one's opinions, feeling, and experience only for himself and should not fear that his expression will be used without his permission. Otherwise the free development of personality could be obviously infringed. BGHSt 19, 325, 327 ff. This description is similar with the definition of "Kernbereich private Lebensgestaltung" given by the BVerfG.

[607] BGHSt 19, 325, 333 ("Handelt es sich um hinreichenden Tatverdacht schwerer Angriffe auf das Leben, auf andere bedeutsame Rechtsgüter, auf den Staat oder um andere schwerere Angriffe auf die Rechtsordnung, so wird der Schutz des privaten Lebensbereichs gegebenenfalls zurücktreten müssen.").

[608] BGHSt 19, 325, 329, 332 ff.

[609] BGHSt 19, 325, 334 ("Das Landgericht darf die Tagebücher in der neuen Verhandlung nicht als Beweismittel verwerten. Über ihren Inhalt darf auch nicht in anderer Weise Beweis erhoben werden, etwa durch Vernehmung von Personen, die Kenntnis von dem Inhalt haben, als Zeugen.").

[610] BGHSt 34, 397, 401.

[611] BGHSt 34, 397, 401.

constitutional complaint with the BVerfG, arguing that the diaries belonged to the "core area of privacy" and thus should not have been admitted.[612] The BVerfG confirmed that Art. 2 Abs. 1 and Art. 1 Abs. 1 GG protect an untouchable private area where no balancing of interests should take place.[613] The BVerfG, however, emphasized that this protection has limits. If the individual has communications with others, his behavior influences other persons and is therefore not absolutely protected.[614] The BVerfG discussed at length what information belongs to the "core area of privacy",[615] and the opinions of the eight judges were equally divided on the question of the admissibility of the diaries at hand. Four judges supported the admission, arguing that the diaries were not covered by the "core area of privacy" because the defendant had written down his thoughts and thus took the risk of an interference.[616] The diaries also had a close relationship with the suspected crime; they described the background of the crime, the defendant's motivation und his understanding of the crime. This relationship excluded the diaries from the "core area of privacy".[617] The other four judges argued, however, that the admission of the diaries infringed upon the defendant's "core area of privacy". Contents of diaries, they wrote, have a personal character which cannot be waived merely by writing it down.[618] Moreover, the diaries described only thoughts and feelings and lacked a direct connection with the crime. If such contents could justify a rejection of the "core area of privacy", the distinction between the "core area of privacy" and the area where a balancing of interests can take place would disappear.[619]

This case, in which the BVerfG failed to give a clear answer to the admissibility of diaries, showed the difficulty of determining the "core area of privacy" in practice. The case law caused some confusion concerning the question whether courts should always balance the interests involved or should first decide whether evidence falls within the "core area of privacy", although there might be no difference in results.[620]

---

[612] BVerfGE 80, 367.

[613] BVerfGE 80, 367, 373.

[614] BVerfGE 80, 367, 373 ("Dies gilt allerdings nicht schrankenlos. Einschränkungen können im überwiegenden Allgemeininteresse insbesondere dann erforderlich sein, wenn der Einzelne als in der Gemeinschaft lebender Bürger in Kommunikation mit anderen tritt, durch sein Verhalten auf andere einwirkt und dadurch die persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt.").

[615] BVerfGE 80, 367, 374 – 375.

[616] BVerfGE 80, 367, 376 ff. Vgl. Fn. 600.

[617] BVerfGE 80, 367, 377.

[618] BVerfGE 80, 367, 381.

[619] BVerfGE 80, 367, 382.

[620] In this context, it can be concluded that a piece of evidence in a murder case can be excluded only if the "core area of privacy" is recognized by courts; otherwise an effective investigation enjoys priority. See *Fezer*, Grundfragen der Beweisverwertungsverbote, 1995, S. 6 ff. This conclusion still remains correct because the seriousness of the crime is widely recognized as one element for "Abwägung" process. Section 2. c), Chapter IV, Part II.

Deferring to the strong constitutional position of the BVerfG, the BGH later accepted this concept and applied it as a ground for excluding evidence.[621]

In a more recent case, the BGH argued that a soliloquy in a car[622] was covered by the "core area of privacy".[623] The defendant was suspected of having killed his wife. Upon a judicial order, the police had adopted several covert investigative measures, including surveillance of telecommunication, of his home and of his car. While driving alone in his car, the suspect talked to himself and several times made references to criminal activity, such as "we have killed her".[624] At the trial, the district court admitted these recordings as evidence, but the BGH held that they should be excluded because they fall within "the core area of privacy". The BGH emphasized that the soliloquy was conducted unconsciously and privately with the feeling of not being heard, thus should be regarded as "thoughts with sound", belonging to the freedom of thinking ("Gedankenfreiheit").[625] This decision follows the BGH's earlier case law concerning a soliloquy in a hospital room.[626] Although cars enjoy much less protection than homes ("Wohnung"), "the core area of privacy" is not limited to the space of homes.[627] This is because this concept is rooted in Art. 2 I and Art. 1 I GG, not Art. 13 GG. With regard to the decision of the BVerfG which had excluded crime-related contents from "the core area of privacy",[628] the BGH explained that the contents of a soliloquy do not play as decisive a role as they do in conversations with third persons or in diaries.[629] In the latter situation, suspects willingly gave up the privacy of their thoughts.[630]

The BGH emphasized the uniqueness of a soliloquy, namely, the high expectation of privacy, as a reason to exclude even a soliloquy involving self-incriminating words. This distinction, however, is not quite convincing. It is doubtful whether a soliloquy *per se* can justify a decision to exclude incriminating information.

---

[621] For example, the hospital-room-case. Fn. 849 and Section 1. b) ff), Chapter II, Part II. See also § 31 sec. 1 Bundesverfassungsgerichtsgesetz: "Die Entscheidungen des Bundesverfassungsgerichts binden die Verfassungsorgane des Bundes und der Länder sowie alle Gerichte und Behörden." The discussion on the exclusion on the ground of "core area of privacy" can be found in Section 3. a) aa), Chapter IV, Part II.

[622] Cars are not considered "Wohnung" and thus do not enjoy the protection of Art. 13 GG; see Fn. 826 and the companying text.

[623] BGH, NJW 2012, 945.

[624] BGH, NJW 2012, 945, 945.

[625] BGH, NJW 2012, 945, 946.

[626] See Fn. 849.

[627] BGH, NJW 2012, 945, 946.

[628] BVerfGE 109, 279.

[629] BGH, NJW 2012, 945, 946.

[630] BGH, NJW 2012, 945, 946.

bb) The Right to the Spoken Word ("Recht am gesprochenen Wort")

The "Tonband-Beschluss"[631] recognized that the right to the spoken word is covered by the right to the free development of the personality in Art. 2 Abs. 1 GG.[632] In this case, the BVerfG argued that one's words, including their contents and different ways to express them in different places and times, are highly personal.[633] Anyone, therefore, has the right to decide who can record his conversation as well as to decide whether and by whom the recording can be replayed.[634] The right to the free development of the personality would be seriously compromised if people had to fear that their words spoken in a non-public context can be recorded without their permission and be used against them in other situations.[635] Recordings will be allowed only if the common interest outweighs the privacy interest[636] and if the conversations do not fall within the absolutely untouchable area of private life ("unantastbaren Bereich privater Lebensgestaltung").[637] In this case, the BVerfG decided that the right to one's spoken word is necessary to the free development of one's personality in Art. 2 Abs. 1 GG.[638]

cc) The Relationship between Art. 10, Art. 2 GG and Art. 1 GG

As stated above, the BVerfG developed the right to images of oneself ("Recht am eigenen Bild"),[639] the right to one's spoken words,[640] and the right to data autonomy ("Recht auf informationelle Selbstbestimmung")[641] from the general personality right guaranteed by Art. 2 Abs. 1 and Art. 1 Abs. 1 GG. The information conveyed by photos, conversations or data must be personal in order to fall within the protection of this general right. Art. 10 GG, however, focuses more on the protection of the form of communications, regardless of its contents. This means that it does not matter what photos or data are transmitted. If certain information lacks importance for the free development of the personality, such as standardized communications in business, it will not be covered by Art. 2 Abs. 1 and Art. 1 Abs. 1 GG; but it may still be protected

631 BVerfGE 34, 238. Vgl. Section 1. b) aa) of this Chapter.

632 BVerfGE 34, 238, 246.

633 Later in the decision, BVerfG denied "das Recht am gesprochen Wort" on certain spoken words, which lacked characteristics of personality, for instance, stock market information. BVerfGE 34, 238, 247.

634 BVerfGE 34, 238, 246.

635 BVerfGE 34, 238, 246, 247.

636 See Section 1. d), Chapter I, Part II.

637 BVerfGE 34, 238, 248.

638 BVerfGE 34, 238, 246.

639 "Das Recht am eigenen Bild" is also regarded as a concrete type of "das Recht auf informationelle Selbstbestimmung". Vgl. *Di Fabio*, in: Maunz/Dürig, GG, 2020, Art. 2, Rn. 193.

640 BVerfGE 34, 238, 246.

641 BVerfGE 65, 1, 43.

by Art. 10 GG if it is communicated in certain ways.[642] The consent of one party to the conversation to waiving the privacy of the conversation does not remove the protection of Art. 10 GG from the other party; thus, Art. 10 GG is violated if one participant allows a state agent to covertly overhear the conversation without a judicial order.

In conclusion, Art. 10 and Art. 2 Abs. 1 and Art. 1 Abs. 1 GG each have their own areas of application, the former focusing on the process of communication, the latter concerning the contents of the information transmitted. In certain situations, the protection of Art. 10, Art. 2 Abs. 1 and Art. 1 Abs. 1 GG can overlap.[643]

c) New Basic Rights

aa) The Right to Data Autonomy

In 1983, the BVerfG had the opportunity to interpret Art. 2 Abs. 1 and Art. 1 Abs. 1 GG concerning personal data protection in the so-called "Volkszählungsurteil". In this case, rules on data collection and transmission provided by *Volkszählungsgesetz* (VZG) 1983 were challenged. The BVerfG held that on one hand, data is fact, and transmission of facts is "not an expression of one's opinion in the sense of Art. 5 Abs. 1 GG".[644] On the other hand, the BVerfG held that the autonomy ("Selbstbestimmung") on data deserves special protection because personal data can be automatically collected and stored without limitation and without the knowledge of the persons affected.[645] The BVerfG emphasized that human dignity safeguards autonomy as an integral part of a free society and that people have the right to freely decide when and to what degree to make their personal information public.[646] If the behavior of a person is known to the government through collected data, there is a high risk for the person's fundamental rights, for instance, the freedom of assembly.[647] This will not only violate the free development of the individual's personality but might also damage free democracy as a whole.[648] The BVerfG therefore held that the general personality right guaranteed by Art. 2 Abs. 1 and Art. 1 Abs. 1 GG covers the right to data autonomy and protects personal data from unlimited collection, access and transfer.[649] The BVerfG, however, also held that the individual has no absolute, unlimited right to his or her data. This right can be restricted by the state in accordance with the proportionality principle, if the autonomy interest of the in-

[642] Vgl. *Di Fabio*, in: Maunz/Dürig, GG, 2020, Art. 2, Rn. 197.

[643] Art. 2 Abs. 1 and Art. 1 Abs. 1 GG have a supplementary function in relation to Art. 10 GG and Art. 13 GG. *Di Fabio*, in: Maunz/Dürig, GG, 2020, Art. 2, Rn. 197.

[644] BVerfGE 65, 1, 40, 41.

[645] BVerfGE 65, 1, 42.

[646] BVerfGE 65, 1, 41, 42; vgl. *Di Fabio*, in: Maunz/Dürig, GG, 2020, Art. 2, Rn. 175.

[647] BVerfGE 65, 1, 42, 43.

[648] BVerfGE 65, 1, 43.

[649] BVerfGE 65, 1, 43.

dividual is outweighed by interests of society.[650] The right to data autonomy has been reconfirmed by the BVerfG in several cases since 1983.[651] This right continuously gains importance because of the high ability of modern technology on data collection and transmission and because of the massive amount of information on individuals' life reflected by personal data.

bb) The Right to the Integrity of Information Systems

Given the important role of personal computers and smartphones in daily life, the BVerfG has recognized in 2008 that the protection of personal data from infiltration and the right to data autonomy have a loophole in one's electronic equipment.[652] Art. 10 GG protects only on-going telecommunication but not data stored in one's computer, and Art. 13 GG limits its protection to the information system located in the space of homes.[653] The right to data autonomy focuses on the use of one's personal data, including the scope of collecting data and the way in which they are used. This right, however, cannot protect one's information system from infiltration, especially if there is no further data collection and processing.[654] Since data stored in information systems such as computers and smart phones reflect a large part of one's personality, they offer new possibilities for assaults on the free development of one's personality.[655] In order to fill this gap, the BVerfG developed the guarantee of the confidentiality and integrity of information systems ("Gewährleistung der Ver-

[650] BVerfGE 65, 1, 44.

[651] BVerfGE 78, 77, 84 ("Das durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht umfaßt die Befugnis jedes Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen (Recht auf informationelle Selbstbestimmung – vgl. BVerfGE 65, 1 (41 ff.))"); 92, 191, 197 ("Insbesondere sind sie bei verfassungskonformer Auslegung mit dem aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG folgenden Recht auf informationelle Selbstbestimmung vereinbar."); 96, 171, 181 ("Es verleiht jedem unter anderem die Befugnis, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er persönliche Sachverhalte offenbaren will (vgl. BVerfGE 65, 1, 41 f.; 85, 219, 224). In besonderer Weise schützt das Grundrecht vor dem Verlangen, Informationen preiszugeben, die den Betroffenen selbst belasten.").

[652] BVerfGE 120, 274, 308, 313.

[653] BVerfGE 120, 274, 309–311.

[654] BVerfGE 120, 274, 313 ("Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.").

[655] BVerfGE 120, 274, 305 ("Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen.").

traulichkeit und Integrität informationstechnischer Systeme") from the general personality right (Art. 2 I and Art. 1 I GG).[656] This new right protects people from state agents' illegal access to their information systems. In the case decided in 2008, the BVerfG held the law at issue to be unconstitutional[657] because it allowed covert online searches by the state and thus violated the principles of legality[658] and of proportionality.[659] As with other fundamental rights, the right to the integrity of information systems can be restricted for preventive purposes as well as for the investigation of crime.[660] The BVerfG has thus made it possible for the legislature to limit this right. The Federal legislature has introduced a new provision on online searches (§ 100b StPO) and has extended telecommunication surveillance beyond the data concerning on-going telecommunication (§ 100a I 2 and 3 StPO).[661] The new law has since been challenged before the BVerfG and the outcome is still not clear.

d) Proportionality (Verhältnismäßigkeit)

Art. 10 I GG protects the privacy of communications, that is, the free development of the personality by means of a private exchange of information, thoughts and opinions that remains concealed from the eyes of the public.[662]

Art. 10 II GG permits the legislature to limit the protection of the privacy of telecommunication. Such limitations can only be imposed by law, and any restriction to the fundamental right defined by Art. 10 GG must be proportional. The BVerfG has established three criteria of proportionality, i. e., suitability ("Geeignetheit"), necessity ("Erforderlichkeit") and proportionality in the narrow sense ("Verhältnismäßigkeit im engeren Sinne").[663]

aa) Suitability

The first factor of proportionality is the suitability of measures that restrict fundamental rights. Suitability describes the connection between the adopted measures and the purpose.[664] A measure is "suitable" if it can help to bring about the

[656] BVerfGE 120, 274, 302.

[657] Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW, S. 620).

[658] BVerfGE 120, 274, 315 – 318.

[659] BVerfGE 120, 274, 318 – 322.

[660] BVerfGE 120, 274, 315 ("Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist nicht schrankenlos. Eingriffe können sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein.").

[661] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Auflage, 2018, § 100a Rn. 90.

[662] BVerfGE 67, 157, 171.

[663] BVerfGE 67, 157. See also BVerfGE 30, 292; 90, 145; 100, 313.

[664] *Durner*, in: Maunz/Dürig, GG, 2020, Art. 10, Rn. 187; *Schlink*, in: Rosenfeld/Sajó (eds.), Oxford Handbook of Comparative Constitutional Law, 2013, S. 723; *Oreschnik*, Ver-

desired result.[665] The final achievement of the result is not required.[666] An abstract probability is sufficient to define suitability.[667] A measure can still be "geeignet" if there are negative side-effects, as long as the goal can be achieved.[668] This element can also be understood from the negative side, i. e., if certain measures do not serve the purpose of the legislation, they will be regarded as unsuitable. For instance, the *Bundesjagdgesetz* required falconers to have knowledge about shooting guns. This rule was regarded by the BVerfG as unsuitable because knowledge on guns is not relevant in the case of hunting with a falcon and thus the measure was unsuitable for the goal, namely, orderly hunting.[669] In practice, however, it is very rare for a measure to be deemed unconstitutional only because of unsuitability.[670] Moreover, the purpose offered by Art. 10 GG is vaguely formulated,[671] the legislature therefore has some leeway in deciding which measure is suitable to achieve this purpose.

bb) Necessity

Necessity refers to the relationship among all possible measures suitable to achieve the purpose.[672] The BVerfG has defined a measure as necessary if the legislature could not have chosen other measures with the same effect but less intrusive on fundamental rights.[673] Necessity is a test for what measures should be adopted among all suitable ones. The core requirement is that the chosen method must be the least restrictive ("geringstmöglicher Eingriff" [674]) among all possible alternatives with the same effect; alternative measures are not taken into account if by using them the achievement of the purpose would be impossible or seriously impeded ("aussichtslos oder wesentlich erschwert").[675] Taking the purpose of legislation into ac-

---

hältnismäßigkeit und Kontrolldichte, 2019, S. 2; *Klatt/Meister*, JuS 2014, 193, 195; *Voßkuhle*, JuS 2007, 429, 430; *Daiber*, JA 2020, 37, 37.

[665] BVerfGE 30, 292, 316; *Durner*, in: Maunz/Dürig, GG, 2020, Art. 10, Rn. 187.

[666] *Oreschnik*, Verhältnismäßigkeit und Kontrolldichte, 2019, S. 103.

[667] BVerfGE 67, 157, S. 173 – 175; 90, 145, 172; 100, 313, 373.

[668] BVerfGE 83, 1, 18.

[669] BVerfGE 55, 159 (Falknerjagdschein). Cf. *Alexy*, in: Schliesky/Ernst/Schulz (Hrsg.), Die Freiheit des Menschen in Kommune, Staat und Europa, 2011, S. 4 ff.

[670] *Oreschnik*, Verhältnismäßigkeit und Kontrolldichte, 2019, S. 104.

[671] The purpose of Art. 10 GG is to protect "die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes".

[672] *Hirschberg*, Der Grundsatz der Verhältnismäßigkeit, 1981, S. 148 ("Mittel-Mittel-Relation"); *Durner*, in: Maunz/Dürig, GG, 2020, Art. 10, Rn. 189; *Klatt/Meister*, JuS 2014, 193, 195; *Voßkuhle*, JuS 2007, 429, 430.

[673] BVerfGE 30, 292, 316; 67, 157, 176; 90, 145 172 ("… wenn der Gesetzgeber nicht ein anderes, gleich wirksames aber das Grundrecht nicht oder doch weniger fühlbar einschränkendes Mittel hätte wählen können").

[674] *Degenhart*, Staatsrecht I, 29. Aufl. 2013, § 4 Rn. 419.

[675] BVerfGE 67, 157, 177. The same expression can be found in the subsidiarity clauses discussed in Section 1. f) of this Chapter.

count, the legislature has the prerogative to initially decide which method is suitable and necessary. When the law's constitutionality has been challenged, however, the BVerfG will decide according to the characteristics of the area in which the method is applied and its aptness to reach its purpose.[676]

cc) Proportionality in the Narrow Sense

The criterion of proportionality "in the narrow sense" reflects the overall seriousness of the infringement of fundamental rights in relation to the purpose to be achieved.[677] No comparison with other alternative measures is involved here.[678] In a case where the constitutionality of G10 was challenged, the BVerfGE required that the infringement upon the freedom protected by constitutional law must not be disproportionate to the common good that this infringement serves.[679] The legislature has the duty to keep the common interest ("Allgemeininteresse") and individual interest in a proportionate relation. If the common interest outweighs the infringement of individual rights, then such infringement and the measure leading to this infringement are justified.[680] The BVerfG has described in detail what elements are to be taken into consideration on each side of the scales when deciding on "Angemessenheit" of surveillance measures. On the side of individual interests, the intensity of the infringement is analyzed, including a) the number and the identities of the telecommunication partners, b) types and contents of the telecommunications, and c) the threatened rights and the negative effects suffered by the individuals. For the common interest, a) the importance of the purpose, b) the severity and emergency of the danger or the investigated crime, and c) the probability of getting desirable results are considered.[681]

The BVerfG held that strategic surveillance of telecommunication is proportionate because the purpose of this measure, i. e., to prevent a war against Germany, is

[676] BVerfGE 90, 145, 173 ("Bei der vom Verhältnismäßigkeitsgrundsatz geforderten Beurteilung der Eignung und Erforderlichkeit des gewählten Mittels zur Erreichung des erstrebten Zwecks sowie bei der in diesem Zusammenhang vorzunehmenden Einschätzung und Prognose der dem Einzelnen oder der Allgemeinheit drohenden Gefahren steht dem Gesetzgeber ein Beurteilungsspielraum zu, welcher vom Bundesverfassungsgericht nur in begrenztem Umfang überprüft werden kann.").

[677] *Ogorek*, in: Epping/Hillgruber, BeckOK Grundgesetz, 46. Edition, 2021, Art. 10, Rn. 68.

[678] *Voßkuhle*, JuS 2007, 429, 430.

[679] BVerfGE 100, 313, 375 ("… die Einbußen an grundrechtlich geschützter Freiheit [dürfen] nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkung dient").

[680] BVerfGE 100, 313, 376 ("Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, daß der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen").

[681] BVerfGE 100, 313, 376; 90, 145, 173.

particularly important.[682] By contrast, adopting such a measure to prevent money counterfeiting is regarded as disproportionate, since money counterfeiting does not necessarily threaten the safety of Germany.[683]

When creating the provisions on covert surveillance measures, the legislature sought to carefully adapt the law to the principle of proportionality, for example, by establishing requirements on the crime categories that can be investigated under § 100a StPO, on exclusion of the "core area of privacy", on the duration of a judicial order, etc.[684]

As stated above, these three criteria describe a "purpose means test" ("Zweck-Mittel-Kontrolle") approach from different perspectives and can also be regarded as a "three step test" to decide on proportionality. Suitability, as the first step, examines the relationship between the means ("Mittel") and the purpose ("Zweck") that the measure serves. If a measure is not suitable for a legitimate purpose, it is disproportionate because it infringes upon a basic right without being able to reach a legitimate purpose. The second test, necessity, offers a standard for deciding which measure should be chosen among those who have passed the first test. The answer is: the least invasive one which has the same effect. The last test, proportionality in the narrow sense, describes further the relationship between the measure and its purpose. If the chosen measure is overly restrictive in relation to its positive effect, this measure is disproportionate even though it may be the least invasive measure available.

The proportionality principle emerged originally in German administrative law and was incorporated into German constitutional law in the late 1950s and early 1960s and became a central doctrine through several landmark decisions of the BVerfG.[685] Thereafter, it spread relatively quickly to other jurisdictions, including EU law and international law, such as ICCPR.[686] It is therefore regarded as the most important "German legal invention" after the Second World War.[687] According to

[682] BVerfGE 100, 313, 378.

[683] BVerfGE 100, 313, 384, 385.

[684] Details will be discussed in Chapter III, Part II.

[685] *Cohen-Eliya/Porat*, Proportionality and Constitutional Culture, 10, 11; see also *Dumbs*, Die Entwicklung des Grundsatzes der Verhältnismäßigkeit in der Rechtsprechung des Bundesverfassungsgerichts, 2015, S. 27 ff.

[686] *Franck*, Proportionality in International Law, Law and Ethics of Human Rights 4 (2010), 46. More details about the diffusion of the proportionality principle can be found in *Sweet/Mathews*, in: Bongiovanni et al. (eds.), Reasonableness and Law, 2009, 193 ff.

[687] *Peters*, in: Baade/Ehricht et al. (eds.), Verhältnismäßigkeit im Völkerrecht, 2016, S. 2; *Wahl*, in: Heckmann/Schenke/Sydow (Hrsg.), Verfassungsstaatlichkeit im Wandel, 2013, S. 823; *Beatty*, The Ultimate Rule of Law, 2004.

some authors, the reason for its widespread use is its flexibility, which allows the law to develop naturally and leaves courts enough room to make their own evaluations.[688]

e) Summary

GG protects fundamental rights of individuals. The BVerfG makes continuous contributions to clarifying the meaning of these rights. The concept of the "core area of privacy" is a good example. The BVerfG developed a general personality right from Art. 2 I and Art. 1 I GG,[689] which guarantees a "core area of privacy".[690] Furthermore, new basic rights, the right to one's image, the right to one's spoken word, and the right to data autonomy have been deduced from this general right by the BVerfG.[691]

Yet, no right is absolute and guaranteed beyond restriction. Any restriction of rights, including surveillance measures, is limited by the principle of proportionality.

2. Surveillance of Telecommunication under § 100a StPO

§ 100a StPO allows investigators to listen to and record telecommunications. This provision thus restricts the right under Art. 10 GG and at the same time stipulates the criteria for telecommunication surveillance for criminal investigation purposes. The constitutional basis can be found in Art. 10 II 1st sent. GG.[692] Taking account of the development of communication technology and the privatization of telecommunication services, § 100a StPO was modified by *the Law on Telecommunications (TKG)*[693] in 1997. The term "Fernmeldeverkehr" in § 100a and § 100b StPO, as well as in Art. 1 and Art. 3 G10, has been replaced by "Telekommunikation", without any change in the meaning.[694] In 2007, § 100a was reformulated by the *Law for the Regulation of Telecommunication Surveillance and other Covert Investigative Measures.*[695] The latest version was introduced by the *Law for a More Effective and More Practice-oriented Arrangement of Criminal Proce-*

[688] A discussion of the reasons of popularity of proportionality principle can be seen: *Cohen-Eliya/Porat*, Proportionality and the Culture of Justification, American Journal of Comparative Law 59, 463, 466.

[689] BVerfGE 54, 148, 153; 27, 1. 6.

[690] See Section 1. b), Chapter I.

[691] See Section 1. c), Chapter I.

[692] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a Rn. 2. See also Section 1. a) of this Chapter.

[693] Telekommunikationsgesetz (TKG) (BGBl. I 3108).

[694] *Vassilaki*, JR 11 (2000), 446, 446.

[695] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG v. 21. 12. 2007 (TKÜG) (BGBl. I 3198).

dure.[696] According to this law, the information that can be collected by the investigators is no longer limited to on-going telecommunications but extends to completed communications.[697]

a) Protected Area of "Telekommunikation"

§ 3 Nr. 22 TKG defines the German term "Telekommunikation" as the technical process of sending, transferring and receiving signals by means of telecommunication devices.[698]

From the case law of the BVerfG and the historical context of Art. 10 GG, it is clear that "Fernmeldegeheimnis" in Art. 10 GG refers to all kinds of telecommunications, even those that were not known in 1949.[699] The word "technische" in § 3 Nr. 22 TKG refers not only to traditional ways of telecommunication, such as telegram and telephone, but also to modern technologies, such as mobile phone, radio, satellite signal, fax, and telecommunication via computer and internet, like emails, "Internet-Telefonie", such as Skype talks, and photos or videos via Whatsapp.[700] "Signale" are not limited by the technologies that are used to produce or transmit the signals. Moreover, the BVerfG stated that Art. 10 GG protects not only the contents of telecommunication but also the whole process of communicating ("Kommunikationsvorgänge"), including the related telecommunication data ("die näheren Umstände des Fernmeldeverhältnisses", "Kommunikationsumstände" or "Verbindungsdaten").[701] This includes the information whether, when and among whom the telecommunication was or was meant to be conducted.[702] In addition, connection data ("Verbindungsdaten") also include the telephone numbers of all participants, the number of participants to the communications, the location of a calling cell phone, and how long the communication lasted.[703] Correspondingly, the

---

[696] Gesetz zur effektiveren und praxistaugli cheren Ausgestaltung des Strafverfahrens vom 17. 8. 2017 (BGBl. 2017 I 3202).

[697] See Section 2. a), Chapter I, Part II.

[698] § 3 Nr. 22 TKG: "'Telekommunikation' der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen".

[699] BVerfGE 100, 313, 358 ("Der Grundrechtsschutz bezieht sich vielmehr auf alle mittels der Fernmeldetechnik ausgetauschten Kommunikationen."); vgl. *Vassilaki*, JR 11 (2000), 446, 446.

[700] Vgl. *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 31 and 32.

[701] BVerfGE 85, 386, 396; 100, 313, 358. "Verbindungsdaten" is defined by § 2 Nr. 4 *Telekommunikations-Datenschutzverordnung* (TDSV) vom 18. Dezember 2000 (BGBl. I 2000 s. 1740) as: "personenbezogene Daten eines an der Telekommunikation Beteiligten, die bei der Bereitstellung und Erbringung von Telekommunikationsdiensten erhoben werden."

[702] BVerfGE 67, 157, 172; 85, 386, 396; 100, 313, 358.

[703] Vgl. § 6 TDSV; *Schenke*, in: Badura/Fabio/Robbers (Hrsg.), Archiv des Öffentlichen Rechts, Band 125, 2000, S. 19.

new § 100a I 3 and V 1 StPO makes it clear that the content and circumstances of the communication are treated equally.

In 2017, two sentences were added to § 100a I. § 100a I 2 allows for the infiltration of one's information system if it is necessary for the purpose of enabling surveillance of encrypted data, and § 100a I 3 has expanded the possibility of surveillance to completed communications. The stored content and circumstances of the communication in one's information system can be collected when such data could have been collected during its transmission process. These changes were meant to address the difficulty of intercepting encrypted signals during their transmission.[704] The new provisions enable investigators to intercept the communication before the encryption from the sender or after de-encryption from the receiver.[705] Since this method also involves the infiltration of information systems, its relationship with online searches regulated in § 100b is not clear, for example in the case of searching one's stored email. Moreover, the fact that the new law permits the surveillance of completed communications raises the problem of undermining the protection of Art. 10 GG of on-going telecommunication.[706]

b) Crime Catalogue under § 100a StPO

§ 100a II StPO provides a list of offenses that can be investigated by using telecommunication surveillance. Since 1968, this list has been expanded several times. After the amended formulation by TKÜG in 2007, § 100a StPO lists crimes according to the statutes in which they are regulated. Crimes regulated by the German *Criminal Code* (hereafter referred as to StGB) come first and appear according to their order in StGB. These crimes can be divided into three categories: 1) crimes threatening national security, such as § 100a II No. 1a) and c) StPO; 2) crimes against individual rights, such as § 100a II No. 1h) murder and killing, f) rape, k) robbery and n) fraud; and 3) crimes against the public and economic order, such as § 100a II No. 1d), e), p), q) and r) StPO. The decision whether to include a crime in this catalogue has been made not only based on its seriousness, such as murder and rape, but also based on its nature; many crimes in this list have characteristics of organized crime, such as § 100a II No. 1m) and j), Nos. 2, 4, 5, 7 and 11 StPO.[707]

Issuance of a judicial order for telecommunication surveillance under § 100a StPO requires that the crime under investigation is serious ("schwere Straftat"),[708] which falls between the categories of "especially serious offenses" ("besonders schwere Straftaten") for the surveillance of a home and "offenses of significant

[704] *Weigend*, Mobile Phones as a Source of Evidence in German Criminal Procedure, in: Essays in Honor of Masahito Innouye, 2019, 877.

[705] See BT-Drucks 18/12785, S. 46; *Roggan*, StV 2017, 821, 822.

[706] *Roggan*, StV 2017, 821, 824.

[707] Vgl. *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 47 ff.

[708] § 100a I No. 1 StPO.

seriousness" ("Straftaten von erheblicher Bedeutung") for the authorization of an undercover agent.[709] According to the sentencing system of StGB, serious offenses refer generally to an offense with a maximum sentence of 5 years or more.[710] If the legal interest that the offender infringed upon was especially important or if there exists a special public interest in the prosecution, wiretaps are permissible even if the offense in question carries a lesser statutory maximum sentence of more than one year.[711]

§ 100a II No. 2 StPO further requires that the individual offense under investigation is serious.[712] In order to determine individual seriousness, the judge takes into consideration the consequences of the crime, especially on the victims,[713] as well as the potential sentence in the concrete case, not only the abstract sentencing frame provided by StGB.

According to the statistics on surveillance of telecommunications for 2018 published by the *Bundesamt für Justiz*, judicial orders were most frequently issued for violations of the *Drug Law ("Betäubungsmittelgesetz")* (§ 100a II No. 7b StPO); they made up 39 % (8792 out of 22514) of all procedures involving telecommunication interception. Fraud and Computer Fraud under § 100a II No. 1n StPO was the second-most frequently cited crime with 13 % percent, followed by gang theft under § 100a II No. 1j StPO with 10 %.[714]

c) Persons Targeted and Third Persons

§ 100a III StPO limits the judicial order of telecommunication surveillance to suspects and third persons who receive or transmit messages for or of the suspects, or whose telephone connection is used by the suspect.

---

[709] BT-Drucks 16/5846, S. 39, 40.

[710] *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 10.

[711] BT-Drucks 16/5846, S. 40 ("Im Vergleich zu den von Artikel 13 Abs. 3 Satz 1 GG vorausgesetzten besonders schweren Straftaten und den Straftaten von erheblicher Bedeutung nehmen die in § 100a Abs. 1 Nr. 1 StPO-E in Bezug genommenen schweren Straftaten eine Zwischenstellung ein. Hierunter können solche Straftaten verstanden werden, die eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsguts oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe. Eine Höchststrafe von einem Jahr Freiheitsstrafe entspricht dem Begriff der schweren Straftat nicht mehr.").

[712] "Die Tat auch im Einzelfall schwer wiegt".

[713] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 11.

[714] See https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html, visited 29. 04. 2021.

aa) Persons Targeted

The identity of the suspect to be intercepted is not necessarily known at the time when the judicial order is issued.[715] Suspected accomplices of the perpetrators of listed crimes are also subject to surveillance as suspects. The same applies to persons who are suspected of having committed a punishable attempt of a listed offense. Activities in preparation of a listed offense can give rise to a surveillance order when such activities constitute independently punishable (not necessarily serious) offenses, or when they are punishable in accordance with § 30stGB.[716]

bb) Third Persons

The BVerfG has confirmed that it is permissible to intercept the telecommunications of non-suspect persons who are receiving or transmitting messages intended for, or originating from, the suspect, or whose telephone connection or information system is used by him.[717] In that case, it is not necessary that the non-suspect person knows of his role in the transmission of information. He need not be involved in the criminal activities or even know about the contents of the telecommunications.[718] The transmitting person's role must be established by certain facts ("bestimmte Tatsachen"). The BVerfG has declared that vague connections between the non-suspect person and the suspect or the existence of rumors are not sufficient to support a surveillance order against the third person.[719] The decisive issue is the degree of probability that the third person and the suspect will be in contact; moreover, the judge must examine whether the measure is proportional to the expected results and the seriousness of the crime.[720]

A surveillance order may affect persons who have nothing to do with the crime and have no relation with the suspect, so-called "Unbeteiligte". For instance, when a public telephone cell or a WLAN Hotspot is under surveillance, anyone who uses them will be intercepted.[721] Records from such an interception that are not necessary for the investigation must be deleted without delay.[722]

According to an empirical study published in 2003, only 39.4 % of the telecommunication surveillance measures were conducted directly against the telephone lines of suspects, while 49.5 % of surveillance measures were ordered against third

[715] *Deckers*, StraFo 2002, 109, 113.

[716] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 12; BGH 32, 10, 16 (a conspiracy to commit murder falls within the catalogue of crimes in § 100a).

[717] BVerfGE 30, 1, 22.

[718] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 19, 20.

[719] BVerfGE NJW 2007, 2753.

[720] BVerfGE NJW 2007, 2753.

[721] Vgl. *Joecks*, JA 1983, 59, 60; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 20.

[722] § 101 VIII StPO.

persons. Around 8 % of measures were ordered on non-private telephones, such as telephones in hotels.[723]

In many situations, non-suspects have close relations with suspects as family members or good friends. Although § 52 StPO guarantees the relatives of the suspect the right to refuse to testify, and close relations can support the assumption of "the core area of privacy",[724] telecommunications among them are not excluded from surveillance. Even the proportionality clause provided in § 100d V StPO[725] does not apply to § 100a StPO.[726]

cc) Lawyer-client Communications

§ 137 I 1 StPO provides that the suspect has the right to access a lawyer at any stage of the criminal proceedings. The confidentiality of the communication between a defense lawyer and his client is mainly protected by the lawyer's right to refuse to testify (§ 53 I StPO) and the right to communication (§ 148 StPO). The latter guarantees the unsupervised communication between the lawyer and his client except for terrorist-related crimes (§ 148 2 StPO). In principle, communications between the lawyer and his client must not be intercepted.[727] Telecommunications defined under § 100a StPO are also covered by the protection of § 148 StPO.[728] The protected interest is not the lawyer's personal privacy but the confidentiality of his professional relationship with his client.[729] The BGH held that the conversation between a defense lawyer and his client can be used as evidence against other clients.[730] According to the BGH, the privilege has a protective effect only on the persons whose privacy is infringed upon, but has no effect on third persons.[731]

---

[723] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 24.

[724] The discussion on the relationship between § 52 StPO and "the core area of privacy" can be seen in Section 1. b) gg), Chapter II, Part II.

[725] § 100d V StPO: "…wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten steht."

[726] More about this proportionality clause in § 100d V can be found in Section 1. b) ff), Chapter II, Part II.

[727] *Jahn*, in: Löwe/Rosenberg, StPO, Band 4/2, 27. Auflage, 2020, § 148, Rn. 14; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 21; see also *Werle*, JZ 1991, 482, 487.

[728] *Jahn*, in: Löwe/Rosenberg, StPO, Band 4/2, 27. Auflage, 2020, § 148, Rn. 15 ff.; BGHSt 33, 347, 350.

[729] BVerfGE 109, 279, 326, 327.

[730] BGHSt StV 1990, 435. E. K. and F. K., the father and the son, were charged of arson. During the investigation their company-telephone was intercepted with a judical order. Mrs. K., the wife of E. K., called the lawyer of E. K. and F. K. via this phone and discussed about the case. In accordance with the BGH, this piece of conversation can cannot be used against Mrs. K., but possible to be used against E. K. and F. K. because this conversation was not covered by the lawyer-client privilege between the lawyer and E. K. and F. K. Therefore, in the proceeding

§ 160a I StPO prohibits the interception of communications between clients and their lawyer with a right to refuse to testify. Yet, according to § 160a IV StPO, the communication between the lawyer and his client may be intercepted if the defense lawyer is suspected of being an accomplice in the offense under investigation. If the lawyer himself is suspected of having committed an offense listed in § 100a II StPO, an order can be issued against the lawyer. In that case, it is important to distinguish between communications concerning the lawyer's offense and those concerning his professional capacity. If the latter are recorded, they must be deleted without delay (§ 160a I 3 StPO).

A landmark case on the interception of communications between a lawyer and his client was decided by the BGH in 1985. In this case, Suspect P had been at large for a long time. In order to find out where P was, a judge issued an order to intercept the telephone of A, P's lawyer. The recordings proved that A assisted P in obtaining money to enable P to stay abroad. A was then accused of attempting to obstruct P's punishment (§ 258 StGB).[732] The BGH declared that from a constitutional perspective there was no objection to ordering the surveillance of telecommunications of a lawyer who is suspected to be an accomplice of a catalogue crime provided in § 100a StPO.[733] The suspicion of a catalogue crime by itself, however, cannot justify a measure under § 100a StPO when the right to an unsupervised communication guaranteed by § 148 StPO is infringed upon.[734] Therefore, the telecommunications between P and A should not have been intercepted.

d) Chance Finds ("Zufallsfunde")

Problems of chance finds arise when a legal wiretap[735] leads to the recording of incriminating conversations of persons or on criminal activities not envisaged by the judicial order.

aa) Background Conversations

Recording of background conversations is a good illustration of chance finds. The term "background conversations" refers to conversations that are conducted in the background of an intercepted telecommunication and are recorded along with it. Law

against them, this conversation can be used as a "normal" legally recorded conversation without violating § 148 StPO.

[731] This conclusion follows the "Rechtskreis" theory which is discussed in Section 2. a), Chapter IV, Part II.

[732] BGHSt 33, 347.

[733] BGHSt 33, 347.

[734] BGHSt 33, 347, 349.

[735] The exclusion of evidence concerning core area of privacy, as well as the "distance effect" of illegally obtained results are not involved here.

enforcement officers normally do not expect to get information from background conversations. With regard to such conversations, German courts differentiate between those recorded during an on-going telecommunication and those recorded after the telecommunication has been concluded.

This problem was first dealt by the BGH in 1983 in a case where a conversation between a couple in their house was unintentionally recorded because the telephone receiver in their house was not replaced correctly after the end of an intercepted telephone conversation.[736] The BGH declined to admit the couple's live conversation as evidence based on § 100a StPO, because the conversation did not fall within the definition of "long-distance communications" ("Fernmeldeverkehr").[737] Based on a literal interpretation of "long-distance communications", the BGH held that conversations conducted in the house without the need of any telecommunication facility are not covered by the authority to wiretap in § 100a StPO.[738] Moreover, the BGH declined to give an expansive interpretation to "long-distance communications" because § 100a StPO restricts not only Art. 10 GG but also general personal rights,[739] and such restrictions cannot be imposed without an express legal authority. The BGH also held that conversations between a couple in their own home belongs to the core area of private life and enjoys absolute protection provided by Art. 2 Abs. 1 and Art. 1 Abs. 1 GG.[740] As a result, the conversation was excluded from the evidence.

In 1995, the *OLG Düsseldorf* also had to decide on the admissibility of a background conversation. In this case, the suspect called his lawyer on a telephone line under surveillance in accordance with the version of § 100a StPO applicable in 1995. Before the lawyer picked up the phone, the suspect discussed his criminal activity with his accomplice in the same room for about 30seconds.[741] This conversation was recorded via the recorder installed on the suspect's telephone line.[742] The *OLG Düsseldorf* admitted the conversation as evidence, because after dialing the "long-distance communication" had begun, and therefore the conversation was covered by the term "Fernmeldeverkehr".[743] The court claimed that its decision did not contradict BGHSt 31, 297 where the live conversation was held not to be "long-distance communication". In that decision the BGH had, however, ruled that, according to general usage, only signals with a direct and necessary connection with telephone

[736] BGHSt 31, 296, 296, 297.
[737] BGHSt 31, 296, 297.
[738] BGHSt 31, 296, 297.
[739] BGH 31, 296, 298.
[740] BGH 31, 296, 299, 300.
[741] OLG Düsseldorf NJW 1995, 975, 975.
[742] OLG Düsseldorf NJW 1995, 975, 975.
[743] OLG Düsseldorf NJW 1995, 975, 976.

calls, such as dial signals, can be regarded as "long-distance communications".[744] Given the BGH's clear rejection of an expansive interpretation of "long-distance communications", it is difficult to treat the suspect's conversation in the Düsseldorf case in the same way as dial signals. Moreover, that conversation had no direct and necessary connection with the following telephone call.[745] The BGH nevertheless in 2008 followed the argument of the *OLG Düsseldorf*'s decision, stating that the background conversation recorded during a "voluntary telecommunication contact" ("willentliche Telekommunikationsverbindung") can be admitted, even during the period that the ringing signal can be heard but the receiver has not picked up the phone on his side.[746] The BGH argued that the conversation in this short time period has a direct relation with the telephone connection.[747]

bb) Admissibility of Chance Finds

Chance finds can be used in two ways: as evidence in court ("zu Beweiszwecken"; cf. §§ 161 III and 479 II 1 StPO); and as background information that can trigger further investigation.

§ 161 III StPO regulates that chance finds from investigative measures may be used as evidence in another criminal process only if the measure which produced them could have been ordered to investigate the new offense. The results of covert telecommunication surveillance may accordingly be used for evidentiary purposes for other catalogue crimes listed in § 100a StPO, but not for proving offenses that are not listed in § 100a II StPO.[748]

According to case law of the BGH and the BVerfG, chance finds may be used to trigger further investigations or for locating suspects even of non-catalogue-crimes.[749] The evidence obtained from such further investigations can in principle be

[744] BGHSt 31, 296, 297 ("Hierunter fallen nach dem allgemeinen Sprachgebrauch außer dem Telefongespräch nur die unmittelbar mit dem Telefonieren notwendigerweise verbundenen Vorgänge, z. B. das Anwählen des Gesprächspartners.").

[745] The connection here refers only to functional connection, not contents.

[746] BGH StV 2009, 398, 398 ("Ebenso konnte der Tatrichter ohne Rechtsfehler Äußerungen verwerten, welche vom Angeklagten oder von mit ihm sich unterhaltenden Personen gemacht wurden, während dieser willentlich eine Telekommunikationsverbindung herstellte, auch wenn zu diesem Zeitpunkt erst das Klingelzeichen hörbar war und der Angerufene das Gespräch noch nicht angenommen hatte; denn auch insoweit handelt es sich um unmittelbar mit dem Telefonieren verbundene Vorgänge").

[747] BGH StV 2009, 398.

[748] BGHSt 26, 298, 302 ff.; 28, 122, 127 ff.; 32, 10, 14 ff. LG Münster, StV 2008, 460; *Hilger*, in: Löwe/Rosenberg, StPO, Band 9, 26. Auflage, 2010, § 477, Rn. 8 ff.; MDR 82, 690.

[749] BGHSt NStZ 1998, 426, 427; BVerfG NJW 2005, 2766; OLG München wistra 2006, 472; *Hilger*, in: Löwe/Rosenberg, StPO, Band 9, 26. Auflage, 2010, § 477, Rn. 8 ff.; *Zöller* StraFo 2008, 24.

admitted as evidence.[750] The BVerfG based this conclusion on a balancing between the protection of the rights guaranteed in Art. 10 GG and an effective fight against crime.[751] § 161 III and § 479 II StPO expressly limit the prohibition of using chance finds to their use as evidence ("zu Beweiszwecken") in non-catalogue crimes, which invites the conclusion that they can be used as a trigger for further investigations.

Sometimes it is difficult to decide, however, whether evidence obtained from a different investigation is used as "evidence" or as a mere clue. In an early case, a police officer confronted a person suspected of a non-catalogue crime with a tape-recording from a related investigation for a catalogue crime, and the suspect thereupon confessed to the non-catalogue crime. The BGH held that the confession could not be used as evidence because the police officer had used the tape-recording for a "Vorhalt" and invited the suspect to comment on it, which the BGH considered to be use as "evidence".[752] A similar case was decided by *OLG Karlsruhe* in 2004: A police officer had learned from telephone surveillance of X for drug dealing that Y was one of X's customers. The officer interrogated Y on the suspicion of buying prohibited drugs, which is a crime not listed in § 100a II StPO. The officer told Y that he "knew" that she had bought drugs from X, and Y thereupon admitted that that was true. The *OLG Karlsruhe* upheld the lower court's exclusion of the confession, arguing that the police officer had made illicit use of the information from the wiretap for investigating a non-catalogue offense.[753] This decision seems to go too far in excluding evidence. Whereas in the BGH case, the police officer had actually used the tape-recording of the telephone surveillance to confront the suspect, in the Karlsruhe case the officer only verbally referred to it when interrogating the suspect. That can hardly be regarded as evidentiary use of the result of the surveillance. Courts should, however, also beware of undermining the requirement of a catalogue offense by limiting too narrowly the concept of evidentiary use of the results of a wiretap.

To resolve this problem properly, it should be kept in mind that results from telecommunication surveillance are in principle inadmissible as evidence for non-catalogue crimes. This indicates that the courts may use only new evidence found in a further investigation, which must be substantially different from the chance finds from telecommunication surveillance. For instance, if chance finds from telecommunication surveillance justify the authorization of an undercover agent, then this agent might find new incriminating evidence during his work. If, on the other hand, a suspect's confession basically just confirms the contents of the chance find

[750] *Hilger*, in: Löwe/Rosenberg, Band 9, 26. Auflage, 2010, § 477, Rn. 8a; BVerfG 2005 2766; BGHSt 27, 355; *Singelnstein*, ZStW 120, 871 ff.

[751] BVerfG NJW 2005, 2766 ("Diese Rechtsprechung berücksichtigt einerseits den Schutz des Grundrechts aus Art. 10 GG, indem weitergehende Ermittlungen nur in den Fällen für zulässig gehalten werden, in denen die Maßnahme nach § 100a StPO rechtmäßig war; andererseits wird dem Interesse an einer wirksamen Strafrechtspflege hierdurch Rechnung getragen.").

[752] BGHSt 27, 355.

[753] OLK Karlsruhe, 03.06.2004 – 2 Ss 188/03; NStZ 2004, 643.

that has been presented to him without adding anything to it, the confession should not be admitted.

e) Degree of Suspicion under § 100a I 1 Nr. 1.

Surveillance under § 100a StPO can only be ordered if certain facts ("bestimmte Tatsachen") have been found to support the suspicion of one or more offenses included in the list of § 100a II StPO,[754] and the suspected individual offense is serious ("auch im Einzelfall schwer wiegt"). For instance, the mere fact that a person went into a building where criminals were meeting cannot justify the order of telecommunication surveillance against him. The police must prove that this person actually joined the meeting.[755] In addition, the suspicion of a catalogue crime has to be made concrete through certain evidence,[756] for example, witnesses, results from tracking and observation, or fingerprints.[757] An empirical study shows that between 1996 and 1998 20 % of 381 telecommunication surveillance orders were supported by the testimony of informants; 19 % were based on reports made by police or prosecutors; 26 % were based on the investigative activities of law enforcement agents, including information from other proceedings; and 18.4 % were supported by information from other telecommunication surveillance. Only 0.2 % of orders were based upon a search.[758]

The degree of suspicion does not need to reach the standard of "sufficiently suspicious" ("hinreichend verdächtig") for courts to open a trial provided by § 203 StPO nor the standard of "strongly suspicious" ("dringend verdächtig") for issuing an arrest order under § 112 I StPO,[759] but "simple suspicion" ("einfacher Tatverdacht") is sufficient.[760] The standard of suspicion must be adapted to each case[761] and its application also depends on the personal criminalistic experience of the investigator.[762] Therefore, different people can evaluate the same situation differently.[763]

---

[754] BVerfG NJW 2007, 2749, 2610; BGH NStZ 2010, 711, Rn. 10.

[755] BGH NStZ 2010, 711, Rn. 22.

[756] OLG Celle, StV 2011, 4, 215; BT-Drucks. V/1880 s. 11 ("Der Verdacht muss durch schlüssiges Tatsachenmaterial ein gewisses Maß an Konkretisierung erlangt haben.").

[757] Vgl. *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Auflage, 2018, § 100a, Rn. 42.

[758] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 21–22. 14 % of surveillance have mixed sources of information and 1.5 % were issued upon § 31 of *the German Drug Law.* 2 % did now show the source of information.

[759] *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 9; *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Auflage, 2018, § 100a Rn. 42; BGH NStZ 2010, 711, Rn. 10. *Bernsmann/Jansen*, StV 1998, 217, 219, 220.

[760] NStZ 2003, 279, Rn. 6; StV 2011, 216.

[761] BGH NStZ 2010, 711, Rn. 10; *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 30.

[762] BGH NStZ 10, 711, Rn. 10.

[763] BGHSt 41, 30, 33.

There is thus no strict threshold of suspicion for issuing a surveillance order,[764] and it is difficult for the defense to challenge an order for lack of proper suspicion in accordance with § 100a I No. 1 StPO.[765]

f) Subsidiarity Principle

§ 100a I No. 3 StPO states that telecommunications can be intercepted only if a successful investigation of the matter without surveillance would be "much more difficult or would offer no prospect of success" ("wesentlich erschwert oder aussichtslos"). This so-called subsidiarity clause can be seen as an application of the proportionality principle.[766] "Much more difficult" describes the situation where other investigative methods require more time to get the desired results and thus lead to undue delay in the criminal process.[767] The expenditure of labor and money for reaching the result of an investigation is normally not taken into consideration, except when the necessary amount of labor would be excessive.[768] "No prospect of success" means that no other investigative method is available, that alternatives would fail or would be unable to reach the goal of determining the relevant facts.[769]

The subsidiarity clause of § 100a I No. 3 StPO indicates a hierarchy between telecommunication surveillance and other investigative measures that can reach similar results. When more than one investigative measure is available for obtaining equivalent results, the one limited by the subsidiarity clause should not be chosen. The legislature has established an objective standard for comparison with other methods in order to prevent a purely subjective evaluation.[770] When all possible measures are limited by subsidiarity clauses, a hierarchy among them has to be established.

---

[764] Vgl. *Zöller*, StraFo 2008, 15, 19; BGH NStZ 10, 711, Orientierungssatz.

[765] The possibilities of the inadmissibility of the evidence on the ground of insufficient suspicion required by § 100a-c StPO can be found Section 3.b)cc), Chapter IV, Part II.

[766] More discussion about proportionality principle can be found in Section 1.d) of this Chapter.

[767] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 13; *Rieß*, Meyer-GedSchr, 1990, S. 385.

[768] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 13; *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 31. However, some authors argue that the required labor should not be taken into consideration. *Rudolphi*, in: Grünwald (Hrsg.), Festschrift für Friedrich Schaffstein zum 70. Geburtstag, 1975, S. 437. Others argue that both labor and money can be considered. *Dorsch*, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, 2005, S. 49.

[769] Vgl. *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Auflage, 2018, § 100a Rn. 45; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 13.

[770] BGHSt 41, 30, 35.

Subsidiarity clauses are not identical with the concept of "last resort" in common law systems,[771] since quite a few investigative methods are restricted by subsidiarity clauses in StPO instead of only one as the "last resort". Moreover, subsidiarity clauses in different paragraphs of StPO have their own system, consisting of different levels of subsidiarity for different investigative measures. Among these measures, the acoustic surveillance of the home is subject to the most restrictive subsidiarity standard, formulated as "other means … would be disproportionately more difficult or would offer no prospect of success" ("auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre") (§ 100c I No. 4 StPO). This measure is designed by the legislature to be "ultima ratio".[772] Then follows telecommunication surveillance (§ 100a I No. 3 StPO), surveillance of conversations outside the home (§ 100f I), collection of stored data (§ 100g II StPO), video surveillance (§ 100h II No. 2 StPO) and secret agents (§ 110a I StPO), which share the same level. Then comes police observation (§ 163e I StPO) and long-term observation (§ 163f I StPO) with the expression "other means …would offer much less prospect of success or would be much more difficult" ("auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre").[773] Finally, the collection of traffic data requires simply "necessary" ("erforderlich") and "in appropriate relation to the importance of the matter" ("in einem angemessenen Verhältnis zur Bedeutung der Sache steht") in § 100g I 1 and 3 StPO.

The system of subsidiarity clauses was introduced with good intentions but has become too complicated[774] and creates confusion. First, the hierarchies among the subsidiarity clauses are not totally clear. With this system, the legislature tried to create the impression of having established a ranking system according to the intrusiveness of each investigative method.[775] The less intrusive methods should be considered first.[776] With the same or very similar expressions of subsidiarity for different measures, however, it is very difficult to make a decision which measure should be the proper one in individual cases.[777] For instance, it leads to much confusion when prosecutors or judges have to decide between telecommunication surveillance and the measure of undercover agent since both have exactly the same requirement of subsidiarity. If both methods are available and the investigation would be "much more difficult or would offer no prospect of success" without either of the alternatives, then the requirement for neither is met because the prosecution could always choose the other, equally effective alternative. Schmitt argues that in this situation the prosecutor is free to choose among the measures with the same sub-

[771] See Section 2. b) cc) (3), Chapter IV, Part I.

[772] *Günther*, in: Kudlich, MüKoStPO, Band 1, 1. Aufl., 2014, § 100c, Rn. 35.

[773] Vgl. *Zöller*, StraFo 2008, 15, 19.

[774] *Blozik*, Subsidiaritätsklauseln im Strafverfahren, 2012, S. 233.

[775] Vgl. *Bernsmann/Jansen*, StV 1998, 217, 220.

[776] Vgl. *Zöller*, StraFo 2008, 15, 19.

[777] It is suggested that the levels of "Subsidiaritätsklauseln" should be reduced. See *Blozik*, Subsidiaritätsklauseln im Strafverfahren, 2012, S. 233.

sidiarity clause.[778] The BGH also observed this problem, and nevertheless decided that the measure of undercover agent is more, or at least not less intrusive than telecommunication surveillance, thus the former is not always to be considered first.[779] Secondly, a measure attached with a subsidiarity requirement implies that it is more intrusive than all those without a subsidiarity clause. This can be problematic in individual cases, such as the selection between the investigative measures with subsidiarity clauses and the search of a home (§ 102 StPO). According to a literal interpretation, the methods with subsidiarity clauses should only be adopted if the search of a home will not produce the desired result.[780] The search of a home, however, can be more intrusive in individual circumstances than measures with a subsidiarity requirement. Under the proportionality principle, less intrusive methods should always be considered first.

Due to its inefficiency, the necessity of subsidiarity clauses has been challenged and the introduction of a better terminology has been recommended.[781] Furthermore, such subsidiarity clauses should be limited to the most intrusive investigative methods.[782]

g) "Core Area of Privacy"

As stated in Section 1. b) aa) of this chapter, the term "core area of privacy" was first developed by the BVerfG in 1957, when it defined the untouchable area of human privacy.[783] This term was later incorporated into § 100c IV StPO.[784] Given the close relationship and similarities between § 100a (telecommunication surveillance) and § 100c (acoustic surveillance of a home), the BVerfG agreed to apply the same

---

[778] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 14.

[779] BGHSt 41, 30, 36 ("Mangels zulässiger Rüge bedarf es hier nicht der Entscheidung, in welchem Verhältnis die in den §§ 100a, 110a StPO geregelten Maßnahmen mit Blick auf den für sie jeweils geltenden Subsidiaritätsgrundsatz zueinander stehen. Insofern läge es aber eher fern, den Einsatz eines Verdeckten Ermittlers – entsprechend der Auffassung der Revision – als eine gegenüber der Telefonüberwachung grundsätzlich mildere und deswegen stets vorgreifliche Maßnahme anzusehen.").

[780] *Rieß*, Meyer-GedSchr, 1990, S. 370 and Fn. 10.

[781] *Zöller*, StraFo 2008, 15, 20 argues that "Subsidiaritätsklauseln" do not introduce any new idea or restrictions other than proportionality principle provided by GG. See also *Rieß*, Meyer-GedSchr, 1990, S. 390, the author criticized that the flexibility of investigative methods has been limited and the relevant terminologies should be defined more clearly. See also *Blozik*, Subsidiaritätsklauseln im Strafverfahren, 2012, S. 238, arguing that it is better to abolish "Subsidiaritätsklauseln" system.

[782] Vgl. *Rieß*, Meyer-GedSchr, 1990, S. 390. The discussion on the exclusion of evidence in case of violation of a subsidiarity requirement can be found in Section 3. b) cc), Chapter IV, Part II.

[783] BVerfGE 6, 32, 41.

[784] Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005.

protection on telecommunication surveillance in 2005.[785] As a consequence, TKÜG (BGBl. I 3198) added the term "core area of privacy" into the last version of § 100a IV StPO. In 2017, the legislature allowed another covert investigative measure, i. e. online search, under § 100b StPO, therefore, the legislature decided to regulate the "core area of privacy" in an independent provision (§ 100d StPO) instead of treating it separately in three provisions.[786] § 100d I and II StPO, however, provide more or less only the rules for excluding the information from the "core area of privacy"[787] without further explanation of what it actually is. The answer to this question can only be found in the earlier case law.

What kind of telecommunication falls within the "core area of privacy" follows the standards established by BVerfGE 80, 367 and 109, 279 discussed above.[788] A conversation dealing with concrete information on criminal activities, such as the plan or report of a crime, does not belong to the "core area of privacy" regardless of the relationship between the speakers.[789] In the context of § 100a III StPO, telecommunications between wife and husband do not get any special protection. Moreover, a spouse is even in a more vulnerable position because he or she is highly likely to be identified as a person who meets the requirement of § 100a III StPO as a communication helper.[790]

The BVerfG has recognized that it is not possible to absolutely prohibit the recording of telecommunications within the "core area of privacy" because it cannot be predicted in advance what communications will be recorded. That risk must be accepted and regarded as constitutional when the legal interests threatened by potential crimes are of particular importance.[791] Such communications must be deleted without delay and cannot be admitted as evidence at the trial.[792] Furthermore, they are not allowed to be used even as clues for further investigation.[793]

---

[785] BVerfGE 113, 349, 390, 391. This case also supported the preventive telecommunication surveillance.

[786] Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 24. August 2017.

[787] Thus, § 100d StPO will be discussed later in Section 3. a) aa), Chapter IV, Part II.

[788] See Section 1. b) aa) of this Chapter.

[789] See Fn. 605 and accompanying text. This decision conflicts with BGHSt 31, 296 where the incriminated conversation as background conversation between the couple was decided as "unantastbaren Bereich der privaten Lebensgestaltung".

[790] Of course, the partnership is given more consideration when the courts decide on the "Kernbereich privater Lebensgestaltung" issue.

[791] BVerfGE 113, 349, 392 ("Da bei der Anordnung einer Telekommunikationsüberwachung oder bei ihrer Durchführung aber nicht sicher vorhersehbar ist, welchen Inhalt die Gespräche haben werden, ist das Risiko nicht auszuschließen, dass die Abhörmaßnahme Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst. Verfassungsrechtlich hinzunehmen ist dieses Risiko allenfalls bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur zukünftigen Begehung der Straftat schließen lässt.").

[792] BVerfGE 113, 349, 392.

The BVerfG has stated that personal telecommunication enjoys less protection than live conversations in a home, because Art. 13 GG has an "especially close relation to human dignity".[794] The BVerfG also pointed out that Art. 10 I GG, in contrast to Art. 13 GG, provides no special restrictions on telecommunication surveillance but only refers to the general requirement of regulation by law.[795] That difference is reflected by the additional requirements for the surveillance of homes (§ 100c StPO) provided in § 100d IV StPO.[796]

§ 100d I StPO provides that "a measure in accordance with §§ 100a - 100c is not permissible if facts are giving rise to the expectation that only information from the core area of privacy will be collected". The protection offered by the "core area of privacy" in the telecommunication surveillance differs from that of the surveillance of a home. Telecommunication surveillance is in principle permitted under certain conditions and can only be denied if it is likely, under the circumstances, that only information from the "core area of privacy" will be collected. By contrast, the surveillance of a home is in principle not permissible, unless the facts indicate that the "core area of privacy" will not be infringed upon (§ 100d IV 1 StPO). Investigation of this matter is required before the measure can be approved.[797] In addition, the infringement upon the "core area of privacy" in a case of telecommunication surveillance is decided only upon the contents and the relationship between the persons talking, such as conversations among family members, with priests and lawyers.[798] Normally a surveillance order will not cover conversations with such persons. In the

[793] *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 25. More discussion can be found in Section 4, Chapter IV, Part II.

[794] BVerfGE 113, 349, 391 ("Der Schutz (von Art. 10 GG) ist allerdings anders ausgestaltet als der des Grundrechts der Unverletzlichkeit der Wohnung nach Art. 13 GG. Aufgrund des besonders engen Bezugs dieses Grundrechts zur Menschenwürde gewährt Art. 13 GG einen absoluten Schutz des Verhaltens in den Wohnräumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstellt… Die Bürger sind zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation angewiesen wie auf eine Wohnung.").

[795] BVerfGE 113, 349, 391 ("Dementsprechend normiert Art. 10 Abs. 1 GG anders als Art. 13 GG keine spezifischen Eingriffsvoraussetzungen, sondern verweist nur implizit auf die allgemeinen rechtsstaatlichen Anforderungen."). At the same time, BVerfG emphasized that Art. 10 GG guarantees the protection of free development in core area of private life. ("Die nach Art. 1 Abs. 1 GG stets garantierte Unantastbarkeit der Menschenwürde fordert auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung.").

[796] This has an impact on the standards of issuing a surveillance order and the exclusion of illegal evidence. BT-Drucks 16/5846, S. 44.

[797] BT-Drucks 68/5846, S. 43 – 44.

[798] See Section 2. c), Chapter I and Section 1. b) gg) and hh), Chapter II, Part II; see also Fn. 880 and the companying texts.

surveillance of a home, the location where communications take place also needs to be taken into consideration.[799]

3. Telecommunication Traffic Data (§ 100g StPO)

The collection of telecommunication traffic data plays an important role in criminal investigations, especially for offenses committed by means of telecommunication, such as fraud by use of the Internet or a telephone.[800] In addition, to locate a suspect through tracking his cell phone can also be helpful for arresting him or can serve as a piece of evidence for the later trial. The current version of § 100g StPO no longer requires that the measure be conducted "without knowledge of the person involved" ("auch ohne Wissen des Betroffenen") so that § 100g is no longer a measure of covert investigation.[801] This provision, however, imposes no obligation on the investigators to inform the person concerned in advance, hence in practice this remains by and large a covert measure.

§ 100g I - III StPO provides three different situations according to the types of data to be collected. § 100g I StPO refers to the traffic data defined in § 96 TKG and § 100g II StPO to the data described in § 113b TKG. § 100g III StPO regulates the collection of data in a cellular network ("Funkzellenabfrage"). § 100g IV StPO excludes from collection the data regarding professionals protected under § 53 StPO and § 160a StPO.

a) Collection of Telecommunication Traffic Data under § 96 TKG

aa) Definition

The definition of telecommunication traffic data ("Verkehrsdaten") under § 100g StPO can be found in § 96 I and § 113b TKG. It includes the numbers (IMSI und IMEI) of all participants or users, the exact time of the beginning and the end of a call and internet connection, the IP address, and other data necessary for maintenance of a telecommunication, as well as the amount of the data used.[802] The information on the location of cell phones or the equipment that provides access to the Internet can only be collected upon a judicial order (§ 100g I 3 StPO). The connection data stored by the participants after a communication are not covered by § 100g StPO but by § 100a

[799] BVerfGE 129, 208, 229 ("Zudem lasse sich bei der Überwachung der Telekommunikation die Gefahr einer Kernbereichsverletzung vor der Durchführung der Maßnahme kaum abschätzen, da sich der Kernbereichsbezug nicht aus der geschützten Räumlichkeit, sondern allein aus den (noch unbekannten) Gesprächspartnern und -inhalten ergeben könne.").

[800] *Bär*, NZWiSt 2017, 81.

[801] *Bär*, NZWiSt 2017, 81.

[802] Vgl. BT-Drucks 16/5846, S. 51.

StPO or by §§ 94 ff. and §§ 102 ff. StPO and can be collected under a normal seizure order.[803]

bb) Offenses Covered by § 100g I StPO

§ 100g I StPO allows for data collection if the person is suspected, "on the basis of certain facts", of having committed or participated in a criminal offence with substantial significance in the individual case, particularly one of the offences referred to in § 100a II StPO, or if he attempted to commit such an offence where the attempt is punishable, or has prepared such an offence by committing a criminal offence, or has committed a criminal offence by means of telecommunication. By referring to the crime catalogue of § 100a II StPO, § 100g I StPO offers examples of "a criminal offence with substantial significance". An order under § 100g I StPO can be made on the suspicion of an offense not listed in § 100a StPO, but the offense needs to be of equivalent significance in the individual case as those in the catalogue. The crimes committed by means of telecommunication (§ 100g I 1 No. 2 StPO) can be less serious than the crimes in the catalogue, given that it is not possible to investigate such cases without knowledge of the numbers of the connection used by the suspect.[804] In this case a higher standard of subsidiarity clause is introduced by § 100g I 2 StPO to balance the lower threshold of crimes committed by means of telecommunication.[805]

b) Collection of Data Stored under § 113b TKG

§ 113b TKG obligates telecommunication companies to systematically store certain data, such as telephone numbers of participants and the duration of telecommunications (§ 113b II and III TKG), for ten weeks (§ 113b I No. 1 TKG) and location information for four weeks (§ 113b I No. 2 TKG).

Given that disclosure of these data causes a more serious infringement on the privacy of telecommunication users than fragmental data, § 100g II StPO adopts a stricter standard for obtaining such information. § 100g II StPO requires an investigation of "especially serious offenses" rather than cases with "significant seriousness" in § 100g I No. 1 StPO and "serious offenses" in § 100a StPO. The corresponding catalogue in § 100g II StPO is also shorter than the one in § 100a StPO. A comparison between these two catalogues shows that some less serious offenses listed in § 100a StPO do not appear in § 100g II StPO, such as corruption, fraud, violation of anti-doping laws, and forgery of documents. In addition, some offenses, such as theft committed as a member of a gang and robbery, must have been serious

[803] § 100g V; and *Schmitt*, in: Meyer-Großner/Schmitt, StPO, 63. Aufl., 2020, § 100g, Rn. 44.

[804] *Schmitt*, in: Meyer-Großner/Schmitt, StPO, 63. Aufl., 2020, § 100g, Rn. 18.

[805] See Section 3. d), Chapter I, Part II.

("schwer") in § 100g StPO; and money laundering has to be even especially serious ("besonders schwer") in § 100g II 1 (g) StPO.

c) Traffic Data in a Cellular Network (Funkzellenabfrage)

§ 100g III StPO refers to all data that have been recorded by a cellular network in a certain period, in order to determine which cell phones or other equipments used this network during this time and thereby to identify suspects.[806] This data collection can only be ordered if cell phones with which incriminating conversations were made cannot be identified.[807] The measure does not focus on any concrete telecommunication from a certain cell phone or its location but extends to all data in a cellular network.[808]

Such an order was issued for the first time by the BGH investigating judge in a case where cables of trains were attacked in different places at the same time and it was believed that the suspects communicated with each other via cellphones during the commission of the crimes.[809] Since no suspects were identified by the police, the BGH agreed to collect the data from a cellular network.

This measure necessarily extends to data of persons not under suspicion ("Unbeteiligte Dritte"). It can therefore be taken only under strict conditions.[810] In accordance with § 100g III 1 StPO, only if the conditions provided in § 100g I No. 1 StPO are met and the proportionality principle (§ 100g III No. 2 StPO) and the subsidiarity clause (same as § 100a I No. 3 StPO) in § 100g III No. 3 StPO are respected can a measure be issued under § 100g III StPO.[811] Generally speaking, judges need to balance the interests of the investigation and the individual rights of the persons affected.[812]

d) The Subsidiarity Clause in § 100g

As stated above, a strict subsidiarity clause has been adopted in § 100g I 2 for crimes committed by means of telecommunication: the measure can only be used if it would be futile to investigate in any other way ("auf andere Weise aussichtslos

[806] *Schmitt*, in: Meyer-Großner/Schmitt, StPO, 63. Aufl., 2020, § 100g, Rn. 36; *Hilger*, GA 2002 228, 230.

[807] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100g, Rn. 52.

[808] *Graf*, in: Graf, BeckOK StPO, 39. Edition, 2021, § 100g, Rn. 47.

[809] BGH NStZ 2002 107.

[810] BT-Drucks 249/15, S. 33.

[811] BT-Drucks 249/15, S. 33.

[812] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100g, Rn. 53.

wäre").[813] The collection of location information is only allowed for the cases of § 100g I Nr. 1 when it is necessary ("erforderlich").

Although the subsidiarity clause in § 100g II StPO is the same as in § 100a I No. 3 StPO, i. e., "much more difficult or would offer no prospect of success" ("wesentlich erschwert oder aussichtslos wäre"), the shorter catalogue in § 100g II StPO shows that the collection of stored data is actually deemed more intrusive than the interception of telecommunication (§ 100a StPO).

The subsidiarity clause and the crime catalogue in § 100g III StPO are the same as in § 100a I No. 3 StPO. In addition, the data collection must be "in an appropriate relation to the gravity of the matter" ("in einem angemessenen Verhältnis zur Bedeutung der Sache").

The subsidiarity clause is regarded as an application of the proportionality principle, which balances the interest of data protection against the interest of criminal investigation. However, given the imprecise wordings of the various subsidiarity clauses, law enforcement officers are almost free to choose which investigative measures to apply in individual cases.

e) Protection of Professionals (§ 100g IV StPO)

The protection of professionals applies only to the data stored under § 113 TKG, i. e., § 100g II and III 2 StPO, not to the traffic data in § 100g I StPO. Moreover, the data of professionals is not exempted from systematic storage under § 113b TKG because their separation would technically not be feasible.[814] Yet, § 100g IV StPO prohibits criminal investigators from collecting stored data on which the professional could withhold testimony under § 53 I StPO.

II. Acoustic Surveillance (akustische Überwachung)

The interception of oral communications is provided for in two provisions, i. e., § 100c StPO for oral communications in homes and § 100f StPO for oral communications in public areas.

[813] BT-Drucks 16/5846, S. 52. More discussion on subsidiarity clauses can be found in Section 3. d), Chapter I, Part II.

[814] *Bär*, NZWiSt 2017, 81.

1. Acoustic Surveillance of Home

a) Art. 13 GG: Inviolability of the Home

Art. 13 GG is lex specialis in relation to the general personality rights guaranteed by Art. 2 and Art. 1 GG.[815]

aa) Historical Background

Art. 115 of *Weimarer Reichsverfassung* of 1919 guaranteed the inviolability of the home: "Every German's home is for him a sanctuary and is inviolable. Exceptions are allowed only based on laws."[816]

As a reaction to massive infringements upon human rights during the National-Socialist regime, the GG afforded civil rights the most prominent position. Its authors adopted the expression "the home is inviolable" ("die Wohnung ist unverletzlich") and placed it at the beginning of Art. 13 GG.

The first version of Art. 13 GG passed in 1949 consisted of only three paragraphs, i. e., Paras. 1, 2 and 7 of the current version. Art. 13 III - VI GG was added by the *Law to Modify the Basic Law (Art. 13) ("Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998").*[817] The proponents stated the purpose of this amendment as follows: "In the interest of an effective fight against organized crime in particular, the draft is to establish the constitutional foundation for the use of technical means of acoustic surveillance of homes for the purpose of criminal investigation."[818] The legislature further explained that organized crime had increased significantly in Germany, and that it was necessary for effective law enforcement to listen to and record the spoken word in homes, as confirmed by experts from police and prosecutor's offices.[819] This shows that the justification given for this amendment

[815] BVerfGE 109, 279, 326. Compared with Section 1. b) cc), Chapter I, Part II.

[816] "Die Wohnung jedes Deutschen ist für ihn eine Freistätte und unverletzlich. Ausnahmen sind nur auf Grund von Gesetzen zulässig." See *Huber*, Dokumente zur deutschen Verfassungsgeschichte, Band III, 1990, S. 146. A short summary of the historical development can also be found in BVerfGE 32, 54, 69.

[817] BGBl I S. 610.

[818] BT-Drucks 13/8650, S. 1 ("Der Gesetzentwurf soll im Interesse einer wirksamen Bekämpfung insbesondere der Organisierten Kriminalität die verfassungsrechtliche Grundlage für den Einsatz technischer Mittel zur akustischen Überwachung von Wohnungen zum Zweck der Strafverfolgung schaffen.").

[819] BT-Drucks 13/8650, S. 4 ("Das Organisierte Verbrechen hat in der Bundesrepublik Deutschland in der letzten Zeit erheblich zugenommen. Für eine wirksame Strafverfolgung in diesem Bereich ist es, auch nach Auffassung zahlreicher Experten aus der staatsanwaltschaftlichen und polizeilichen Praxis, notwendig, das gesprochene Wort in Wohnungen abhören und aufzeichnen zu können.").

is simply practical necessity. Art. 13 III GG[820] enables law enforcement agents to adopt such methods for criminal investigation and thus is regarded as the constitutional foundation for acoustic surveillance of homes in § 100c StPO.[821]

bb) The Definition of "Home"

Art. 13 GG guarantees individuals a spatial private area, which is important for one's free development. The person has a right "to be left alone" in this area.[822] "Home" ("Wohnung") is defined in Art. 13 GG as an area not accessible to the general public. Access can be prevented by a wall, a door or even only a sign.[823] Without doubt, a private home is "home". The question was raised whether a workplace is also covered by the term "home" although normal usage of this word refers only to space for living purposes. In order to include workplaces, the term "home" has been given two extensions, i. e., the home in the narrow sense ("Wohnung im engeren Sinne") and the home in the broad sense ("Wohnung im weiteren Sinne").[824]

The first category refers to the space for living and for the activities of private life. This is also how this German word is interpreted in daily life. Besides the house itself, the areas attached to the house, such as a private garden (or front garden[825]), cellar, stairs, terrace and a garage, are also regarded as part of "Wohnung". Moreover, hotel rooms, motor homes, and holiday houses have the same residential function and are also protected by Art. 13 GG. Cars that serve only for traveling, i. e., not as a place of living, however, are not covered by the term "Wohnung".[826]

The second category refers to spaces for business, work, or social purposes. The BVerfG has dealt with this question intensively in a judgment of 1971. In this case, the BVerfG held that the term "Wohnung" in Art. 13 GG includes spaces for business purposes.[827] It reviewed its constitutional history, the case law back to Prussian time

[820] Three of these new paragraphs serve to different purpose of such methods, namely, for crime investigation (Art. 13 III GG), for prevention of danger (Art. 13 IV GG), and for the protection of undercover agents or informants (Art. 13 V GG). Art. 13 VI GG requires a parliamentary control over such methods.

[821] BT-Drucks 13/8650, S. 4 ("Der neue Absatz 3 des Artikels 13 GG soll deshalb die verfassungsrechtliche Grundlage für entsprechende gesetzliche Regelungen schaffen.").

[822] BVerfGE 32, 54, 75.

[823] *Gornig*, in: v. Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, 7. Aufl., 2018, Art. 13, Rn. 15.

[824] *Gornig*, in: v. Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, 7. Aufl., 2018, Art. 13, Rn. 13 ff.; BGHSt 50, 206, 212.

[825] BGH NJW 1997, 2189, Nr. 20.

[826] LG Stendal NStZ 1994, 556; LG Freiburg NJW 1996, 3021; BGH NJW 1997, 2189, Nr. 19. It is still possible for a car to be considered as the "core area of privacy". Vgl. Section 1. b) ff), Chapter II, Part II.

[827] BVerfGE 32, 54, 68 ff.

as well as legal theories in Weimar time, and determined that the extension of the concept of "Wohnung" to spaces for business and organizational purposes has a long history.[828] The Court saw no reason to change this interpretation in modern times. Moreover, it found that it is essential for the free development of one's personality that one's work is not disturbed and that this requires an inviolable work space.[829] The Court thus reached the conclusion that "Wohnung" should be understood as a "spatial private area" ("räumliche Privatsphäre").[830] This interpretation is also important for preventing arbitrary searches.[831] In a case decided by the BGH, the office at issue was not open to the public and could only be used by a limited number of persons.[832] Following the case law of the BVerfG, the BGH stated that the understanding of "Wohnung" should go further than daily language and should include offices without general access, such as separate rooms in a club. The BGH, however, left open the question whether a hall open for public access should also be protected by Art. 13 GG.[833] Hospital rooms are also covered by Art. 13 GG. Because doctors or nurses have access to such rooms, however, such rooms do not have full protection like private rooms.[834] The same applies to rooms for consultation on drug problems.[835] Furthermore, the BVerfG has recognized that legal persons also enjoy the inviolability of the home under Art. 13 GG.[836]

The fact that technological measures of surveillance are expressly mentioned in Art. 13 GG shows that such methods are regarded as an infringement on the inviolability of "Wohnung", and thus need to be legitimated by law. This has also been confirmed by the BVerfG, which stated that the infringement of the right under Art. 13 GG refers not only to physical intrusions but also to the installation of apparatus and surveillance of activities with acoustic equipment.[837] It has been emphasized, however, that a conversation that is conducted within the house but can be overheard from outside without any special device is not covered by Art. 13 GG because the speakers themselves make overhearing possible.[838]

---

[828] BVerfGE 32, 54, 69. Vgl. Section 1. a) aa), Chapter II, Part II.

[829] BVerfGE 32, 54, 70.

[830] BVerfGE 32, 54, 72.

[831] BVerfGE 32, 54, 72, 73.

[832] BGH NStZ 1997, 196.

[833] BGH NStZ 1997, 196.

[834] BGHSt 50, 206, 212.

[835] BVerfGE 44, 353, 371 (seizure of documents of clients from a consultation on drug problems).

[836] BVerfGE 42, 212, 219 (searching the office of a newspaper company); BVerfGE 44, 353, 371.

[837] BVerfGE 109, 279, 327.

[838] BVerfGE 109, 279, 327. This situation can be covered by § 100h StPO when a recording device is installed outside the house.

cc) Restrictions of Inviolability under Art. 13 III GG

Art. 13 III 1 GG permits restrictions on the inviolability of the home for the purpose of criminal investigation. This restriction is limited to acoustic surveillance, photos may not be taken.[839] Secondly, measures may only be taken if certain facts indicate that an especially serious crime had been committed. Finally, a subsidiarity clause applies: "if the investigation of the matter by other means would be unproportionally difficult or futile" ("wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos ware").[840] In the explanation of the draft law, it has been noted that this measure should only be used as a final resort ("ultima ratio").[841] This reflects the cautious attitude of the legislature to the justification of intrusions of the home. According to the principle of legal certainty, the law must precisely define the offenses for whose investigation the measure may be used (Art. 13 III 1 GG).[842] § 100c StPO has by and large copied these requirements from Art. 13 III 1 GG and created a crime catalogue.[843]

b) § 100c StPO

After the modification of Art. 13 GG, acoustic surveillance of homes was first introduced into the StPO by the *Law to Improve the Combat against Organized Crime* in 1998.[844] Due to a decision of the BVerfG on the acoustic surveillance of homes,[845] the legislature had to reformulate § 100c StPO to ensure its constitutionality.[846] At the same time, the legislature emphasized the need for acoustic interceptions of homes for the fight against criminal organizations, terrorism and other especially serious crimes and for the identification of persons involved.[847]

---

[839] More limitations are provided by Art. 13 III GG, in Sentence 2, 3 and 4, which will be discussed in the procedural chapter.

[840] These criteria will be discussed in the context of § 100c StPO.

[841] BT-Drucks 13/8650, S. 5 ("Abhörmaßnahmen als besonders schwere Eingriffe in das Wohnungsgrundrecht dürfen nur ultima ratio der Strafverfolgung sein.").

[842] BT-Drucks 13/8650, S. 4 ("Aus Gründen der Rechtsklarheit und Rechtssicherheit muß dieser die in Betracht kommenden Delikte im Gesetz einzeln bestimmen und darf sich nicht auf eine generalklauselartige Umschreibung beschränken.").

[843] The crime-catalogue in § 100c will be further discussed in Section 1. b) bb), Chapter II, Part II.

[844] Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität, BGBl. I S. 845.

[845] BVerfGE 109, 279.

[846] Vgl. Section 1. b) ff), Chapter II, Part II.

[847] BT-Drucks 15/4533, S. 1 ("Die akustische Wohnraumüberwachung hat sich als unverzichtbar erwiesen, um die strafrechtliche Bekämpfung der organisierten Kriminalität, des Terrorismus und anderer besonders schwerer Formen von Kriminalität zu verbessern, insbesondere bei der Ermittlung und Überführung der Hauptverantwortlichen, der Organisatoren, der Finanziers und der Drahtzieher solcher Straftaten.").

After a restructuring of the relevant part of the StPO in 2017,[848] § 100c StPO contains only two paragraphs regulating the preconditions of acoustic surveillance of homes.

aa) Definition of "Not Publicly" ("nichtöffentlich")

§ 100c I StPO provides that not publicly spoken words[849] can be recorded with technological means without the knowledge of the persons concerned. The term "not publicly" is identical with the one in § 201 StGB.[850] Soliloquies, conversations or talks among a limited number of participants who prevent their words from being heard by random members of the public can be defined as not publicly spoken words.[851]

The intention of the participants plays a role in determining whether a conversation is public. If the speaker wants his words to be public or knows that they will be heard by the public, these words will be regarded as spoken "publicly" even if they are in fact not heard by any member of the public.[852] The general circumstances should also be taken into consideration. A conversation conducted in a home protected by § 13 GG but open to anyone is deemed to be a public one. By contrast, a conversation conducted in public but among selected people can be regarded as "not public".[853] The size of the audience is not relevant for the determination of "not publicly" spoken words. Instead, it depends on whether only persons who meet certain criteria may be present. For instance, a speech at a party meeting open only to party members or of persons with invitation letters is not a public speech.[854]

bb) Crime Catalogue of § 100c StPO

§ 100c StPO refers to the crime catalogue of § 100b II 2 StPO. This list is significantly shorter than the one in § 100a StPO. This shows a higher threshold of the measure under § 100c StPO. Under § 100c II 1 StPO, there are 13 offenses from StGB (from § 100c II (1) (a) to (m) StPO) compared to 21 offenses under § 100a II 1 No. 1(a) to (u) StPO. Only very serious crimes are listed in § 100b II 1 No. 1 StPO.[855]

[848] Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 24. August 2017, BGBl. I 2017 S. 3202.

[849] It is not necessary to be a conversation. For instance, the words that someone said to himself in a hospital room recorded by police were excluded from the evidence. BGH NStZ 2005, 700.

[850] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100c, Rn. 83.

[851] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100c, Rn. 83.

[852] *Eisele*, in: Schönke/Schröder, StGB, 30 Aufl., 2019, § 201, Rn. 9.

[853] *Eisele*, in: Schönke/Schröder, StGB, 30 Aufl., 2019, § 201, Rn. 8.

[854] *Eisele*, in: Schönke/Schröder, StGB, 30 Aufl., 2019, § 201, Rn. 8. The discussion about "nichtöffentlich" words in public areas can be found in Section 2. a) of this Chapter.

[855] § 100a II 1 (d) refers to the general crimes against public order.

Moreover, "besonders schwere Straftaten" are especially required for some crimes in the catalogue, for instance, "aggravated robbery and robbery resulting in death" ("schwerer Raub und Raub mit Todesfolge") in § 100b II 1 No. 1(i) StPO, "extortion by means of force" ("räuberische Erpressung") and "especially serious cases of extortion" ("besonders schwerer Fall einer Erpressung") in § 100b II 1 No. 1(j) StPO. The same goes for money laundering in § 100b II 1 No. 1(l) StPO, corruption in § 100b II 1 No. 1(m) StPO, Drug Law offenses (§ 100b II 1 No. 4(a) StPO), and weapons offenses (§ 100b II 1 No. 5(b) and No. 7(a)(b) StPO). The legal foundation of this crime catalogue is Art. 13 III GG, which requires "certain especially serious offense". Normally, such offenses should carry a maximum sentence of five years imprisonment or more.

In accordance with § 100c I 1 No. 2 StPO, the crimes have to be "especially serious" not only generally, but also in the individual case.[856] The seriousness of a crime can be determined through, for instance, the result and the involved legal interest of the criminal activities, and special circumstances.[857] Moreover, when there is a criminal network and several offenses are committed resulting in the violation of different legal interests, they can also be regarded as serious; a typical example is organized crime.[858]

cc) Concerned Persons and Concerned Homes

In principle, the measure under § 100c StPO may be taken only against suspects and in their home, not against any other person.[859] An exception is provided, however, in § 100c II 2 StPO: based on certain facts, homes of other persons may also be placed under surveillance if the suspect stays there and surveillance of the suspect's home will not lead to the discovery of the evidence or of the location of a co-defendant. The measure against third persons' homes can only be adopted when the suspect has been identified. According to the parliamentary document, however, it is permissible to adopt this measure against one suspect in order to collect information about an accomplice if the measure cannot be directed against the latter, or even in order to determine who is the accomplice, for instance, in the case of organized crime.[860] The

[856] BVerfGE 107, 299, 322.

[857] BT-Drucks 15/4533, S. 12 ("Als Anhaltspunkte für die Schwere der Tat nennt das Bundesverfassungsgericht beispielhaft die Folgen der Tat für betroffene Rechtsgüter, die Schutzwürdigkeit des verletzten Rechtsguts und das Hinzutreten besonderer Umstände, wie etwa die faktische Verzahnung mit anderen Katalogstraftaten oder das Zusammenwirken des Beschuldigten mit anderen Straftätern."). Vgl. Section 2. b), Chapter I, Part II.

[858] BT-Drucks 15/4533, S. 12 ("Diese Lage ist bei einem arbeitsteiligen, gegebenenfalls auch vernetzt erfolgenden Zusammenwirken mehrerer Täter im Zuge der Verwirklichung eines komplexen, mehrere Rechtsgüter verletzenden kriminellen Geschehens gegeben, wie es der verfassungsändernde Gesetzgeber für die organisierte Kriminalität als typisch angesehen hat.").

[859] § 100c II 1 StPO.

[860] BT-Drucks 15/4533, S. 13 ("Zulässig ist vielmehr auch die Erhebung von Daten als Beweismittel gegen eine mitbeschuldigte Person oder zur Ermittlung von deren Aufenthaltsort.

legislature evidently recognizes the important role played by this measure in the fight against organized crime and supports the use of information obtained from the measure against not only the suspect named in the judicial order but also against his accomplices.

In addition, § 100c II 3 StPO permits the measure even if other persons beyond the suspect are unavoidably affected. Such persons can be the conversation partners of the suspect, or persons who live in the same house or work in the same office as the suspect.

dd) Facts to Support Suspicion

The degree of suspicion necessary for issuing an order under § 100c StPO is identical with the one provided in § 100a I 1 No. 1 StPO, i. e., "certain facts to support the suspicion" ("bestimmte Tatsachen den Verdacht begründen").[861] There must be concrete indications or evidence to support the suspicion that individual catalogue crimes have been committed or are about to be committed. A mere assumption is not sufficient. For example, the *OLG Celle* explained that the mere fact that representatives of a company had regular meetings with a civil servant who assigned work for the city is not concrete enough to support the suspicion of cartel-building; evidence that is more directly related to cartel activities would have been required.[862]

ee) Subsidiarity Principle

§ 100c StPO contains a subsidiarity clause identical to the one in Art. 13 III GG, i. e., "would be disproportionally difficult or futile by other means". Although the law does not expressly say so, according to the parliamentary document on Art. 13 III GG it is clear that acoustic surveillance of a home should be the final resort ("ultima ratio").[863] Given the close relationship between Art. 13 III GG and § 100c StPO, the subsidiarity clause in § 100c I 1 No. 4 StPO should be interpreted in this way. Since the measure under § 100c StPO should be the last choice among covert investigative measures,[864] acoustic surveillance of the home should not be authorized if there are other investigative measures available.

Gerade in dem für Ermittlungshandlungen schwer zugänglichen Bereich der organisierten Kriminalität wird die Erhebung von Beweismitteln gegen Hintermänner häufig nur durch Maßnahmen möglich sein, die sich unmittelbar zunächst gegen im Vordergrund agierende mitbeschuldigte Personen richten. Dies ist etwa der Fall, wenn der Aufenthaltsort des Hintermanns nicht bekannt ist oder wenn dessen Wohnung dergestalt mit Sicherungseinrichtungen versehen ist, dass dort die Durchführung der Maßnahme faktisch nicht möglich ist.").

[861] See Section 2. e), Chapter I, Part II.

[862] OLG Celle StV 2011, 4, 217.

[863] Vgl. Fn. 841 and companying text.

[864] Detailed discussion and criticism on subsidiarity clauses can be found in Section 2. f), Chapter I, Part II.

ff) The Core Area of Privacy

In a landmark decision of 2004, the BVerfG discussed the constitutionality of this measure. The BVerfG did not find the acoustic surveillance of homes unconstitutional *per se* but required stricter preconditions and procedural guarantees.[865] The BVerfG extensively discussed the concept "inviolable core area of privacy" ("unantastbarer Kernbereich privater Lebensgestaltung"). It emphasized its close relation with human dignity and the absolute protection of this area. The concept of balancing of interests does not apply here, even if the public interest would prevail.[866]

The BVerfG, however, does not identify a physical space with the concept of "core area of privacy".[867] The BVerfG recognizes the important role of private homes as "ultimate refugium" for human dignity, but there is no absolute protection of this space. "Core area" rather refers to the highly personal behavior that takes place in this space.[868] Therefore, the physical space of a private home serves only as the basis for assuming that the conversations held in this space, in principle, fall within the scope of the "core area of privacy". Following the same logic, business offices enjoy lesser protection than private homes.[869] Both assumptions, however, are reversible depending on individual circumstances.[870] For example, if there is sufficient evidence to expect that conversations in a private home are probably crime-related, surveillance can be adopted. Conversely, highly personal conversations conducted in the workplace or an office can still belong to the "core area of privacy";[871] and the same applies to a soliloquy concerning information on a crime in a car.[872]

§ 100d IV StPO provides that the measure under § 100c may be ordered only if it is to be assumed, based on factual clues ("auf Grund tatsächlicher Anhaltspunkte"), that core private information will not be recorded. This requirement is impractical, however, especially where surveillance is applied in a private residence. For example, even if a couple living in a house together are highly suspected and there is enough evidence to show that their conversations will probably disclose criminal in-

[865] *Weßlau*, in: Roggan (Hrsg.), Lauschen im Rechtsstaat, 2004, S. 47.

[866] BVerfGE 109, 279, 313 ("Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen.").

[867] What kinds of contents should be regarded as "core area of privacy" were described by the BVerfG, see BVerfGE 109, 279, 313, 314; see also Section 2. g), Chapter I, Part II.

[868] BVerfGE 109, 279, 314 ("Die Privatwohnung ist als 'letztes Refugium' ein Mittel zur Wahrung der Menschenwürde. Dies verlangt zwar nicht einen absoluten Schutz der Räume der Privatwohnung, wohl aber absoluten Schutz des Verhaltens in diesen Räumen, soweit es sich als individuelle Entfaltung im Kernbereich privater Lebensgestaltung darstellt.").

[869] BVerfGE 109, 279, 321.

[870] This can also be called "Korrektur" function of concrete situations. *Weßlau*, in: Roggan (Hrsg.), Lauschen im Rechtsstaat, 2004, S. 51.

[871] VerfGE 109, 279, 321.

[872] In this case, discussed in detail above, the BGH applied the "core area of privacy" theory to a space covered by § 100f StPO (public space); BGH NJW 2012, 945.

formation, it can be expected that a large part of their conversations will be highly personal, for instance, discussing their sexual life. Therefore, because of the limits set by § 100d IV 1 StPO, very few judicial orders have been made under § 100c StPO.

gg) Protection of Close Relationships

The fact that a conversation is conducted between spouses or close family members is a factor supporting the assumption that core private information is likely to be involved, hence there should be no surveillance under § 100d IV StPO.[873] In addition to family members, close friends also belong to such close relationships. This proposition is problematic in light of the principle of legal certainty,[874] because the standards for determining what is a close relationship are not clear. It has been suggested in the literature that a close relationship should be assumed when the persons involved have the right to refuse to testify in accordance with § 52 StPO.[875] The BVerfG, however, has expressly differentiated the values behind the protection of close relationships from the right to refuse to testify on personal grounds in § 52 StPO. The former protects the special trust among persons with close relationships, while the latter is based on a formal criterion.[876] Conversations between good friends can fall within the "core area of privacy", while talks between relatives without mutual trust need not do so.[877] The BVerfG has introduced separate substantive standards to define close relationships. Yet, the existence of a relationship listed in § 52 StPO often implies mutual trust, which should be taken into consideration. This is also indicated by § 100d V StPO, providing that in the case of § 52 StPO results from surveillance measures can only be used when this is not disproportionate to the interest in establishing the facts or determining the location of suspects if the significance of the underlying relationship of trust is taken into consideration.

hh) Protection of Professionals

Although the BVerfG recognized that the value behind § 53 StPO is to protect the mutual trust between some groups of professionals and their clients (suspects in this context), the BVerfG divided the professionals in § 53 StPO into three categories according to the different purposes of such protection.[878] The first category refers to clergymen and lawyers, whose advice often plays an important role in protecting human dignity, by permitting the faithful to discuss issues of an intimate character in a religious context, and to avoid being a mere object of the legal process, re-

[873] BVerfGE 109, 279, 319.

[874] *Warntjen*, Zwangsmaßnahmen, 2007, S. 99.

[875] *Warntjen*, Zwangsmaßnahmen, 2007, S. 99.

[876] BVerfGE 109, 279, 322.

[877] *Bludovsky*, Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100c Abs. 1 Nr. 3 StPO, 2002, S. 87.

[878] BVerfGE 109, 279, 322, 323.

spectively.[879] Doctors belong to the second category; their conversations with patients can be regarded as core private information only in individual cases. Journalists and representatives of parliament belong to the third category: conversations with these professionals are not covered by "the core area of privacy", because the protection of § 53 StPO aims to guarantee, for instance, the function of the parliament, not the privacy of individuals.[880]

Such a distinction, however, cannot be found in § 100d V StPO, which applies to all professionals listed in § 53 StPO, without further explanation on which grounds different professionals are protected. The "bleibt unberührt" ("remains unaffected") clause in § 160a V StPO shows that the rules of § 100d V StPO apply exclusively and supersede those of § 160a StPO regarding the surveillance measures under §§ 100b and 100c StPO (online search and acoustic surveillance of homes). This means that such surveillance measures are generally prohibited regarding the professionals listed in § 53 StPO, whereas § 160a II StPO requires a balancing between the interest of the fight against crime and professional secrecy where the professionals in § 53 I 1 No. 3 to 3b or No. 5 StPO are involved. An explanation may be that the representatives of these professions persuaded the legislature that their buildings and computer systems should be free from state intrusion. § 100d V StPO provides that "§ 160a IV applies accordingly". This means that the surveillance measures under §§ 100b, 100c StPO may be used against professionals protected by § 53 StPO if they are suspected of having been accessories (even after the fact) of the crime under investigation.[881]

2. Acoustic Surveillance in Public Areas (§ 100f StPO)

§ 100f StPO regulates acoustic surveillance "outside homes" ("außerhalb von Wohnraum"), i. e., in a space not covered by the definition of "Wohnung" under Art. 13 GG[882] and § 100c StPO.

a) The Borderline Cases between § 100c and § 100f StPO

In this Chapter, "home" has been defined as a space where members of the public cannot enter without permission. In some cases, however, the legal nature of spaces is doubtful. The BGH held that the visiting room of a jail is not a "home" in the meaning of Art. 13 GG because such rooms and the cells can be entered by officials without

[879] BVerfGE 109, 279, 322.

[880] BVerfGE 109, 279, 323; 129, 208, 231 ff.

[881] See Section 2. c) cc), Chapter I, Part II.

[882] See Section 1. a) bb), Chapter II, Part II.

the agreement of the detainees in accordance with the rules of the facilities.[883] The detainees have no right to privacy in such areas.[884] Moreover, in principle, the "core area of privacy" rules provided in § 100d StPO do not apply to areas outside a home.[885] The BGH declared, however, that a conversation between a pretrial detainee and his wife in a visiting room of the jail could nevertheless be protected by the "core area of privacy" doctrine due to the close personal relationship of the persons involved; but in the case at hand the BGH concluded that the conversation was, on principle, subject to surveillance because there was a reasonable expectation that the spouses would talk about criminal offenses. The result of the surveillance was nevertheless held to be inadmissible because the authorities had misled the persons involved about the privacy of their talk and thus violated the principle of fair trial.[886]

A car is generally not regarded as "home" and thus the interception of conversations in a car is regulated by § 100f StPO. Only in exceptional cases (e. g., if the driver speaks to himself) must a recording be excluded from the evidence based on the "core area of privacy" theory.[887]

A further problem concerns the question whether words can be spoken "non-publicly" although they are pronounced in a public area. So-called "factually public conversations" ("faktisch öffentliche Gespräche") are conversations or telephone calls held in a public area, such as on the street or in a bus. Such conversations are regarded as publicly spoken words, thus can be recorded without a judicial order under §§ 161, 163 StPO.[888] What, then, are "non-publicly" spoken words in a public space? Does the speaker have to make a special effort to indicate that the talk is not public? For example, does it make a difference whether a street where the person is making a phone call is empty or busy? What if persons intend to create a private space in a public area, for instance, by sitting alone in the far corner of a cafe? Is a police officer allowed to use a device with a sound-enhancing function to catch the sound from a far distance? Given the definition of "nichtöffentlich" discussed in Chapter II, the only way to make words spoken in a public area non-public is for the speaker to

[883] BGH 53, 294, 300. The same conclusion can also been seen in BGH 44, 138. However, at the time when BGH 44, 138 was decided in 1998, there were no special rules in StPO for the interception outside of "Wohnung". See also BVerfGE, NJW 1996, 2643. There was also opposite opinion, which argued that the celle in prison should be regarded as "Wohnung" in certain degree. *Bernsmann*, in: Feltes/Pfeiffer/Steinhilpe (Hrsg.), Kriminalpolitik und ihre wissenschaftlichen Grundlagen, 2006, S. 515.

[884] BGH 53, 294, 300.

[885] BGH 53, 294, 301, 301. The BGH, however, did not exclude the situation where the interception of communications outside of the "Wohnung" can involve the core area of privacy in the individual cases. For instance, the case BGH, NJW 2012, 945 is a good example, where the BGH decided the self-conversation in a car fall within the scope of "the core area of privacy". BGH, NJW 2012, 945. See also Section 1. b) ff), Chapter II, Part II.

[886] BGHSt 53, 294, 303 – 305.

[887] BGH, NJW 2012, 945.

[888] *Eisele*, in: Schönke/Schröder, StGB, 30 Aufl., 2019, § 201, Rn. 9; see also *Hilger*, NStZ 1992, 457, 462, Fn. 96; *Graf*, in: Graf, BeckOK StPO, 39. Edition, 2021, § 100c, Rn. 6.

take measures to exclude an audience. This is neither possible on a public street nor in a café during its business hours, whether empty or not. In both situations the speaker cannot prevent people from walking by or from sitting next to him, listening to what he is saying.

b) Conditions for Acoustic Surveillance outside Homes (§ 100f I StPO)

Generally speaking, the preconditions for an acoustic surveillance outside homes provided in § 100f I StPO are similar to those provided in § 100a StPO.[889] The crime catalogue in § 100f I StPO refers to § 100a II StPO and also requires that the offenses are serious in the individual case under investigation.[890] The subsidiarity clause in § 100f I StPO is exactly the same as the one in § 100a I No. 3 StPO, i. e. "other means of establishing the facts or determining the suspect's whereabouts would be significantly more difficult or would offer no prospect of success."[891]

If police officers listen to non-public communications covertly without using technical devices this is not subject to § 100f StPO but is permissible under § 161 and § 163 StPO.[892] Investigators can testify as witnesses on what they heard. It is also not practical to introduce a special judicial order process for "just listening", since people hear others' conversations daily, especially in public spaces.

For installing the technical equipment for surveillance, the police often need to get access to the object in question (e. g., a car). According to the dominant view, § 100f StPO also covers necessary preparatory and "accompanying" measures ("Begleitmaßnahmen"), subject to the principle of proportionality.[893] The opposing view would require a separate judicial order for the requisite intrusion into the suspect's property and private sphere.[894]

c) Persons Affected by the Measure

Acoustic surveillance outside of a home can be adopted against suspects and non-suspects who have a connection with the suspect. An unavoidable involvement of

[889] See *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100f, Rn. 2.

[890] See Section 2. b), Chapter I, Part II.

[891] § 100a I No. 3 StPO provides: "die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre." The discussion about this expression of the subsidiarity clause and problems of the "Subsidiaritätsklausel" system can be seen Section 1. f), Chapter I, Part II.

[892] *Hilger*, NStZ 1992, 457, 462, Fn. 97.

[893] BGHSt 46, 266, 271; AG Hamburg StV 2009, 636, 637; *Janker*, NJW 1998, 269; *Schneider*, NStZ 1999. 388, 388.

[894] See BGH NJW 1997, 2189; *Bernsmann*, StV 2001, 385; *Wolter/Greco*, in: Wolter, SK-StPO, 5. Aufl., 2016, § 100f, Rn. 7.

third persons is legitimate. This rule is a combination of § 100a III StPO and § 100c II 2 StPO.

The protection of non-suspects is a critical issue here because the surveillance takes place in public space. To minimize the involvement of unrelated non-suspects, § 100f II StPO provides three preconditions for the surveillance of non-suspects outside of a home: 1) having a connection with a suspect; 2) only for the purpose of the investigation of facts or the location of suspects; and 3) only if the investigation with other means would be futile or significantly more difficult (subsidiarity clause). Two categories of non-suspects deserve special attention, i. e., relatives of suspects listed in § 52 StPO (and the persons with intimate relations with suspects) and professionals as listed in § 53 StPO. According to the BGH, since surveillance of family members of suspects is allowed even in the home, there is no problem in applying § 100f StPO to them.[895] According to § 100d V StPO, evidence from measures under § 100c StPO affecting relatives of the suspect may be used only if the intrusion into the family relationship is not out of proportion to the interest of the investigation. § 100f StPO does not have a similar restriction on the use of the results of surveillance outside the home. Information gained from measures under § 100f StPO against relatives of suspects is therefore admissible unless the "core area of privacy" has been infringed upon.[896] By contrast, surveillance of defense lawyers, clergy, and members of parliament as listed in § 53 I Nos. 1, 2 and 4 StPO is generally impermissible, even outside of the home, and the results of such surveillance are inadmissible in accordance with § 160a I StPO. The BVerfG has justified this difference by arguing that the professionals in § 53 StPO are forbidden to disclose the related information to anyone, not only the investigators (§ 203 StGB), while the persons named in § 52 StPO are not subject to this rule.[897] Thus, suspects should know that what they tell their relatives can be disclosed to third persons and take the risk.[898] The most controversial problem in the context of surveillance here, however, is not that suspects are "betrayed" by their relatives, rather that the conversations are overheard by the police while the relatives keep the secret. The meaning of § 52 StPO, i. e., to protect the trust relationship among family members and relatives, would be lost if the covert surveillance of communications between suspects and their relatives can be used to bypass § 52 StPO.[899]

[895] *Duttge*, JZ 1999, 261, 263.

[896] See BVerfG StV 2011, 261. The case BGH 53, 294 (surveillance of conversations between a couple in the visiting room of a prison) shows that the surveillance under § 100f StPO is also subject to the "core area of privacy" theory although § 100d StPO applies only to §§ 100a-c StPO. The judicial order in this case is against suspect, however, without doubt, the same will apply when the relatives of suspects are intercepted.

[897] BVerfGE, StV 2011, 261, 262.

[898] BVerfGE, StV 2011, 261, 262.

[899] The same criticism applies to §§ 100a, 100b, 100c StPO.

III. Procedure

In the latest version of StPO enacted in 2017, the procedural requirements for §§ 100a - 100c StPO have been integrated into one provision (§ 100e StPO). The procedure for the measure of § 100f StPO is subject to § 100e StPO in accordance with § 100f IV StPO. This is only a structural modification, and the substantial contents have largely been left unchanged. The contents of the former § 100b and § 100d StPO have been moved to § 100e StPO and those different rules still apply separately to § 100a and §§ 100b StPO and 100c StPO in accordance with § 100e StPO.

1. Jurisdiction of the Issuing Court and of the Prosecution

a) Jurisdiction of the Issuing Court

aa) Telecommunication Surveillance under § 100a StPO

No preventive judicial control system can be found in Art. 10 GG. Nevertheless, § 100e I StPO provides for the issuance of a surveillance order by a judge as a principle and by prosecutors only in situations of emergency ("bei Gefahr im Verzug").[900] In the latter situation, the order becomes invalid if it is not approved by the judge within 3 days after it had been issued by the prosecutor.[901] Courts, as neutral and independent institutions, are in the best position to act as "control organs" and to prevent the abuse of telecommunication surveillance.[902]

The jurisdiction of the court for an order of telecommunication surveillance is subject to the general rules concerning the jurisdiction on investigative measures regulated in § 162 StPO (jurisdiction of investigating judge ("Ermittlungsrichter") of *Amtsgericht* [AG]) and § 169 StPO (jurisdiction of *Oberlandesgericht* [OLG] and BGH).[903] Investigating judges of AG are in principle in charge of issuing orders for investigative measures upon application by prosecutors whose offices are located in their jurisdiction. Jurisdiction is thus organized based on territoriality, not by the seriousness of the measure. The same rule applies to surveillance outside of homes in accordance with § 100f IV StPO.

bb) Acoustic Surveillance of a Home

Whereas investigating judges at AG may order telecommunication surveillance, the legislature shows a more cautious attitude towards surveillance of homes by

[900] According to BVerfG, Art. 13 GG shows the same idea. BVerfGE 103, 142, 153.

[901] § 100b I StPO.

[902] BVerfGE 107, 299, 325; *Gusy*, JZ 2001, 1033, 1034.

[903] *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100e, Rn. 4.

providing that only a special criminal chamber of a *Landgericht* (LG) at the seat of an OLG has jurisdiction to issue an order for such a measure.[904] As a result of the high substantive barriers in § 100c StPO, there are extremely low numbers of orders issued for the acoustic surveillance of homes, i. e., one case per year in some states, and no case at all in other states.[905] Since the number of applications submitted by prosecutors is not published, it is not possible to estimate how many applications are rejected by the courts. It is nevertheless evident that home surveillance is authorized only in exceptional situations.

In accordance with § 74a IV *Gerichtsverfassungsgesetz* (GVG) the special criminal chamber of LG is a chamber of LG that is not seized of main proceedings in criminal matters. This scheme has been suggested by the BVerfG, which argued that the chamber in charge of the main proceedings should not receive any information about the case before the defendants have been identified.[906]

The prosecutor submits the application for a judicial order to the LG where the prosecution office is situated. This means that the Federal Attorney General (*Generalbundesanwalt*, GBA) applies to the *LG Karlsruhe.* An appeal against the LG's decision will be decided by the corresponding OLG. In this situation, a division of the OLG that is not seized of main proceedings has jurisdiction according to § 120 IV GVG.

b) Jurisdiction of the Prosecutor "bei Gefahr im Verzug"

§ 100e I StPO provides that in an emergency (*bei Gefahr im Verzug*) the prosecutor may issue an "emergency order" for surveillance of telecommunication, while § 100e II StPO authorizes presiding judges to issue orders of home surveillance in emergency situations. The expression "bei Gefahr im Verzug" can also be found in Art. 13 GG, § 98 StPO (seizure) and § 105 StPO (search). That expression is a compromise between the necessity of judicial review for the protection of personal rights and the need of efficient law enforcement. The BVerfG has defined "Gefahr im Verzug" as a situation where the effectiveness of the procedural measure will be endangered by the delay caused by the application for a judicial order.[907] The BVerfG emphasized that an "emergency order" can only be an exception and should not be used to undermine the principle of judicial control.[908] Therefore, "Gefahr im Verzug"

[904] § 100e II StPO.

[905] Statistics for the acoustic surveillance of "Wohnung" in Germany can be found https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Wohnraum/Wohnraumueberwachung_node.html, visited at 25.12. 2018.

[906] BVerfGE 109, 279.

[907] BVerfGE 51, 97, 111; 103, 142, 156. According to an interview with a prosecutor, judges sometimes cannot be reached even during working hours. *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 105.

[908] BVerfGE 103, 142.

must be strictly interpreted. Furthermore, the existence of such a situation needs to be supported by facts of the individual case, not only an abstract assumption or general experience.[909] In order to enhance judicial control *ex ante* and to reduce abuse of the emergency power, the BVerfG has required courts to offer organizational support and establish an "emergency service" to guarantee their accessibility.[910] According to § 22c GVG, each German state may regulate the accessibility of their judges. For example, Bayern, Brandenburg, Hessen, Nordrhein-Westfalen, and Saarland require courts to ensure the accessibility of a judge between 6 and 21 o'clock.[911]

In order to provide an effective judicial *ex post* review of emergency orders, the BVerfG further requires that the materials that supported the "emergency order" made by the prosecutor should be presented to the judge.[912] This means that any facts supporting the suspicion, the expectation of evidence to be found, and the need to act immediately should be included in the application for a judicial confirmation order.[913] A general declaration that "there exists an emergency situation" is not sufficient.[914] In addition, the materials must show whether the prosecutor tried to reach the judge and the reason why he did not succeed.[915] Police or prosecutors must not themselves cause an emergency situation by delaying an application for a judicial order.[916] The BGH made it clear that evidence obtained without a judicial order can be excluded if judicial *ex ante* review was avoided intentionally or arbitrarily.[917]

The judicial rules described here mainly concern conventional searches and seizures. Regarding telecommunication surveillance, prosecutors rarely take emer-

[909] BVerfGE 103, 142, 155 ("Im Konkreten sind reine Spekulationen, hypothetische Erwägungen oder lediglich auf kriminalistische Alltagserfahrung gestützte, fallunabhängige Vermutungen als Grundlage einer Annahme von Gefahr im Verzug nicht hinreichend. Gefahr im Verzug muss mit Tatsachen begründet werden, die auf den Einzelfall bezogen sind. Die bloße Möglichkeit eines Beweismittelverlusts genügt nicht."); AG Essen StraFo 08, 199, 200; *Amelung*, NStZ 01, 337; *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 42.

[910] BVerfGE 103, 142, 156 ("Dem korrespondiert die verfassungsrechtliche Verpflichtung der Gerichte, die Erreichbarkeit eines Ermittlungsrichters, auch durch die Einrichtung eines Eil- oder Notdienstes, zu sichern.").

[911] https://www.rechtslupe.de/strafrecht/der-nicht-erreichbare-ermittlungsrichter-oder-anforderungen-an-einen-richterlichen-bereitschaftsdienst-3139932#richterlicher-bereitschaftsdienst-in-den-bundeslndern, visited at 25.04.2021. It reports some empirical studies in the regions where 24-hour accessibility is provided, such as Amtsgericht Neuruppin since 2010. The statistics show that the accessibility between 21 o'clock and 6 o'clock is not necessary because judical orders are pursued very rarely during this period.

[912] BVerfGE 103, 142, 159, 160.

[913] BVerfGE 103, 142, 160.

[914] BVerfGE 103, 142, 160.

[915] *Müller/Trurnit*, StraFo 08, 144, 145; AG Essen StraFo 08, 199, 200.

[916] *Müller/Trurnit*, StraFo 08, 144, 145; AG Essen StraFo 08, 199, 200.

[917] BGH 51, 285. More discussion on this case can be found Section 3.b)aa), Chapter IV, Part II. See also StraFo 07, 465.

gency measures.[918] According to an empirical study, 12 % of telecommunication surveillance orders were "emergency orders", and only 5 % of them were not later confirmed by a judge.[919]

c) Judicial Control

As has been shown above, a judicial order is needed for surveillance either in advance, or afterwards in an emergency situation. Nevertheless, police dominate the decision-making in this area of the law. According to an empirical study of 2003, 88 % of the application materials were prepared by police, and prosecutors made applications to the judge based exclusively on these materials in 97 % of the cases.[920] Police often discuss with prosecutors the possibility of a surveillance order in advance. If prosecutors orally reject such a measure, police will not initiate the process.[921] Police may call the judge directly and ask whether a potential application will be approved so that they can decide whether it is worth drafting an application. In such a situation, applications are then normally approved by judges.[922]

The only information source for judges when requested to issue an order is the materials prepared by police and prosecutors. In other words, judges have no way to collect information to check the reliability of the information in applications. Judges therefore hesitate to reject an application for a surveillance order filed by the prosecutor.[923] In practice, judges may not even be interested in reading through the files and often only ask where to make their signature.[924] One judge said in a conference that he is not sure that he could make a smarter decision based on the files presented by the police and examined carefully by prosecutors.[925] In addition, to reject an application takes more time for judges than to approve it.[926] According to an empirical study, judges just signed 92.3 % of draft decisions prepared by prosecutors without any changes.[927] Statistics published by researchers of the Max Planck In-

[918] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 53, 54, 79, 110; *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung, 2003, S. 451.

[919] *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung, 2003, S. 452. Another empirical study found that 20.5 % of orders for telecommunication surveillance were "emergency orders"; *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 53.

[920] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 37–39. The dominating position of police is also confirmed by interviews of police. *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 73, 75.

[921] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 39.

[922] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 110.

[923] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 91.

[924] *Deckers/Gercke*, StraFo 2004, 84, 87.

[925] *Deckers/Gercke*, StraFo 2004, 84, 87.

[926] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 110.

[927] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 46.

stitute for Foreign and International Criminal Law in Freiburg[928] show a similar tendency: more than 90 % of applications made by prosecutors were approved by judges without any changes, 4 % of them were supplemented, while only 1 % were changed.[929] The orders issued without changes were not necessarily of good quality.[930]

2. Criteria for Judicial Review of an Application

While § 100e StPO provides procedural requirements for the measures under §§ 100a - 100c StPO, the substantive criteria for each measure are stated in the relevant provisions; in addition, constitutional restrictions such as the protection of the "core area of privacy" must be taken into consideration. The following criteria are to be examined by the courts: a) whether the suspected offenses are included in the applicable crime catalogue; b) whether there are sufficient facts to support the suspicion of a catalogue crime;[931] c) whether the police or the prosecutors have the technical ability to obtain the desired results without violating the rules (§ 100a V StPO); d) whether the measures sought will infringe upon the "core area of privacy", e) the necessity and the proportionality of the measures, and f) the subsidiarity clauses in the relevant provisions.

The potential costs of the implementation of the measures are not a legally relevant factor to be taken into the consideration. This factor is neither mentioned in any legal texts regarding covert investigative measures nor included in the statistics regarding surveillance of telecommunication released by the Federal Ministry of Justice.[932] Moreover, since prosecutors do not need to include information on potential costs in their applications for a surveillance order, the courts have no basis to make a proper decision on this point. Prosecutors may, however, consider the cost of a measure before applying for its authorization.

---

[928] Since 2020 the institute was renamed as Max Planck Institute for the Study of Crime, Security and Law.

[929] *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung, 2003, S. 452.

[930] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 48 – 52.

[931] Vgl. Section 2. e), Chapter I, and Section 1. b) dd), Chapter II, Part II.

[932] https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html, visited at 24. 04. 2021. However, the costs are included in the statistics on acoustic surveillance under § 100c StPO. https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Wohnraum/Wohnraumueberwachung_node.html, visited at 24. 04. 2021.

3. The Contents of a Surveillance Order

§ 100e III StPO regulates what information should be included in a surveillance order issued in accordance with §§ 100a - 100c StPO.

All such orders must be in writing, even if there is "danger in delay". They should to the extent possible include the name and the address of the persons against whom the measure is issued (§ 100e III No. 1 StPO). Yet, an order can be issued even if the identities of all the participants have not been established in the case of a meeting of a criminal organization. Third persons can also be listed in accordance with § 100c II StPO.

The investigation of a catalogue crime (§ 100e III No. 2 StPO) is a key element to justify a surveillance order. § 100e III Nos. 3 and 4 StPO requires the order to describe the type, the applicable scope, the duration, and the time for the termination of the surveillance, as well as the type of information to be obtained. The following details should be provided: a) what technical equipment is to be used; b) how the equipment is to be installed; c) whether real-time surveillance is necessary; d) whether the surveillance should only be implemented when a certain person is present, or for a certain period; and e) what information is expected to be obtained and its relevance for the investigation.[933]

The dial number or equivalent codes must be indicated for a telecommunication surveillance (§ 100e III No. 5 StPO), while § 100e III No. 7 StPO requires the exact description of the home or certain rooms to be put under surveillance.

§ 100e IV StPO further requires that the court should indicate grounds for issuing the order.[934] The facts to support the suspicion, the necessity, and the proportionality of the measures as well as the reasons why core private information will not be obtained should be included. Although these questions will be examined by the courts in any case,[935] the law requires the judges to write down their considerations.

The list in § 100e III and IV StPO should be understood as providing a minimal standard. Courts are thus free to add more information if they think it is necessary. The idea behind the list of minimal contents of a surveillance order is to describe the surveillance activities as precisely as possible and to ensure that the surveillance will be conducted only in relation to the crimes named in the order. With this list, the legislature and the courts try to reduce unnecessary intrusions into privacy.[936]

Moreover, the information included in the order is an important basis for determining later whether the order complied with StPO and whether certain parts of

[933] Vgl. *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100e, Rn. 9 ff.

[934] This is also subject to § 34 StPO providing generally that reasonings should be given for a judge decision.

[935] See Section 2, Chapter III, Part II.

[936] The discussions on the accidental results from a surveillance can be found: Section 2. d), Chapter I, Part II.

recorded conversations should be excluded from the trial. An exact description makes it possible for a higher court to examine the order and for a defense lawyer to challenge the legality of the measures, for instance, if the recording shows that the surveillance has massively excceded the scope allowed by the order.

4. Duration and Extension of Surveillance

The different degrees of intrusion between the surveillance of telecommunication and of homes are reflected in the different rules on the duration and extension of different measures. § 100e I StPO provides that the order of telecommunication surveillance can extend to a maximum of three months and can be prolonged for another three months at a time. There is no limitation, however, on how many times a surveillance order can be prolonged, and jurisdiction for extensions remains with the same court. § 100e II StPO, however, allows only one month for a first-time surveillance under §§ 100b and 100c StPO, and for prolongation for another month each time. If the total duration of the surveillance has reached six months, further extensions need to be ordered by the OLG, which can be regarded as an additional procedural control.[937] Moreover, the beginning of the duration is the time when the order is issued, not the time when the measures are implemented.[938] The same rule applies to extension periods.[939]

Regardless of the different rules on duration, § 100e I and II StPO emphasize that, courts should examine each application for an extension in the same way as a new application, i. e., take into account the obtained information and examine whether the conditions justifying the measure continue to exist, including the proportionality of the measure.[940]

An empirical study shows that about 90 % of judicial orders on telecommunication surveillance were issued for three months, while 60 % of all telecommunication surveillance measures were conducted for only two months or less. An extension was issued in only 9 % of cases.[941]

5. Implementation of Surveillance

In accordance with § 36 II StPO, the prosecution office which applies for the judicial order is also responsible for the implementation of the surveillance. The surveillance can be conducted with equipments installed by the police or with the

[937] BT-Drucks 15/4533, S. 28.

[938] BGH 44, 243.

[939] BT-Drucks 16/5846, S. 46.

[940] BGH NStZ-RR 11, 148. See Section 2, Chapter III, Part II.

[941] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 59.

help of telecommunication companies for a telecommunication surveillance. In the latter situation, the prosecution office shall send the original order or an authenticated copy to the telecommunication company by post, or in an emergency, the prosecution office can also send it by fax or email but needs to send the paper version within one week (§ 12 II TKÜV). Telecommunication companies are obliged to cooperate with the investigators.[942] Such cooperation, however, means only that the companies offer technical assistance, but their staff members are not allowed to listen to the intercepted conversations.[943] When core private information may be involved, the police may conduct real-time surveillance in order not to record such information. This can also be required by the judicial order.[944]

Moreover, due to the proportionality principle, surveillance should be limited to conversations of the person referred to in the order. When the conversation is conducted only among third persons, surveillance should be immediately terminated. The part that has been already recorded should be deleted and cannot be used at trial.[945]

6. Termination of the Order

The judicial order indicates the longest period for which surveillance is allowed. According to § 100e V StPO, surveillance must be terminated as soon as the conditions for the measure cease to exist, for example, when there is no more suspicion or the measure is regarded as unnecessary or useless for reaching the desired results.[946]In that case, the prosecution office shall order the police or telecommunication company to terminate the surveillance and then report the results to the court. In the case of a measure under §§ 100b and 100c StPO, the prosecution office should also inform the court about the whole process. The court may require the prosecution office to submit necessary information at any time for judicial control. If the court finds that the conditions for the order no longer exist, the court shall order the termination of the measures, unless termination has already been initiated by the prosecution office. Termination of the measure may also be ordered by the presiding judge. Once the surveillance has been terminated, a new order is needed for restarting it.[947]

It is doubtful, however, whether the prosecution office can find out about changes in the conditions in time, since it is the police that actually conduct the inves-

[942] § 100a IV StPO. Telecommunication companies cannot reexamine whether the legal conditions are fulfilled. *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 38.

[943] BGH NStZ-RR 2015, 345, 346.

[944] See Section 3, Chapter III, Part II.

[945] LG Ulm StV 2006, 8.

[946] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100e, Rn. 19.

[947] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100e, Rn. 19.

tigation.[948] A compulsory report mechanism under which police have to submit regular reports to the prosecution office might be helpful to ensure that the prosecution office keeps well informed and thus can terminate the surveillance in accordance with § 100e V StPO.

7. Notice to Persons under Surveillance

§ 101 StPO contains the procedural rules for the post-implementation period of surveillance,[949] which include rules on delivery of notice of the measures to the persons concerned (§ 101 IV - VII 1 StPO), applications to examine the legality of the surveillance (§ 101 VII 2 StPO), and the deletion and sealing of the obtained information (§ 101 VIII StPO).

The prosecution office is responsible for giving notice to the persons concerned, even if the obtained information has turned out to be meaningless for the criminal investigation and is not used at trial. This is because the fundamental rights of the persons involved have been infringed by the surveillance independently of its results.[950] The requirement to inform is to ensure that the persons affected have the possibility to challenge the legality of the measures in accordance with § 101 VII StPO.[951]

Regarding the measures of §§ 100a, 100c, 100f and 100g StPO, § 101 StPO IV and § 101a VI StPO list the persons to be informed of the surveillance: 1) the participants of the intercepted telecommunication conversations under § 100a StPO; 2) the targeted persons included in the judicial order, other intercepted persons, and the persons who owned or lived in the home placed under surveillance in accordance with § 100c StPO; 3) the targeted persons and other persons significantly affected by measures under § 100f StPO; and 4) the participants of the telecommunication conversations whose traffic data were collected under § 100g StPO.

With this long and detailed list, the legislature tried to ensure that all persons involved in the measures are informed and to reduce uncertainty in practice. Nevertheless, some exceptions are provided. § 101 IV 3 StPO prescribes that notification shall be dispensed with if overriding interest of an affected person that merit protection constitute an obstacle. Furthermore, notification of a person who was not the target of the measures of §§ 100a and 100g StPO may be dispensed with if such person was only insignificantly affected by the measure and it can be assumed that this person has no interest in being notified (§ 101 IV 4 StPO). For example, a person

[948] The prosecutors are described as "head without hands".

[949] According to § 101 I StPO, the applicable scope of this provision is not limited to the surveillance, rather to all following provisions: §§ 98a, 99, 100a to 100f, 100h, 100i, 110a, 163d to 163f StPO.

[950] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 101, Rn. 6.

[951] BGH 36, 305, 311.

who tried in vain to call the telephone number under surveillance will probably not be notified. The owner of the telephone, who is not a participant of the conversation, such as a landlord, however, is normally informed of the surveillance. In the course of a surveillance outside of a home under § 100f StPO, the words of many people can be recorded, for example, strangers accidentally passing by the recorder while talking. Such persons are treated as insignificantly affected and may not receive any notification. By contrast, persons who talked with the targeted persons and thus were recorded must be notified.

If the identities of some participants of conversations are not known, the police need to investigate the identity of such persons only if this appears necessary, taking into account the degree of intrusiveness of the measure, the effort needed for such investigation, and the detriment suffered by the persons involved (§ 101 IV 5 StPO).

What information should be included in a notice is not provided by the StPO. According to § 101 IV 2 StPO, the notice should inform the persons that they have the right to challenge the measures within two weeks after they receive the notification. The notification should further include at least the following points: 1) the type of measures; 2) the duration of the surveillance; 3) the telephone numbers, the home intercepted, or the place outside a home under surveillance; 4) the contents and the time of recorded conversations made by the notified persons. It is not clear whether persons affected by the same measure can be informed differently. For example, while the targeted persons should be informed of the suspected crime and the fact that they have been under investigation, it is doubtful whether it is proper to inform third persons, such as landlords and roommates, of who is/was the suspect of what crime. These persons have no obligation to keep such information secret, and it might cause damage to the reputation of the suspect even if the suspect is later proved innocent.[952] In addition, the notification on core private information might cause further disclosure of such information.

The notification shall take place as soon as there no longer exists a risk to the investigation, the life, physical integrity and personal liberty or significant assets of a person or the possibility to further use an undercover investigator under § 110a StPO. If the prosecutor decides not to send a notification based on these grounds, the reasons shall be documented in the file. According to § 101 VI StPO, if the notification has not been given within twelve months for the telecommunication surveillance and six months for measures under § 100c StPO after the termination of the measure,[953] any further postponement and its duration shall be decided by the court. The court may approve the permanent dispensation with notification where the requirements for notification will probably not be fulfilled in the future.

[952] Vgl. *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 101, Rn. 23.

[953] If several measures have been implemented within a short period of time, the time limit mentioned in the first sentence shall begin upon conclusion of the last measure. § 101 VI 4 StPO.

8. Legal Remedies against Surveillance

The possibility to pursue legal remedies is regarded as an integral part of "Rechtsstaatlichkeit". Therefore, § 101 VII StPO provides that the persons referred to in § 101 IV StPO may apply to the competent court for a review of the lawfulness of the measure, as well as of the manner and means of its implementation within two weeks after they have received the notification on the surveillance.[954] Receiving a notification, however, is not a precondition for applying for review, and affected persons can do so even if they have learned about the surveillance from another source.[955] According to § 101 VII 2 StPO, the persons who shall be notified may apply to the competent court for a review of the lawfulness of the measure as well as of the manner and means of its implementation. § 101 VII 4 StPO provides further that if the defendant has been charged and notified, the court shall decide upon such an application in its concluding decision. Courts, however, are only authorized by § 101 VII 2 StPO to decide upon the lawfulness of the measures, not the admissibility of the evidence gained from those measures. The admissibility of the evidence is subject to the decision of the trial court as discussed in the following Chapter.

9. Deletion and Storage of the Obtained Information

The information obtained must be deleted if it is part of the core area of privacy (§ 100d II and III StPO) and when it is no longer needed (§ 101 VIII StPO).

The deletion of core private information serves the protection of the core area of privacy. It can also be regarded as a remedy if core private information has been wrongly collected during the surveillance. The expression "to be deleted without delay" ("unverzüglich zu löschen") indicates that such information should be deleted as soon as possible when the investigator has determined that the "core area of privacy" has been infringed upon. If it is doubtful whether the information belongs to the "core area of privacy", the investigator may request a decision of the competent prosecution office.[956] The prosecution office in charge of the investigative phase finally determines whether certain information should be deleted. Moreover, the prosecution office may at any time order its investigators to terminate or suspend the surveillance if it suspects that core private information is being collected.[957] The type, the scope and a general description of the deleted information should be filed for possible judicial review under § 101 VII StPO. Since the deletion under § 100d StPO requires "immediate" action, it is not subject to the rule of § 101 VIII 3 StPO, which

[954] It is criticized that two weeks are too short and actually set up an obstacle for potential applicants. *Singelnstein*, NStZ 2009, 481, 483–484.

[955] BT-Drucks 16/5846, S. 62. Vgl. *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 101, Rn. 30.

[956] BT-Drucks 16/5846, S. 45.

[957] See Section 6, Chapter III, Part II.

provides for storage for the purpose of judicial review in the case of a postponed notification or permanent dispensation of notification. The requirement of deletion in § 101 VIII StPO refers to information which does not belong to the core area of privacy. Such information from surveillance is to be deleted without delay as soon as it is no longer needed for the criminal investigation[958] or for judicial review of the surveillance. The periods named in § 489 III StPO can give some guidance for the decision when information is no longer needed for the purpose of the investigation.[959] The information is normally regarded as no longer necessary for judicial review under § 101 VII StPO two weeks following the notification.

If the information has been used as evidence at the trial, it should be stored for a possible retrial.[960] Moreover, the information can be stored by different institutions for further criminal processes in accordance with §§ 483 and 484 StPO. Each institution should continuously review the necessity of the storage and delete the information as soon as possible when the terms of § 489 III StPO have passed.

IV. "Prohibitions of Evidence" ("Beweisverbote")

Exclusion of evidence was not expressly provided by the *Imperial Criminal Procedure Code* ("*Reichsstrafprozessordnung*" (RStPO)) (1879).[961] This is because German procedure law serves essentially to find the truth; any procedural mistakes were meant to be corrected by decisions on defendants' appeals.[962] This concept has changed dramatically in the last century. The German concept of "Beweisverbote" (the literal translation is "prohibitions of evidence") was first discussed in the early 20th century.[963] Within the last decades, "prohibitions of evidence" have become one of the most important and widely discussed topics in German criminal procedure. In 1950, § 136a III 2 StPO for the first time introduced statutory prohibitions of using evidence.[964] On the one hand, finding the truth is still one of the main purposes of the criminal procedure and is also an obligation of the courts. On the other hand, truth-finding is no longer the only goal of criminal procedure law. Its function to protect

[958] The purpose of the criminal investigation also includes the purpose for the prevention of the potential danger under § 100e VI Nr. 2 StPO. Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 101, Rn. 27.

[959] BT-Drucks 16/5846, S. 63.

[960] Vgl. *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 101, Rn. 27.

[961] However, the Reichsgericht has already dealt with complaints from defendant who asked to exclude certain evidence in individual cases. RGSt 8, 122 and 20, 186. Vgl. *Pitsch*, Strafprozessuale Beweisverbote, 2009, S. 28–29.

[962] *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl., 2017, § 24, Rn. 22.

[963] *Beling*, die Beweisverbote als Grenzen der Wahrheitserforschung im Strafprozess, 1903, S. 30, discussed this concept and argued that any piece of evidence that was obtained illegally should be excluded.

[964] BGBl. 1950, 455, 484 f.

fundamental rights is increasingly recognized. Several decades ago, the BGH declared that it is not a principle of criminal procedure law that the truth should be discovered at any cost.[965]

The concept of "prohibitions of evidence" thus also extends to evidence obtained covertly through measures under §§ 100a, 100c, 100f and 100g StPO.

1. The Scope of "Prohibitions of Evidence" and its Subgroups

"Prohibitions of evidence" theory sets up limitations on truth-finding and regulates what rights must not be infringed upon in the investigation of crime. German doctrine distinguishes between "prohibitions of collecting evidence" ("Beweiserhebungsverbote") and "prohibitions of using evidence" ("Beweisverwertungsverbote"). The former group prohibits investigators from collecting certain evidence or from doing so by certain means (e. g., § 136a StPO), whereas the latter group precludes prosecutors and courts from introducing at the trial certain evidence that had been collected (e. g., § 100d II StPO).

With regard to prohibitions of using evidence, German doctrine further differentiates between "independent prohibitions of using evidence" ("selbständige Beweisverwertungsverbote") and "dependent prohibitions of using evidence" ("unselbständige Beweisverwertungsverbote").[966] Exclusion of the former group is directly based on constitutional principles, regardless of whether the evidence was legally collected under StPO, whereas "dependent" prohibitions are always based on a violation of the law in collecting the evidence in question. One example for an "independent prohibition of using evidence" is the prohibition of using evidence that falls within the "core area of privacy", even if a legal surveillance order has been issued under § 100a StPO.

2. Theories of "Prohibitions of Using Evidence"

According to the dominant view, not every piece of evidence that has been collected illegally is subject to a prohibition of using it. Some judgements even declared that to admit such illegally obtained evidence is the norm, and to exclude it is exceptional where it is legally required or there is an overridingly important reason for exclusion.[967] In a few instances, the StPO expressly provides for a prohibition of

[965] BGHSt 14, 358, 365 ("Es ist auch sonst kein Grundsatz der Strafprozeßordnung, daß die Wahrheit um jeden Preis erforscht werden müßte.").

[966] *Rogall*, ZStW 91 (1979), 1, 3.

[967] For example, BVerfG NJW 2011, 2417, 2419 ("Daran gemessen bedeutet ein Beweisverwertungsverbot eine Ausnahme, die nur nach ausdrücklicher gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist. Die strafgerichtliche Rechtsprechung geht daher davon aus, dass insbesondere das Vorliegen eines be-

using evidence as the result of the illegal collection of evidence ("geschriebene Beweisverwertungsverbote"), such as §§ 136a III and 160a I 2 StPO. Many procedural rules, such as the requirement of a judicial order for telecommunication surveillance provided in § 100e StPO, however, do not include any statement on possible exclusion in case of a violation. It is questionable whether and under which conditions a piece of evidence should be excluded when such rules have been violated.

Besides the contributions made by German courts, scholars have also suggested and proposed various theories regarding the question of when to prohibit the use of evidence. The currently representative theories in German legal practice and academic are discussed below.

a) Rechtskreistheorie

"Rechtskreistheorie" means that the defendant can only appeal on points of law ("Revision") on grounds of a violation of rules which serve to protect his own rights, not another person's rights.[968] In 1958, the BGH introduced this theory to limit the scope of prohibitions of using evidence.[969] In this case, a witness was interrogated but was not told that he could have refused to give self-incriminating answers to certain questions in accordance with § 55 StPO. The defendant was convicted based on the witness's testimony and brought an appeal, claiming that the trial court should not have used the witness's self-incriminating statements. The BGH ruled that the witness's testimony was admissible against the defendant because the privilege against self-incrimination protected only the witness, not the defendant.[970] The BGH emphasized that the defendant has no general right to complain about any violation of procedural rules.[971] The court further stated that not every rule infringes upon the rights of the defendant to the same degree:[972] some rules are of overriding importance and guarantee the functioning of a state based on the rule of law, while other rules have significance only for individual participants of the criminal process.[973] In the latter case, only the person whose rights were infringed upon could demand exclusion

sonders schwerwiegenden Fehlers ein Verwertungsverbot nach sich ziehen kann…. Die Unzulässigkeit oder Rechtswidrigkeit einer Beweiserhebung führt auch nach Auffassung des BVerfG nicht ohne Weiteres zu einem Beweisverwertungsverbot.").

[968] *Knauer/Kudlich*, in: Knauer, MüKoStPO, Band 3, 1. Aufl., 2019, § 337 Rn. 27.

[969] BGHSt 11, 213.

[970] BGHSt 11, 213, 218 ("Anders als bei einem Verstoß gegen § 52 Abs. 2 StPO ist die Verwertung einer Zeugenaussage, die unter Verletzung der Belehrungspflicht des § 55 Abs. 2 StPO zustande gekommen ist, gegenüber dem Angeklagten nicht unzulässig. Da sein Rechtskreis durch den Verfahrensfehler nicht wesentlich berührt wird, steht ihm auch nicht das Recht zu, sich gegen die Verwertung einer solchen Aussage im Revisionsrechtszug zu wehren.").

[971] BGHSt 11, 213, 214.

[972] BGHSt 11, 213, 214.

[973] BGHSt 11, 213, 214.

of the evidence.[974] Hence, the defendant in the instant case was precluded from basing his appeal on the fact that a witness had not been properly informed of his right to withhold testimony. This judgement has remained controversial.[975] Some authors criticized that the notion of "Rechtskreis" is not a concept of the StPO and that the BGH failed to offer a clear definition for it although the BGH accorded it such an important function.[976] One author went so far as to declare that this theory misses the goals of criminal procedure.[977]

The BGH further developed this view in later case law.[978] Violations of certain provisions, such as §§ 52 and 136a I 2 StPO, have been held to protect rights of the defendant; he can therefore claim the exclusion of evidence obtained through such violations.[979]

b) "Protective Purpose" Doctrine ("Schutzzwecklehre")

The "protective purpose" doctrine was first developed by Grünwald.[980] According to this doctrine, the purpose protected by the violated provision plays a central role in determining the admissibility of evidence. If the admission of illegally obtained evidence would frustrate the purpose of the violated rule or if admission would further infringe upon the protected interest, such evidence should be excluded.[981] According to Grünwald, this doctrine mainly aims at preventing the further frustration of the purpose of the rule, which had already been violated by the collection of the evidence. By the same token, evidence need not be excluded if its admission would not further frustrate the purpose of the violated rule.[982]

The BGH referred to this doctrine in several decisions. For example, the BGH excluded a confession made by the defendant during police interrogation when he had not been advised of his right to remain silent (§§ 163a IV and § 136 I StPO).[983] The BGH stated that the role of the violated rule in the protection of the defendant's rights should be taken into consideration when deciding on the exclusion of evidence. If the violated rule does not primarily serve the protection of the defendant, the

[974] BGHSt 11, 213, 215.

[975] See *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 365.

[976] *Eb. Schmidt*, JZ 1958, 596; *Rudolphi*, MDR 1970, 93.

[977] *Rudolphi*, MDR 1970, 96; *Jäger*, Beweisverwertung und Beweisverwertungsverbote im Strafprozess, 2003, S. 16; *Jäger*, JA 2017, 74; *Paul*, NStZ 2013, 489.

[978] For example, BGHSt 38, 302, 304.

[979] *Tants*, Beweisverwertungsverbote im Rahmen einer „Gesamtschau in der Rechtsprechung", 2020, S.139.

[980] *Grünwald*, JZ 1966, 489. An introduction to various contributions to this doctrine can be found in *Pitsch*, Strafprozessuale Beweisverbote, 2009, S. 288 ff.

[981] *Grünwald*, JZ 1966, 489, 497.

[982] *Grünwald*, JZ 1966, 489, 492.

[983] BGHSt 38, 214.

evidence will not be excluded; but if the violated rule is fundamental to ensuring the procedural rights of the defendant, the evidence must be excluded.[984] The BGH regarded the right to be informed of the right to silence as an integral part of a fair trial and therefore excluded the confession.[985]

A contrary result was reached in a case in which the defendant's blood sample was forcibly collected by a medical assistant after the suspect had caused a car accident. The defendant demanded the exclusion of the blood sample because only a physician may take such samples in accordance with § 81a StPO.[986] The BGH held that the fact that the blood sample was collected by a medical assistant rather than a doctor should not lead to its inadmissibility. First, the evidentiary quality of the sample was not influenced by the person who took it. Second, the integrity of the body had already been violated, and the admission of the sample at trial would neither further violate nor restore the integrity of the defendant's body. This case also shows a difference between the "Rechtskreistheorie" and the protective purpose theory, which the BGH applied. The "Rechtskreistheorie" would have suggested the exclusion of the evidence because the defendant's personal right to his bodily integrity had been violated. Exclusion of the sample, however, could not have contributed to furthering the purpose of the "physician" rule, that is, to make sure that blood samples are taken in accordance with good medical standards.

Like the "Rechtskreis" theory, the "protective purpose" doctrine has been criticized for its lack of clarity. It is difficult to identify the exact purpose of a provision, and there are always different opinions on that question.[987] In addition, according to Grünwald, evidence is admissible if the violation of the rule is "completed" and the purpose of the rule has irretrievably been frustrated. That may mean that especially grave rule violations that cannot be remedied may remain without a sanction.

[984] BGHSt 38, 214, 220 ("Dient die Verfahrensvorschrift, die verletzt worden ist, nicht oder nicht in erster Linie dem Schutz des Beschuldigten, so liegt ein Verwertungsverbot fern; ein Beispiel ist der Verstoß gegen § 55 Abs. 2 StPO (BGHSt 1, 39; 11, 213). Andererseits liegt ein Verwertungsverbot nahe, wenn die verletzte Verfahrensvorschrift dazu bestimmt ist, die Grundlagen der verfahrensrechtlichen Stellung des Beschuldigten oder Angeklagten im Strafverfahren zu sichern.").

[985] BGHSt 38, 214, 220 ("Die Anerkennung dieses Schweigerechtes entspricht der Achtung vor der Menschenwürde. Sie schützt das Persönlichkeitsrecht des Beschuldigten und ist notwendiger Bestandteil eines fairen Verfahrens.").

[986] BGHSt 24, 125.

[987] *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 366; *Jugl*, Fair trial, 2016, S. 63; *Kelnhofer*, Hypothetische Ermittlungsverläufe im System der Beweisverbote, 1994, S. 73.

c) Balancing Theory

Another approach developed by German courts, which has also gained much support from scholars[988], is the balancing theory ("Abwägungslehre"), according to which the interests and values involved are to be balanced against each other.[989] Balancing theories are proposed for resolving conflicts among different values when they cannot be logically ranked due to a lack of corresponding rules or overriding principles.[990] In distinction from "Rechtskreis" theory and "protective purpose" theory, balancing theory does not give special consideration to the personal right or purpose protected by the violated rule but takes all relevant elements into consideration.[991]

On the one side, the violated interests of the defendant and the significance of the violated procedural rule, such as the fair trial and *nemo tenetur* principles,[992] are to be considered. Courts should also take into account the degree of the infringement of personal rights,[993] the purpose of the violated rules, and the good or bad faith of the investigators.[994] Bad faith of police officers almost always leads to the exclusion of the illegally obtained evidence.[995]

On the other side, the general interests of truth-finding and law enforcement are to be considered, in particular the interest of an effective investigation,[996] the seriousness of the crime,[997] and the importance of the evidence.

---

[988] For example, BVerfGE 38, 105, 118. *Jugl*, Fair trial, 2016, S. 63 and Fn. 281; *Jahn*, Gutachten 67. DJT 2008, CI, C66 ff.; *Kelnhofer*, Hypothetische Ermittlungsverläufe im System der Beweisverbote, 1994, S. 66 ff. and Fn. 105.

[989] "Abwägungstheorie" has not been especially developed for evidence law but describes a general legal method; *Hubmann*, Wertung und Abwägung im Recht, 1997, S. 147.

[990] Vgl. *Rogall*, in: Eber, u. a. (Hrsg.), Festschrift für Ernst-Walter Hanack, 1999, S. 297.

[991] *Jugl*, Fair trial, 2016, S. 63.

[992] Vgl. Section 3. a) bb) of this Chapter.

[993] See Section 2. a) of this Chapter.

[994] BGHSt 24, 125, 130 f. ("Hinzu kommt, daß die Polizeibeamten in gutem Glauben gehandelt, nämlich irrig die tatsächlichen Voraussetzungen angenommen haben, unter denen der Beschuldigte zur Duldung der Blutentnahme gezwungen werden durfte, ihr Vorgehen also rechtmäßig im Sinne des § 113 StGB war").

[995] BVerfG, NJW 2009, 3225, 3226; BGHSt 51, 285, 295. More case law can be found at *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 94 Rn. 21; *Wohlers*, StV 2008, 434, 439; BVerfG, Beschluss der 1. Kammer des Zweiten Senats vom 09. November 2010 – 2 BvR 2101/09 -, Rn. 45,

[996] BVerfGE 44, 353, 373 ff. ("Bei der gebotenen Abwägung steht auf der einen Seite das Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege, zu deren Aufgaben auch die Verfolgung und Ahndung von Straftaten nach dem Betäubungsmittelgesetz gehört und deren Organe dabei im Rahmen der Besonderheiten des jeweiligen Falles auf die Inanspruchnahme der ihnen durch die Strafprozeßordnung zur Verfügung gestellten Zwangsmittel angewiesen sind."); 80, 367, 375.

[997] BGHSt 19, 325, 332 ("Handelt es sich um hinreichenden Tatverdacht schwerer Angriffe auf das Leben, auf andere bedeutsame Rechtsgüter, auf den Staat oder um andere schwerere

This theory has been criticized for violating the principles of certainty and predictability.[998] Without a clear rule, it is difficult to predict outcomes.[999]

Moreover, it has been argued that the balancing theory does not provide for balancing at all but is cited only to explain the results desired by the courts.[1000] Using the pretense of balancing, arbitrary decisions can be made, which cannot be tolerated under the rule of law.[1001]

Exclusion of evidence under the balancing theory is further limited by the notion of "hypothetische Ermittlungsverläufe" (hypothetical course of the investigation).[1002] According to this approach, if a piece of evidence could have been obtained legally, it can be admitted although it was actually obtained illegally. To ensure the proper functioning of procedural guarantees, such as the "Richtervorbehalt", the courts insist that the hypothetical course of the investigation must be examined on the specific facts of each case.[1003] As a consequence, however, similar cases have been decided differently by the BGH.

For example, in the case mentioned above concerning an illegally obtained blood sample,[1004] the BGH supported admission of the blood sample by mentioning the fact that the sample could have been obtained legally at any time.[1005]

Another case concerned a recording obtained after the judicial surveillance order had expired.[1006] In this case, the court approved the surveillance of conversations in a

---

Angriffe auf die Rechtsordnung, so wird der Schutz des privaten Lebensbereichs gegebenenfalls zurücktreten müssen."); 34, 397, 401 ("…daß die Verwertung heimlich hergestellter Tonbandaufnahmen in Fällen schwerer Kriminalität gerechtfertigt sein kann. Entsprechendes gilt auch für Tagebuchaufzeichnungen.").

[998] *Correa Robles*, Die Fernwirkung, 2018, S. 76 ff.; *Eisenberg*, Beweisrecht der StPO, 2016, Rn. 367.

[999] *Schröder*, Beweisverwertungsverbote, 1992, S. 46 ff.

[1000] *Schröder*, Beweisverwertungsverbote, 1992, S. 47.

[1001] *Lesch*, in: Hassemer, u. a. (Hrsg.), In Dubio Pro Libertate, 2009, S. 312; *Correa Robles*, Die Fernwirkung, 2018, S. 77; *Schröder*, Beweisverwertungsverbote, 1992, S. 46; *Weigend*, StV 2003, 436, 440 („subjektive Prioritätensetzung").

[1002] *Schröder*, Beweisverwertungsverbote, 1992, S. 72 ff.; *Beulke*, ZStW 103 (1991), 657, 660 ff.; *Fezer*, NStZ 2003, 625, 629; *Jahn/Dallmeyer*, NStZ 2005, 297, 301.

[1003] *Schröder*, Beweisverwertungsverbote, 1992, S. 113. In this book, the author has suggested the courts have to consider in individual cases: first whether the investigative measures are necessary; and secondly whether the measures could have been legally implemented when they adopt the "hypothetical investigation process" approach. S. 114.

[1004] BGHSt 24, 125.

[1005] BGHSt 24, 125, 130 ("… der Beweiswert der gesetzwidrig erlangten Probe nicht beeinträchtigt. Bedeutsam ist ferner, daß diese auch auf gesetzmäßigem Wege jederzeit hätte gewonnen werden können."). This rule also applies to evidence collected in other EU countries and obtained by German police through judicial cooperation. Even when the rules of judicial cooperation were violated, the evidence can be admitted as long as it could have been obtained legally. BGHSt 58, 32.

[1006] BGH NJW 1999, 959.

car from 8 June 1995 to 8 Sept. 1995 (three months) and again from 5 Oct. 1995 for another three months. The admissibility of information obtained between 8 Sept. and 4 Oct. 1995 was challenged. The BGH upheld its admission although there existed no legal basis for surveillance between 8 Sept. and 4 Oct. 1995. The BGH declared that the StPO does not recognize a principle that any information obtained in violation of a procedural rule must be excluded.[1007] Whether to exclude a piece of information must be decided in each individual case, taking into account the importance of the information to the investigation or general interest and the seriousness of the violation.[1008] Given the background of this case, the material requirements for a surveillance were actually fulfilled between 8 Sept. and 4 Oct. 1995, which the BGH concluded from the fact that the surveillance before and after this period had been approved by the court. Moreover, the lacuna resulted from a negligent mistake of the prosecutor rather than an arbitrary violation of the rules.[1009]

By contrast, in an earlier case,[1010] an undercover agent had called the suspect and recorded their conversation without judicial authorization. The BGH found a violation of § 100a StPO and consequently excluded the recording, although a judge would have issued a surveillance order if requested.[1011]

Some scholars have generally criticized the notion of a hypothetical course of the investigation and have called for its restriction.[1012] They argue that the doctrine hardly has a real function beyond giving the courts a reason to admit illegally obtained evidence that should have been excluded. Others wrote that the doctrine reverses the causal chain between the actual violation of procedural rules and the evidence in question. An assumption of legality *post factum*, in their opinion, cannot repair the actual violation of basic rights.[1013]

d) Summary

The BVerfG has frequently dealt with issues of admissibility of evidence. Like the BGH, the BVerfG considers the exclusion of evidence to be an exception because it

[1007] BGH NJW 1999, 959, 961.

[1008] BGH NJW 1999, 959, 961.

[1009] BGH NJW 1999, 959, 961. This ruling was criticized that it violated the necessity of a judicial order and undermined the principle of judicial control. *Wohlers*, in: Weßlau/Wohlers (Hrsg.), Festschrift für Gerhard Fezer, 2008, S. 327.

[1010] BGHSt 31, 304.

[1011] BGHSt 31, 304.

[1012] See, for example, *Löffelmann*, Die normativen Grenzen der Wahrheitserforschung im Strafverfahren, 2008, S. 58 and Fn. 76; *Wohlers*, in: Weßlau/Wohlers (Hrsg.), Festschrift für Gerhard Fezer, 2008, S. 325 ff.; *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 409.

[1013] *Beulke*, ZStW 103 (1991), 657, 663; *Wohlers*, in: Weßlau/Wohlers (Hrsg.), Festschrift für Gerhard Fezer, 2008, S. 324 ff.

interferes with the truth-seeking function of the criminal process.[1014] The BVerfG has stated that justice ("Gerechtigkeit"), as an integral part of the rule of law ("Rechtsstaatlichkeit"), can only be realized by an effective law enforcement, hence an effective criminal justice system is an element of the rule of law.[1015] In addition, the BVerfG mentioned two further arguments that support the admission of evidence in the public interest: needs of an effective criminal investigation and law enforcement, and the public interest in finding the truth in the criminal process.[1016] The BVerfG therefore tries to prevent frequent exclusion of evidence and supports the statement made by the BGH that an exclusion of evidence should not render the criminal process ineffective.[1017]

The BGH has also held that evidence is not inadmissible whenever it was obtained without a judicial order. The BGH emphasized that the courts have an obligation to investigate the facts and to consider all relevant evidence. Exclusion of evidence is regarded as an exception and is only justified when exclusion is demanded by an express legal rule or is based on important grounds.[1018] In other cases, the question of

[1014] BGHSt 51, 285, 290. Vgl. *Karaaslanoglu*, Beweisverbote im deutschen und im türkischen Strafverfahrensrecht, 2015, S. 39.

[1015] BVerfGE 33, 367, 383; 38, 105, 115; 44, 353, 374 ("Das Interesse an einer leistungsfähigen Strafjustiz gehört in den Gewährleistungsbereich des Rechtsstaatsprinzips (Art. 20 Abs. 3 GG). Soweit der Grundsatz der Rechtsstaatlichkeit die Idee der Gerechtigkeit als wesentlichen Bestandteil enthält, verlangt er auch die Aufrechterhaltung einer funktionstüchtigen Rechtspflege, ohne die Gerechtigkeit nicht verwirklicht werden kann."). A general discussion on the concept of "funktionstüchtigen Strafrechtspflege" can be found *Landau*, NStZ 2007, 121.

[1016] BVerfGE 33, 367, 383; 38, 105, 116; 38, 312, 321; 39, 156, 163; 41, 246, 250; 44, 353, 374 ("Wiederholt hat das Bundesverfassungsgericht deshalb die Bedürfnisse einer wirksamen Strafverfolgung anerkannt, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafprozeß betont und die Aufklärung schwerer Straftaten als wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet".); 77, 65, 76; 80, 367, 375.

[1017] Vgl. *Karaaslanoglu*, Beweisverbote im deutschen und im türkischen Strafverfahrensrecht, 2015, S. 39; *Pitsch*, Strafprozessuale Beweisverbote, 2009, S. 287. BGHSt 32, 68, 71 ("…darf ein Verfahrensfehler, der ein Verwertungsverbot für ein Beweismittel herbeiführt, nicht ohne weiteres dazu führen, daß das gesamte Strafverfahren lahmgelegt wird."). It should make clear here that this argument is limited to the case of small procedural mistakes. When the violation of procedural rule is obvious, this argument cannot be used to support the admission of the evidence obtained through such violation. See *Eder*, Beweisverbote und Beweislast im Strafprozess, 2015, Fn. 142.

[1018] BGHSt 51, 285, 290 ff. ("Dabei muss beachtet werden, dass die Annahme eines Verwertungsverbots, auch wenn die Strafprozessordnung nicht auf Wahrheitserforschung ‚um jeden Preis' gerichtet ist, eines der wesentlichen Prinzipien des Strafverfahrensrechts einschränkt, nämlich den Grundsatz, dass das Gericht die Wahrheit zu erforschen und dazu die Beweisaufnahme von Amts wegen auf alle Tatsachen und Beweismittel zu erstrecken hat, die von Bedeutung sind. Daran gemessen bedeutet ein Beweisverwertungsverbot eine Ausnahme, die nur nach ausdrücklicher gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist. Maßgeblich mit beeinflusst wird das Ergebnis der demnach vorzunehmenden Abwägung vom Gewicht des infrage stehenden Verfahrensverstoßes. Dieses wird seinerseits wesentlich von der Bedeutung der im Einzelfall betroffenen Rechtsgüter bestimmt.") (citation omitted). Vgl. Fn. 1017 and the companying text.

exclusion is subject to a balancing of interests in each individual case.[1019] When the police or the prosecutors operate in good faith ("in gutem Glauben") but are mistaken about the facts,[1020] or when the legal interest has not been violated arbitrarily, often the interest of truth-finding will prevail and the evidence will be used.

3. Grounds for Excluding Evidence

It appears from the foregoing discussion that in certain cases evidence must be excluded under all circumstances, whereas in other cases exclusion or admission depends on the result of balancing the interests involved. In the latter case, sometimes only the tainted piece of evidence is excluded whereas investigators can take clues for further investigative steps (Verwertungsverbot), in other cases the illegally obtained evidence may not be used for any investigatory or evidentiary purpose (Verwendungsverbot). This issue will be further discussed below in Section 4 of this chapter.

a) Grounds Directly Based on Constitutional Law

The BVerfG and the BGH have dealt with many cases concerning the exclusion of evidence on a constitutional law basis ("Verfassungsrechtliche Verwertungsverbote"). With regard to the evidence from technological surveillance, the "core area of privacy" developed from Arts. 1 and 2 I GG is highly relevant.

aa) Evidence Falling within the "Core Area of Privacy"

In the "Tonband-Beschluss", the BVerfG emphasized that even a predominant public interest cannot justify an infringement on the "core area of privacy".[1021] The BVerfG has thus established an absolute protection of the core area, which has a great impact on the exclusion of evidence. Since the "core area of privacy" is deemed untouchable,[1022] information belonging to this area should not be admitted as evi-

[1019] Vgl. *Wohlers*, StV 2008, 434, 439.

[1020] BGHSt 24, 125, 130 ("Hinzu kommt, daß die Polizeibeamten in gutem Glauben gehandelt, nämlich irrig die tatsächlichen Voraussetzungen angenommen haben, unter denen der Beschuldigte zur Duldung der Blutentnahme gezwungen werden durfte, ihr Vorgehen also rechtmäßig im Sinne des § 113 StGB war"). Vgl. Fn. 1005.

[1021] BVerfGE 34, 238, 245 ("Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in den absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen; eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt."). Vgl. Fn. 866 and the companying texts. The definition of the "core area of privacy" can be found in Section 1. b) aa) and 2. g), Chapter I, Part II.

[1022] BVerfGE 34, 238, 245 ("…daß das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung gewährt…").

dence in the trial nor be used to justify other investigative activities.[1023] Any use of such information is prohibited, and information should be deleted without delay.

Evidentiary rules regarding the "core area of privacy" have been adopted in § 100d II StPO.[1024] It provides that information from the "core area of privacy must neither be collected during the investigation nor be used at trial but should be deleted. The legislature has thus guaranteed an absolute protection of the core sphere of privacy, in line with the jurisprudence of the BVerfG.[1025] Although the term "verwerten", instead of "verwenden", is used in § 100d II StPO, the courts and most authors agree that core private information cannot be used as a clue for further investigation.[1026]

bb) The Nemo Tenetur Principle and § 136a StPO

Another constitutional ground for excluding evidence is the *Nemo tenetur* principle ("Selbstbelastungsfreiheit").[1027] This principle means that no one must be forced to incriminate himself. [1028] It is expressly provided neither in the GG nor in the StPO; the BVerfG nevertheless decided that compelling someone to incriminate himself violates not only the general personality right but also human dignity (Art. 1 GG),[1029] as well as the principle of "Rechtsstaatlichkeit" (Art. 20 GG).[1030] German courts do not rule out the use of undercover agents or covert surveillance measures by police. The BGH, however, decided in an exceptional case that the *Nemo tenetur* principle was violated when the ability of the suspect to make a free decision was strongly limited by the pressure resulting from his detention and from a long period of contacts initiated by an undercover agent.[1031] The BGH permits covert investigative measures but regards as unlawful activities by police agents that actively push

[1023] Vgl. Section 3. a) aa) of this Chapter.

[1024] § 100d I StPO on "Beweiserhebungsverbote" is discussed in Section 2. g), Chapter I, Part II.

[1025] Vgl. BVerfGE 129, 208; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 24.

[1026] BVerfGE 129, 208, 229 ("Das gesetzliche Verwertungsverbot in § 100a Abs. 4 Satz 2 StPO schließe auch eine Nutzung der Informationen als Ermittlungsansatz aus."); *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100d Rn. 7; *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100d Rn. 6; *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100d, Rn. 23.

[1027] BGHSt 31, 304, 308.

[1028] *Mahlstedt*, Die Verdeckte Befragung des Beschuldigten im Auftrag der Polizei, 2011, S. 62. See also BGHSt 14, 358, 364 f.; 31, 304, 308.

[1029] BVerfGE 56, 37, 43. More discussion on legal foundations of Nemo-tenetur-principle can be found: *Mahlstedt*, Die Verdeckte Befragung des Beschuldigten im Auftrag der Polizei, 2011, S. 63 ff.

[1030] *Möller*, JR 2005, 314; and *Sowada*, in: Geisler (Hrsg.), Festschrift für Klaus Geppert zum 70. Geburtstag, 2011, S. 689, 698.

[1031] BGHSt 52, 11 and 22 ff. Another similar case is BGHSt NStZ 2009, 343.

suspects toward incriminating themselves in an interrogation-like scenario, using psychological pressure.[1032]

In line with the constitutional protection of the personality right, § 136a StPO prohibits, *inter alia*, deceit ("Täuschung") as a method of interrogation and provides for the exclusion of incriminating statements obtained through deceit. Deceit here refers to untrue statements about legal questions and facts, for example, if the interrogator wrongly declares that the suspect must tell the truth, or that the conversation has no legal effect, or that an accomplice has already confessed.[1033] The BGH tends to interpret deceit under § 136a StPO restrictively, so as to avoid blocking investigative activities.[1034]

According to the BGH, § 136a StPO does not prohibit covert investigative measures because a simple act of surveillance is not deceit in the sense of § 136a StPO.[1035] Accordingly, the BGH declared that it is an inherent characteristic of telecommunication surveillance that it can provide evidence against the person who is intercepted without advance notice of the surveillance. The use of a fake identification by an undercover agent also cannot amount to deceit in the meaning of § 136a StPO.

Some covert measures, however, can be categorized as "interrogation-like" situations to which § 136a StPO can be applied.[1036] In a controversial case decided by the BGH in 1996, a private person following the order of a police officer talked with a suspect over the telephone without telling the suspect the real purpose – criminal investigation – of the conversation and let the police listen to the conversation.[1037] The BGH held that the conversation was admissible based on the following reasoning: (1) simply withholding a fact from the suspect is not deceit because it is not sufficient to violate the freedom of will ("Willensfreiheit"); (2) the private person at hand did not elicit special trust from the suspect[1038] but was just an active citizen who happened to

[1032] BGHSt 52, 11 ("Mit dem Grundsatz der Selbstbelastungsfreiheit ist es jedenfalls nicht vereinbar, dem Beschuldigten, der sein Schweigerecht in Anspruch genommen hat, in gezielten, vernehmungsähnlichen Befragungen, die auf Initiative der Ermittlungsbehörden ohne Aufdeckung der Verfolgungsabsicht durchgeführt werden, wie etwa durch Verdeckte Ermittler, selbstbelastende Angaben zur Sache zu entlocken."); see also *Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, 2012, S. 163.

[1033] *Gleß*, in: Löwe/Rosenberg, StPO, Band. 4/1, 27. Aufl., 2019, § 136a, Rn. 40.

[1034] *Gleß*, in: Löwe/Rosenberg, StPO, Band. 4/1, 27. Aufl., 2019, § 136a, Rn. 39.

[1035] BGHSt 33, 217 ("Zum Wesen der Vorschrift des § 100 a StPO gehört, daß sie zur Selbstbelastung des Beschuldigten führen kann, ohne daß dieser hiervon weiß…In dem bloßen Verschweigen der Überwachung gegenüber dem Beschuldigten kann also eine Täuschung i. S. des § 136 a StPO noch nicht liegen."). It is one of the characteristics of such measures that the concerned person has a feeling of not being observed when he is intercepted. BGH 53, 294, Rn. 46 ("…auch ist es gerade das Charakteristikum von heimlichen Überwachungsmaßnahmen, dass der Überwachte sich unbeobachtet fühlt.").

[1036] *Gleß*, in: Löwe/Rosenberg, StPO, Band. 4/1, 27. Aufl., 2019, § 136a, Rn. 15.

[1037] BGHSt 42, 139.

[1038] Vgl. Section 1. b) hh), Chapter II, Part II.

witness a crime and wanted to help the police; (3) the conversation was not an "interrogation" so that § 136a StPO did not apply; and (4) the *nemo tenetur* principle was not violated because the suspect was not influenced by the authority of the police and did not feel that he was obliged to talk about the crime. He was therefore held to have provided the information voluntarily.[1039] In this case, the BGH emphasized that the definition of deceit under § 136a StPO should be interpreted restrictively and does not cover the situation of causing a misunderstanding by withholding a fact; in addition, the BGH argued that the situation was not comparable to the other means prohibited by § 136a StPO, such as using physical force.[1040]

In another case, the conversation between a married couple was recorded when the wife visited her husband in a jail's visiting room. The BGH confirmed the legality of the surveillance order but held that the guards took advantage of the detention situation and intentionally misled the suspect to believe that he was neither intercepted nor observed, rather than only making use of a misunderstanding of the suspect.[1041] The guards did so in order to get evidence. The BGH stated that this situation did not fall under the definition of deceit but nevertheless violated the *nemo tenetur* and the fair trial principles and that the recording should therefore be excluded.[1042]

b) Violating Procedural Rules as Grounds for Excluding Evidence

The procedural rules for measures under §§ 100a - 100c StPO are mainly provided in § 100e StPO.[1043] No rule on exclusion can be found in this section. Given the established case law that not every violation of procedural rules will lead to an exclusion of the evidence,[1044] the question arises whether and under what conditions evidence collected in violation of § 100e StPO can be admitted. The BGH has

[1039] BGHSt 42, 139, 140 ff.

[1040] BGHSt 42, 139, 140 and 149.

[1041] BGH 53, 294, Rn. 47 ("Sie haben vielmehr bewusst eine von den üblichen Abläufen in der Untersuchungshaft derart abweichende Besuchssituation geschaffen, dass nicht lediglich ein Irrtum des Angeklagten ausgenutzt wurde. Vielmehr wurde, anders kann man das Vorgehen nicht verstehen, die Situation – gezielt – zur Erlangung einer gerichtsverwertbaren Selbstbelastung des Angeklagten herbeigeführt. Im Rahmen ihres Vorgehens haben die Ermittlungsbehörden mit mehreren aufeinander abgestimmten Maßnahmen dem Angeklagten den Eindruck vermittelt, er erhalte nun eine Sonderbehandlung und dürfe sich völlig ungestört und ohne jegliche Überwachung mit seiner Ehefrau – noch dazu in marokkanischer Sprache – unterhalten.").

[1042] BGH 53, 294, Rn. 51 ("Zwar hat diese – wie auch die Verteidigung zu Recht in der Hauptverhandlung hervorgehoben hat – noch nicht die Qualität einer Täuschung oder eines unzulässigen Zwangs im Sinne von § 136a StPO. Jedenfalls in der Gesamtschau stellt sich hier aber das Vorgehen der Strafverfolgungsbehörden mit Blick auf die besondere Situation des Untersuchungshaftvollzuges als Verletzung des Rechts auf ein faires Verfahren dar. Die Beweisgewinnung greift danach in erheblicher Weise in die Verfahrensrechte des Angeklagten ein und war somit unzulässig. Sie hat ein Beweisverwertungsverbot zur Folge.").

[1043] See Chapter III, Part II.

[1044] See Section 2. a) of this Chapter.

distinguished between substantive and formal preconditions of a surveillance order.[1045] The requirements of the crime catalogue, the purpose of the investigation, the degree of suspicion and the subsidiarity clauses are considered substantive, while the written form, the court's jurisdiction and the duration of the measure belong to the formal requirements.[1046]

If important substantive requirements have not been met, the information obtained under such an order is to be excluded.[1047] In addition, the "Richtervorbehalt" can also play an important role in the balancing process.[1048] By contrast, mistakes like using the wrong writing form are tolerated and in principle have no legal effect.

aa) Richtervorbehalt

(1) Without Judicial Order because of "Gefahr im Verzug"

As mentioned above, the prosecutor can issue an order "bei Gefahr im Verzug" in accordance with § 100e II StPO.[1049] It is a contested question, however, whether evidence obtained in the first three days under such an emergency order is admissible if the order has lost effect, either because no decision was made by the competent court after three days or because the court declined to confirm the order. Some authors maintain that the order's loss of validity after three days does not have a retroactive effect, so that the evidence remains admissible unless it needs to be excluded on other grounds.[1050] However, if the court later determines that the emergency order was issued arbitrarily ("willkürlich"), the evidence is inadmissible.[1051] In one case, police officers had known that the suspect G lived in a house for 4 weeks before they arrested him. The police applied to the prosecutor for permission to search the house only about two hours after the arrest. The prosecutor issued an emergency order without calling a judge or explaining why the evidence could be lost.[1052] The BGH held that an emergency could not be established in this case because the order was issued 2 hours after the arrest and the evidence could

[1045] Vgl. BGHSt 31, 304, 309 ("…einer wesentlichen sachlichen Voraussetzung für die Anordnung der Maßnahme nach § 100 a StPO…"). See also BGHSt 41, 30, 32. The checking list discussed below can be compared with the list in Section 2, Chapter III.

[1046] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a Rn. 231 ff. (Wird die Zustimmung der StA entgegen § 110b I 3 StPO nur mündlich erteilt, so liegt darin lediglich der Verstoß gegen eine Formvorschrift, der ein Verwertungsverbot nicht begründet.) BGH NStZ 1996, 48.

[1047] BGHSt 31, 304, 308; 32, 68, 70; 41, 30, 31.

[1048] See Section 3. b) aa), Chapter IV, Part II.

[1049] See Section 1. b), Chapter III, Part II.

[1050] See *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100e, Rn. 26; and *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100e, Rn. 4.

[1051] Vgl. Fn. 917 and the companying texts.

[1052] BGHSt 51, 285, 286.

already have been destroyed by G's friend.[1053] The BGH held that the function of judicial control had intentionally been ignored and that "Gefahr im Verzug" was invoked arbitrarily. Therefore, the police had committed an "especially serious" fault, which led to the exclusion of the evidence.[1054]

(2) Without Judicial Order in Other Situations

In the case where an undercover agent abused the trust relationship with the suspect and recorded their conversation without a judicial order, the BGH held that the undercover agent had intentionally avoided judicial control, which violated the rule of law.[1055]

bb) Offense not Listed

The measures named in §§ 100a - 100c StPO can be adopted only if an offense listed in the catalogue is to be investigated. As stated above, this is a substantive requirement. Evidence collected through these measures consequently cannot be used for prosecuting non-catalogue crimes (§ 100e VI No. 1 StPO).[1056]

The BGH held that legally intercepted telecommunication conversations can be used against a third person who is not named in the order if the conversation is evidence that this person committed a crime listed in the crime catalogue of § 100a StPO. Using the conversations for investigating or prosecuting non-catalogue crimes, by contrast, is regarded as a violation of Art. 10 GG.[1057]

cc) Insufficient Facts to Support Suspicion

According to the BGH, the degree of suspicion at the time when the measure was issued cannot be reviewed *ex post facto*, but the appeals court can review for recognizable arbitrariness.[1058] The degree of suspicion and the possible violation of a

[1053] BGHSt 51, 285, 288 ff.

[1054] BGHSt 51, 285, 292 ff. This case is concerning home search. Therefore it is discussable whether this standard can be applied to the cases concerning the measures under §§ 100a – c StPO. *Müller/Trurnit*, StraFo 2008, 144, 147.

[1055] BGHSt 31, 304, 308.

[1056] Vgl. Section 2. d), Chapter I, Part II.

[1057] BGHSt 26, 298, 302, 303; 28, 122, 125, 129. See also BGHSt 32, 10, 14, 15 ("Die Ergebnisse einer Telefonüberwachung dürfen zum Beweis einer Straftat, die nicht Anlaß für die Überwachungsanordnung war, jedenfalls dann verwendet werden, wenn diese Straftat ihrerseits im Katalog des § 100a Satz 1 StPO aufgeführt ist"). The "distance effect" of the catalogue-crime evidence to the non-catalogue-crime can be found in Section 4 of this Chapter.

[1058] BGHSt 28, 122, 124 ("… daß die Maßnahme grundsätzlich nicht auf den zur Zeit ihrer Anordnung vorliegenden Grad des Verdachts einer Katalogtat geprüft werden könne, der Revisionsrichter aber erkennbare Willkür zu beachten habe."); 41, 30, 31.

subsidiarity requirement can be evaluated differently depending upon the experience of prosecutors and judges. The appeals court must respect the discretion of the issuing judge. Therefore, a judicial order may be regarded as illegal only if its issuance was arbitrary or clearly exceeded the margin of discretion.[1059] In that case, information obtained through such an order cannot be admitted as evidence.[1060]

This case law has, however, been criticized on the ground that it leaves the discretion of prosecutors and judges in practice free from judicial review. Given the intrusiveness of surveillance, such a situation is not deemed acceptable.[1061]

dd) Duration

As discussed in Section 2. c) of this Chapter, the BGH in one case declined to exclude evidence obtained after the judicial order had expired.[1062] If exceeding the time limits of a judicial order is an arbitrary violation, however, this fault can lead to the exclusion of the evidence.[1063]

c) Evidence from Private Investigation

There are two types of private investigations: (1) a private person investigates under the instruction of the police or prosecutor; (2) a private person acts on his own initiative.[1064] The first type is normally treated as state action, thus the rules for undercover agents apply.[1065] The admissibility of the evidence obtained through the second type will be discussed here.

Traditionally, the state has the main responsibility for investigating a criminal case and collecting evidence. With the advance of digitalization, however, private persons can obtain important information for an investigation, both in legal (e. g., video surveillance in a company) and illegal ways (e. g., hacking).[1066]

In accordance with § 201 I and II StGB a person commits a criminal offense if he records or intercepts a non-public conversation without proper authority, makes use of a recording, or grants a third person access to such recording, or discloses the contents of the conversation. If public officers commit the crime, they are subject to

[1059] BGHSt 41, 30, 34. Vgl. *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 220.

[1060] BGHSt 41, 30, 34. Vgl. Fn. 1047 and the companying texts. Two later decisions have followed this reasoning: BGH 47, 362; BGH NJW 2003, 1880.

[1061] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 221.

[1062] BGH 44, 243. To be a formal requirement is not the only reason for the admissibility of the evidence. For more details, please see Section 3, Chapter IV, Part II.

[1063] Vgl. Fn. 1009 and the companying texts.

[1064] More information and discussion can be found in *Stoffer*, Wie viel Privatisierung, 2016.

[1065] See Section 3. a) bb) of this Chapter.

[1066] *Kaspar*, GA 2013, 206, 206.

an aggravated penalty.[1067] If a private person records a conversation with a justification, such recordings will normally be admitted by the courts.[1068]

With regard to illegal recordings made by private persons, German courts apply the balancing theory.[1069] They do not demand automatic exclusion but apply strict standards for admission.[1070] Evidence illegally collected by private persons will be excluded if the person seriously violated human rights.[1071]

In an early case concerning a private recording, witness R, on her own initiative, called the defendant to collect evidence and induced him to incriminate himself, while secretly recording the conversation.[1072] The BGH denied the existence of a self-defense situation, thus her conduct was not justified.[1073] Since R had infringed upon the personality right of the defendant, the recordings were held inadmissible. The BGH added that the defendant's rights would be violated once again by the admission, i. e., playing the recordings at the trial.[1074] This can be regarded as an application of the "protective purpose" theory discussed above.[1075] If the defendant consents to the use of a privately recorded tape at the trial, his consent repairs the illegality of the evidence-taking, and it can be used.[1076] The BGH followed the ruling of the ECtHR[1077] that illegally obtained evidence must not be the only evidence to support a conviction.[1078]

When deciding on the admissibility of evidence from private persons, the BVerfG differentiates among three "spheres".[1079] Information disseminated in the public sphere, such as a public announcement in a train station, can be recorded by anyone without the consent of the speaker.[1080] Such information can be admitted in the courts

[1067] But a public interest may justify the recording; BayObLG NJW 1994, 1671; OLG Frankfurt NJW 1967, 1047, 1048.

[1068] OLG Frankfurt NJW 1967, 1047. Vgl. *Bienert*, Private Ermittlungen und ihre Bedeutung auf dem Gebiet der Beweisverwertungsverbote, 1997, S. 26.

[1069] OLG Frankfurt NJW 1967, 1047, 1408.

[1070] *Stoffer*, Wie viel Privatisierung, 2016, S. 429; *Bockemühl*, Private Ermittlungen im Strafprozeß, 1996, 122.

[1071] *Kölbel*, NStZ 2008, 241.

[1072] BGHSt 14, 358.

[1073] BGHSt 14, 358, 362 ff.

[1074] BGHSt 14, 358, 363 ("Verletzte die Zeugin R. das allgemeine Persönlichkeitsrecht des Angeklagten sonach durch alle drei Tonbandaufnahmen, so darf sie sie auch nicht durch Abhören verwerten; denn dadurch würde sie das Recht des Angeklagten erneut verletzen.").

[1075] *Jäger*, Beweisverwertung und Beweisverbote im Strafprozess, 2003, S. 124 ff.

[1076] BGHSt 36, 167. In this case, the defendant did not challenge the admissibility of the evidence, which the BGH treated as consent.

[1077] ECtHR, *Schenk v. Switzerland* App no 10862/84, Judgment of 12 July 1988.

[1078] BGHSt 36, 167, 173.

[1079] BVerfGE 34, 238. Vgl. Fn. 599 and accompanying text. See also *Stoffer*, Wie viel Privatisierung, 2016, S. 429 ff.

[1080] BVerfGE 34, 238, 247.

without any restriction. The third category is the "core area of privacy". Information belonging to this area should be excluded,[1081] as was declared in the "Tonband-Beschluss" discussed above.[1082] In between is the sphere described as "general personal private sphere". Information from this sphere is admissible if there exists a public interest that outweighs the privacy interest affected. [1083] It is subject to the balancing theory discussed above.[1084] On the one side, the personal right infringed upon, on the other side, the public interest in truth finding, the seriousness of the crime and the interest in effective criminal justice will be balanced. For instance, if the crimes under investigation infringe upon the right to life or other similarly important legal interests, the protection of the private area has to give way.[1085] Balancing must take place on the basis of the concrete facts of each case, not simply on the abstract seriousness of the offense in question.[1086] In the case of "Liechtensteinische Steueraffäre", a former worker K of a bank stole bank documents which proved tax offenses of German clients. K sold the documents to German intelligence agents.[1087] The majority view among commentators supports the admission of the documents since these data did not belong to the "core area of privacy" and the common interest outweighed the secrecy interest of the bank and its clients.[1088] The BVerfG mainly agreed and held that privately obtained evidence can be used even though the private person committed a criminal offense by passing it on to German state agents.[1089]

[1081] See Section 3. a) aa) of this Chapter.

[1082] BVerfGE 34, 238, 246. See Section 1. b), Chapter I, Part II.

[1083] BVerfGE 34, 238, 248; *Bockemühl*, Private Ermittlungen im Strafprozeß, 1996, S. 71 ff.

[1084] BVerfGE 34, 238, 250 ("Hier – wie sonst – kommt es allerdings entscheidend darauf an, ob ein derartiger Eingriff bei einer Abwägung, die alle Umstände des Einzelfalles in Betracht zieht, dem Verhält- nismäßigkeitsgrundsatz entspricht. Das heißt: Einerseits ist zu berücksichtigen, wie tief die beabsichtigte Verwertung einer konkreten Tonbandaufnahme – gemessen an deren Inhalt und Form – in das Recht auf freie Entfaltung der Persönlichkeit des Betroffenen eingreifen würde. Andererseits ist bei der Abwägung der so ermittelten Schwere des Eingriffs in das Recht auf freie Entfaltung der Persönlichkeit gegen berechtigte Erfordernisse der Strafrechtspflege nicht lediglich auf den in einem Straftatbestand abstrakt umschriebenen Deliktsvorwurf abzuheben, sondern auf das im Einzelfall in Betracht kommende konkrete Tatunrecht."). Vgl. Section 2 of this Chapter.

[1085] BGHSt 19, 325, 333.

[1086] BVerfGE 34, 238, 250.

[1087] BVerfG, Beschluss der 1. Kammer des Zweiten Senats vom 09. November 2010 – 2 BvR 2101/09 -.

[1088] *Kölbel*, NStZ 2008, 241; *Trüg/Habetha*, NStZ 2008, 481; *Göres/Kleinert*, NJW 2008, 1353.

[1089] BVerfG, Beschluss der 1. Kammer des Zweiten Senats vom 09. November 2010 – 2 BvR 2101/09 -, Rn. 58 ("Insoweit ist zu berücksichtigen, dass sich die Vorschriften der Strafprozessordnung zur Beweiserhebung und -verwertung nach Systematik, Wortlaut und Zweck ausschließlich an die staatlichen Strafverfolgungsorgane richten. Beweismittel, die von Privaten erlangt wurden, sind – selbst wenn dies in strafbewehrter Weise erfolgte – grundsätzlich verwertbar. Dies bedeutet, dass allein von dem Informanten begangene Straftaten bei der Beurteilung eines möglichen Verwertungsverbotes von vornherein nicht berücksichtigt werden müssen.").

4. Exclusion of Derivative Evidence? ("Fernwirkung")

The discussion of a distant effect ("Fernwirkung") of a procedural fault, or the admissibility of evidence indirectly derived from measures violating procedural rules, involves two problems: 1) whether illegally obtained evidence may be employed as a basis for further investigation ("Spurenansatz" or "Ermittlungsansatz") and 2) whether evidence obtained through such investigatory measures ("derivative evidence") is admissible at trial or whether the original violation has a distant effect precluding use of the derivative evidence.[1090] The opinions on this issue in case law and legal literature are divided.[1091] Opponents of a general "distant effect" of procedural faults argue that such a rule would significantly obstruct truth-finding and that one procedural fault should not be allowed to block the whole criminal process.[1092] In order to fight crime effectively, a general "distant effect" should not be recognized. Supporters of a general "distant effect" claim that it would be too easy to bypass exclusionary rules without such an effect.[1093] Several authors have suggested that the existence of a "distant effect" should be decided in each case by balancing the interests involved.[1094]

German courts recognize a "distant effect" only in exceptional cases where human dignity or fundamental rights have been violated,[1095] for instance, if the primary evidence was obtained through violating § 136a StPO or the *nemo tenetur* principle.[1096] Another example for an unlimited "distant effect" is an intrusion into the "core area of privacy". If primary evidence has been obtained by infringing upon the "core area of privacy", as in the case of § 100d II StPO, evidence derived from that primary evidence is inadmissible.[1097] Although the law does not expressly prohibit

---

[1090] Vgl. *Ossenberg*, Die Fernwirkung, 2011, S. 8.

[1091] A detailed introduction of different opinons can be found: *Robles*, 180 ff. See also *Pitsch*, Strafprozessuale Beweisverbote, 2009, S. 311. Vgl. BGHSt 51, 1, 8 ("Die Literatur bejaht hingegen überwiegend eine Fernwirkung des Verwertungsverbots bei Erkenntnissen aus einer rechtswidrigen Telekommunikations-Überwachungsmaßnahme."). *Ossenberg*, Die Fernwirkung, 2011, S. 50 ff.; *Weigend*, StV 2003 436; *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 403 ff.

[1092] BGH 36, 364; *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 242.

[1093] For a discussion of arguments for and against a distant effect see *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 404–408.

[1094] *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 408; *Gleß*, in: Löwe/Rosenberg, StPO, Band. 4/1, 27. Aufl., 2019, § 136a, Rn. 75; *Weigend*, StV 2003 436; *Ossenberg*, Die Fernwirkung, 2011, S. 50 ff.; *Ambos*, Beweisverwertungsverbote, 2010, S. 147 ff.

[1095] *Rogall*, ZStW 1991, 40; *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 408; *Ambos*, Beweisverwertungsverbote, 2010, S. 147 and Fn. 904.

[1096] *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 408. More discussion about the "Fernwirkung" of § 136a StPO can be found: *Weigend*, StV 2003 436.

[1097] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 234; 100d, Rn. 23.

such information from being used as a clue for further investigation,[1098] courts have held that it must not be used for that purpose.[1099] In support, one may argue that § 100d II 2 StPO requires the immediate deletion of such information, which is to prevent the further disclosure of the core private information and its use for an investigation.

For the information falling within the first sphere of the "three-spheres" theory,[1100] the problem of a "distant effect" does not play a role. Since the primary evidence is generally accessible, derivative evidence can be admitted as evidence.[1101]

If the general personality right has been violated and the direct evidence is subject to exclusion after balancing, there is no agreed-upon solution as to the "distant effect" of the original violation.

In one early case, the BGH excluded a confession made by the defendant under the influence of illegally obtained evidence from telecommunication surveillance.[1102] In a later case, the BGH came to a different conclusion. In that case, illegal telecommunication surveillance provided the information that one co-defendant had a meeting with two witnesses. The meeting was observed by the police. After this meeting, the three were arrested and made statements, which led to the arrest of other defendants.[1103] The BGH declined to exclude the trial testimony of the witnesses and argued that their statements were not influenced by the information obtained from illegal telecommunication surveillance.[1104] A "distant effect" of excluding the testimony of these witnesses would paralyze the criminal process as a whole, the BGH argued.

In a more recent case, the BGH discussed another typical situation of a possible "distant effect".[1105] Telecommunication surveillance was ordered against B, who was suspected of conducting an illegal drug business. The facts to support this order came

[1098] Vgl. Section 3. a) aa) of this Chapter and Fn. 1026.

[1099] BVerfGE 129, 208, 229 ("Das gesetzliche Verwertungsverbot in § 100a Abs. 4 Satz 2 StPO schließe auch eine Nutzung der Informationen als Ermittlungsansatz aus."); LG Ulm, Beschluss vom 19. 04. 2004 – 1 Qs 1036/04, StV 2006, 8 f. ("Weiter muß gewährleistet sein, daß Informationen aus dem unantastbaren Bereich privater Lebensgestaltung der durch diese Maßnahme betroffenen Personen weder im Hauptsacheverfahren verwertet noch zum Anknüpfungspunkt weiterer Ermittlungen werden."); *Schmitt*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl., 2020, § 100a, Rn. 25; *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 67.

[1100] Section 3. c), Chapter IV, Part II.

[1101] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 209.

[1102] BGHSt 27, 355; this ruling was confirmed in BGSt 32, 68, 70 ("Richtig ist es schließlich auch, daß ein Beweisverwertungsverbot für solche Bekundungen von Beschuldigten besteht, die unter dem Eindruck des Vorhalts von unzulässig gewonnenen Erkenntnissen aus einer Telefonüberwachung gemacht worden sind.").

[1103] BGHSt 32, 68, 70. *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 65.

[1104] *Lohberger*, in: Ebert, u. a. (Hrsg.), Festschrift für Ernst-Walter Hanack zum 70. Geburtstag, 1999, S. 261; *Ambos*, Beweisverwertungsverbote, S. 149 ff.

[1105] BGHSt 51, 1.

from an earlier order of telecommunication surveillance against C, and the suspicion against C was based upon another surveillance order against F. B's conviction was based upon chance finds from the order against C. The defense lawyer complained that the court did not review the legality of all three orders. Although the BGH did not decide upon whether information from a surveillance order should be excluded if such an order was issued upon evidence from an illegal order issued earlier, the BGH in principle denied a distant effect of an illegal surveillance.[1106] If the distant effect were recognized, this would lead to a domino effect that would paralyze the whole criminal process.[1107] The BGH therefore limited the review of the legality of the surveillance order to the latest one directly leading to the evidence, namely, the order against B. The ruling in an earlier case that the "distant effect" is to be decided upon the individual facts and the type of the excluded evidence,[1108] can only be considered in exceptional cases.[1109] In sum, according to the BGH illegally obtained evidence can normally be employed for triggering further investigations or for applying for the authorization of further investigative measures,[1110] such as judicial orders for searches[1111] or telecommunication surveillance. Even where a confession based on the confrontation with an illegally made tape recording was ruled inadmissible, the BGH declared that the tape recording could be used as clue for investigating other catalogue crimes.[1112] Information about non-catalogue crimes obtained from surveillance under § 100a StPO is not admissible as evidence but can be used to justify the opening of an investigation of that non-catalogue crime.[1113]

[1106] BGHSt 51, 1, Rn. 14 ("Ob Erkenntnisse aus einer Telekommunikations-Überwachungsmaßnahme, die auf der Grundlage von Erkenntnissen aus einer wegen Fehlens wesentlicher sachlicher Voraussetzungen vorangegangenen anderen rechtswidrigen Überwachungsmaßnahme angeordnet worden ist, ebenfalls unverwertbar sind, hat der BGH – soweit ersichtlich – noch nicht entschieden. Eine Fernwirkung von Beweisverwertungsverboten hat er jedoch grundsätzlich abgelehnt".). ("An dem allgemeinen Grundsatz, dass Beweisverwertungsverboten keine Fernwirkung zukommt, ist festzuhalten.").

[1107] BGHSt 51, 1, 8; vgl. Fn. 1017. The similar expression can be found: BGHSt 27, 355, 358; 32, 68, 71; 34, 362, 364; 35, 32, 34.

[1108] BGHSt 27, 355, 357 ("Die allgemein einem Verwertungsverbot gesteckten Grenzen liegen nicht fest. Sie richten sich jeweils nach der Sachlage und der Art des Verbots."). The same for BGHSt 29, 244, 249.

[1109] BGHSt 51, 1, 7 ("Allenfalls *ausnahmsweise* kann nach der Sachlage und der Art des Verwertungsverbots dessen Fernwirkung anzunehmen sein.").

[1110] *Gless*, in: Thaman (eds.), Exclusionary Rules in Comparative Law, S. 129.

[1111] *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 65 ff. According to *Lohberger*, in: Ebert, u. a. (Hrsg.), Festschrift für Ernst-Walter Hanack, 1999, S. 264 ff. and *Ambos*, Beweisverwertungsverbote, 2010, S. 149 and Fn. 917 a search judicial order cannot exclusively be supported by inadmissible evidence.

[1112] BGHSt 27, 355.

[1113] *Bruns*, in: Hannich, KK-StPO, 8. Aufl., 2019, § 100a, Rn. 65; *Allgayer/Klein*, wistra 2010, 132; OLG München wistra 2006, 472.

V. Empirical Reports

The German Ministry of Justice releases annual statistics on the surveillance of telecommunications under § 100a StPO and of homes under § 100c StPO on its website in accordance with § 101b StPO.[1114] The reports from the years 2000 to 2018 can be found on this website. The reports include the numbers of original and extension judicial orders issued under § 100a and § 100c StPO in each state, the numbers of judicial orders issued for each crime of the crime catalogue, and the types of telecommunications intercepted. In the reports on the acoustic surveillance of homes, surveillance judicial orders issued in accordance with Art. 13 IV GG to prevent danger and with Art. 13 V GG to protect individual security are included. In this chapter, however, only judicial orders issued for the purpose of criminal investigations are discussed.[1115]

1. Numbers of Judicial Orders under § 100a and § 100c StPO

The number of judicial orders of telecommunication surveillance under § 100a StPO is not identical with the number of procedures in which such measures are taken.[1116] In one procedure, more than one order can be issued. An order can be issued to intercept only one or more than one telephone numbers or facilities.

Table 7
Number of Procedures with Measures under § 100a and § 100c StPO

	Number of Procedures with Measures under § 100a StPo	**Numbers of Original Judicial Orders Issued under § 100a StPo**	**Number of Original Judicial Orders per Procedure**	**Number of Procedures with Measures under § 100c StPo**
2008	5,348	13,949	2.6	7
2009	5,301	17,208	3.2	8
2010	5,493	17,351	3.2	4
2011	5,516	18,029	3.3	10
2012	5,678	19,616	3.5	8

[1114] https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html, visited at 19. 05. 2020.

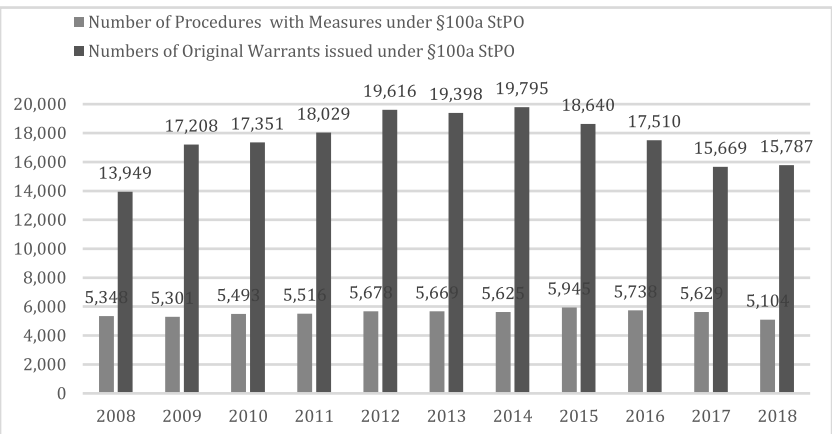
[1115] In reports, this part of data is labeled as "repressive Maßnahmen gemäß Art. 13 Abs. 3 GG".

[1116] According to the report of telecommunication surveillance 2012, the calculation method of Hessen on the number of judicial orders was not identical with that of other states. It is not clear whether Hessen adopted different methods for all years through or only in 2012. Compared with the numbers in other states, it can be assumed that this different method resulted in more orders reported in Hessen.

Table 7 (Continued)

	Number of Procedures with Measures under § 100a StPo	Numbers of Original Judicial Orders Issued under § 100a StPo	Number of Original Judicial Orders per Procedure	Number of Procedures with Measures under § 100c StPo
2013	5,669	19,398	3.4	7
2014	5,625	19,795	3.5	6
2015	5,945	18,640	3.1	6
2016	5,738	17,510	3.1	6
2017	5,629	15,669	2.8	12
2018	5,104	15,787	3.1	12
Total	61,046	192,952	3.2	86

Table 7 shows that more than three judicial orders per procedure were issued from 2008 till 2018. The number of procedures with acoustic surveillance of a home is rather small compared to that of telecommunication surveillance. One reason is the higher procedural barrier in § 100c StPO than in § 100a StPO. Another reason might be the high costs of home surveillance.[1117] There is no data about how many judicial orders were issued per procedure under § 100c StPO. From the limited number of such orders, it can be assumed that in most situations only one judicial order per procedure was issued.



Graph 9: Number of Procedures with Measures and Number of Judicial Orders Issued under § 100a StPO

[1117] See Section 5. c), Chapter V, Part II.

Graph 9 shows that the number of procedures with telecommunication surveillance has remained quite stable in the past eleven years. The Standard Deviation (SD) of the number of procedures from 2008 till 2018 is only 4% of its mean value.

2. Reasons for Non-Implementation of Judicial Orders under § 100c StPO

The number of judicial orders actually installed was reported only for measures authorized under § 100c StPO, not under § 100a StPO. According to the reports on judicial orders issued under § 100c StPO, 9 out of 92 orders were not implemented for various reasons between 2008 and 2018.

Table 8
Reasons for Non-Implementation of Judical Orders under § 100c StPo

	Number of Non-Executions	**Reasons for Non-Executions**
2008	1	not reported
2012	1	The object in judicial order is not used any more.
2013	2	not reported
2014	3	not reported
2015	1	The suspect was arrested.
2017	1	The risk of being discovered is too high.

3. Types of Intercepted Telecommunications

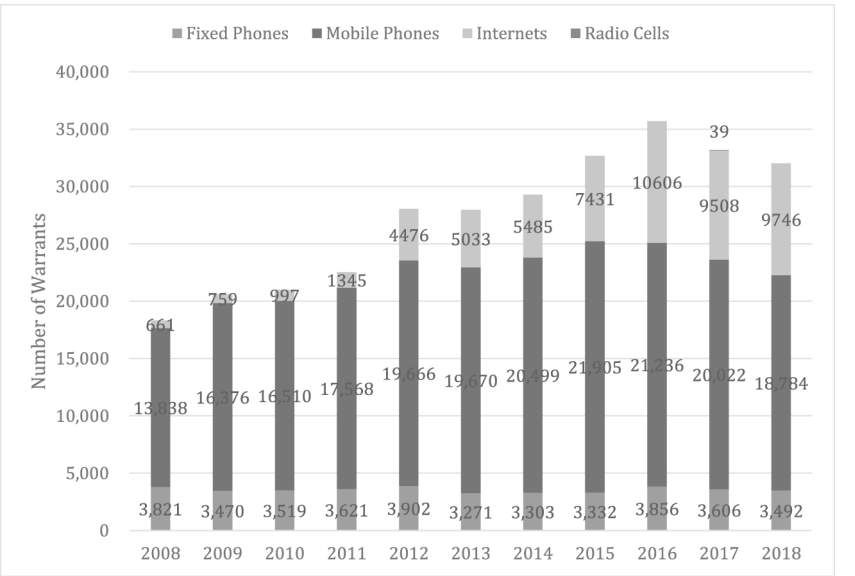
The reports on telecommunication surveillance divide the intercepted telecommunications into four categories: telecommunications with fixed phones, mobile phones, internet and telecommunications intercepted through radio cells. The last category occurs very rarely. As mentioned above, each judicial order can intercept more than one type of telecommunications, therefore, one order can be calculated more than once. In addition, orders for extensions are also included in the following numbers of orders for each type of telecommunications.

Table 9
Number of Judicial Orders for Each Type of Telecommunications

	Fixed Phones	**Mobile Phones**	**Internet**	**Radio Cells**
2008	3,821	13,838	661	0
2009	3,470	16,376	759	0
2010	3,519	16,510	997	0
2011	3,621	17,568	1,345	0
2012	3,902	19,666	4,476	0

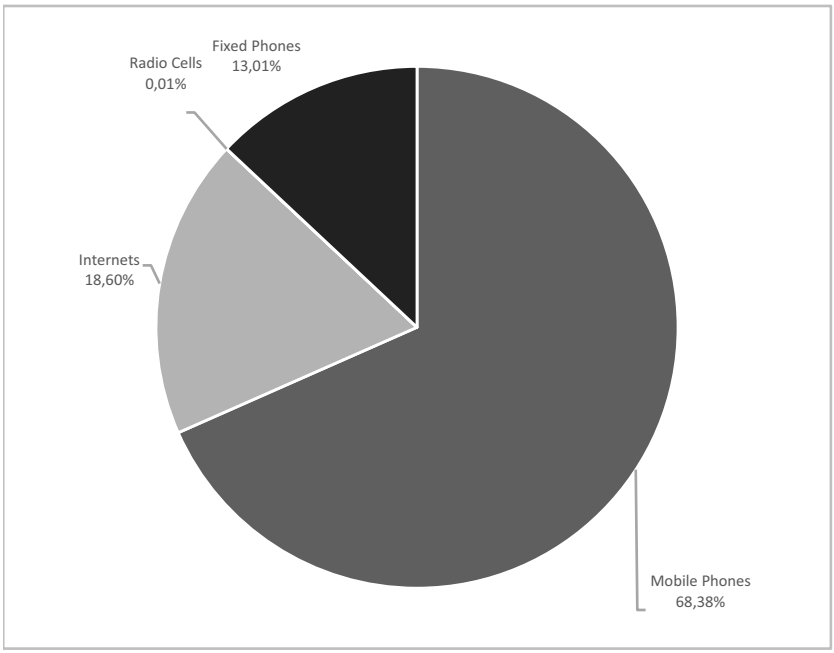
Table 9 (Continued)

	Fixed Phones	Mobile Phones	Internet	Radio Cells
2013	3,271	19,670	5,033	0
2014	3,303	20,499	5,485	0
2015	3,332	21,905	7,431	0
2016	3,856	21,236	10,606	0
2017	3,606	20,022	9,508	39
2018	3,492	18,784	9,746	0
Total	39,193	206,074	56,047	39



Graph 10: Number of Judicial Orders for Each Type of Telecommunication from 2008 to 2018

According to Table 9, Graph 10 and Graph 11, it is evident that telecommunications with mobile phones are intercepted with the highest frequency. The practice of interception of fixed phones has remained stable in the past eleven years, while the number of orders on telecommunication surveillance via internet has increased dramatically. SD of the latter is 72 % of its mean value. The number of judicial orders on telecommunication via internet in 2016 is 16 times that of 2008. The number of orders on mobile phones does not increase as fast as that on internet but shows a general increasing tendency between 2008 and 2016. The increase of judicial orders on telecommunication surveillance with mobile phones and internet is the result of more persons using mobile phones and internet.



Graph 11: Percentages of Judicial Orders on Each Type of Intercepted Telecommunication in Total Numbers from 2008 to 2018

4. Catalogue Crimes Cited ("Anlassstraftaten")

a) Number of Procedures of Telecommunication Surveillance

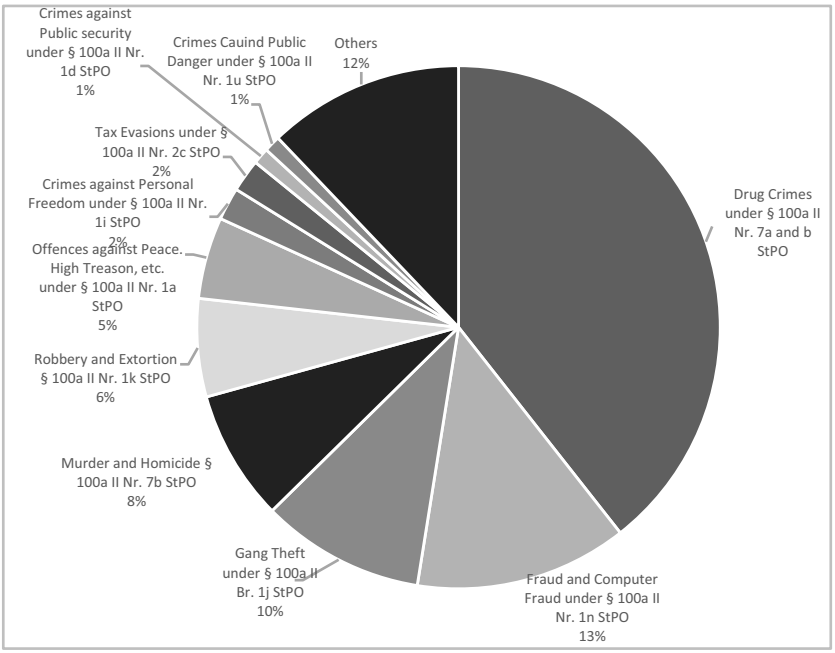
Table 10
Crimes in Catalogue under § 100a II StPO in 2018

	Crimes in Catalogue of § 100a II StPO	**Number of Procedures in 2018**	**Percentage of Each Crime**
1	Drug Crimes (§ 100a II Nos. 7a and b StPO)	8792	39 %
2	Fraud and Computer Fraud (§ 100a II No. 1n StPO)	2874	13 %
3	Gang Theft (§ 100a II No. 1j StPO)	2341	10 %
4	Murder and Homicide (§ 100a II No. 1h StPO)	1895	8 %

Table 10 (Continued)

	Crimes in Catalogue of § 100a II StPO	**Number of Procedures in 2018**	**Percentage of Each Crime**
5	Robbery and Extortion (§ 100a II No. 1k StPO)	1278	6 %
6	Offences against Peace, High Treason, etc. (§ 100a II No. 1a StPO)	1098	5 %
7	Crimes against Personal Freedom (§ 100a II No. 1i StPO)	495	2 %
8	Tax Evasion (§ 100a II No. 2c StPO)	436	2 %
9	Crimes against Public security (§ 100a II Nr. 1d StPO)	396	2 %
10	Crimes Causing Public Danger (§ 100a II Nr. 1u StPO)	279	1 %
11	Others	2630	12 %
Total		22514[1118]	100 %

[1118] If one procedure involves more than one crime, it can be caculated more than once. See the Report on the telecommunication surveillance 2018, https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html, visited at 07.01.2021.



Graph 12: Percentages of Procedures with Catalogue Crimes in Orders in 2018

Graph 12 shows that drug crimes were most frequently cited as triggering offenses for a procedure in 2018. One procedure can be calculated more than once if it cited more than one crime as its triggering crime. The situations are the same in other years. The percentage of total numbers of procedures citing drug crimes as triggering crimes between 2015 and 2018 are 40 % (2018: 39 %; 2017: 38 %; 2016: 42 %; 2015: 42 %). By studying the statistics from 2015 to 2018, the catalogue crimes cited most frequently were gang theft, fraud and computer fraud, as well as murder and homicide. The rankings differ. The first nine crimes, as present in Table 10, remain the same between 2015 and 2018, with different rankings. This implies that the crime structure investigated by telecommunication surveillance has remained stable in past years.

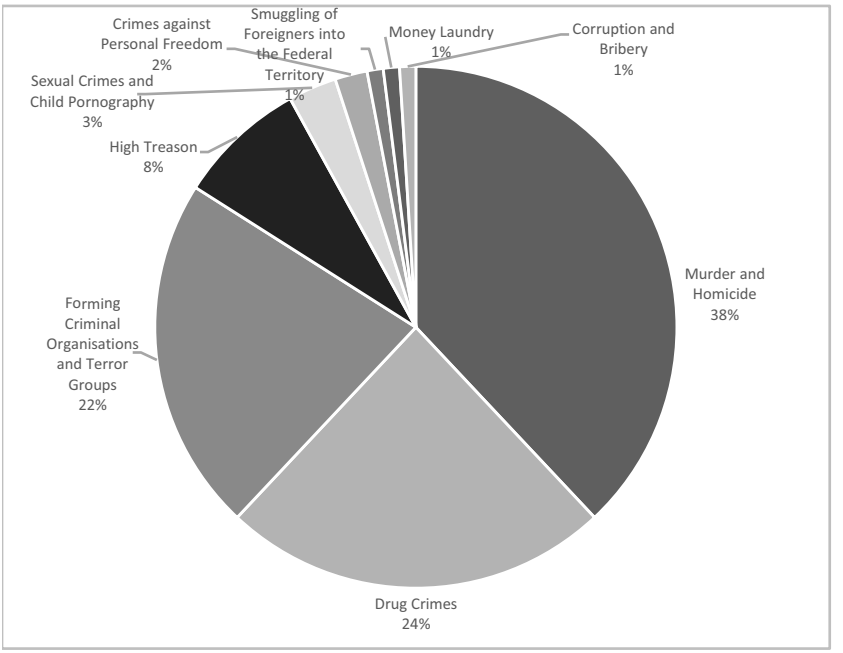
b) Number of Procedures of Home Surveillance

Table 11
Number of Procedures of Catalogue Crimes for Home Surveillance between 2008 and 2018[1119]

Crimes in Catalogue of § 100c StPO 2008 – 2018	Number of Procedures
Murder and Homicide	36
Drug Crimes	22
Forming Criminal Organisations or Terroristic Groups	21
High Treason	7
Sexual Crimes and Child Pornography	3
Crimes against Personal Freedom	2
Smuggling of Foreigners into the Federal Territory	1
Money Laundering	1
Corruption and Bribery	1

Table 11 and Graph 13 show that home surveillance orders were issued most often in homicide investigations (38 % of all surveillance orders issued between 2008 and 2018), followed by drug crimes and crimes of forming criminal organizations or terroristic groups.

[1119] If one procedure has more than one initial crime for judicial orders of home surveillance, it may be calculated also more than once. For instance, one procedure with a judicial order (or judicial orders) of home surveillance in 2018 whose initial crimes were sexual crime, child pornography, and drug crimes. This procedure is calculated twice in this table.



Graph 13: Percentage of Procedures of Catalogue-Crimes for Home Surveillance between 2008 and 2018

5. Duration and Extension

a) Extension of Judicial Orders under § 100a StPO

Table 12
Number of Extensions of Orders of Telecommunication Surveillance

	Number if Original Judicial Orders Issued under § 100a StPO	Number of Extensions	Rate of Extension
2008	13,949	2,514	18.0 %
2009	17,208	3,150	18.3 %
2010	17,351	3,047	17.6 %
2011	18,029	3,089	17.1 %
2012	19,616	3,445	17.6 %
2013	19,398	3,519	18.1 %
2014	19,795	3,950	20.0 %
2015	18,640	3,587	19.2 %

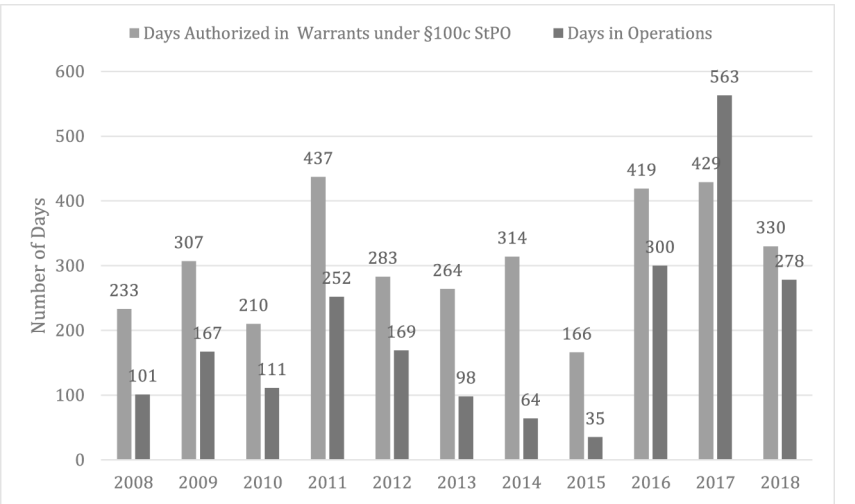
Table 12 (Continued)

	Number if Original Judicial Orders Issued under § 100a StPO	Number of Extensions	Rate of Extension
2016	17,510	3,845	22.0 %
2017	15,669	2,982	19.0 %
2018	15,787	3,687	23.4 %
Total	192,952	36,815	19.1 %

§ 101b II StPO requires that the annual number of extension orders issued under § 100a StPO is reported to the Federal Ministry of Justice. Neither the duration of an order nor the actual days in operation, however, is required to be included in the reports. Table 12 shows that approximately 19 % of the original orders issued under § 100a StPO were extended between 2008 and 2018.

b) Duration and Extension of Home Surveillance under § 100c StPO

The duration of home surveillance is required to be reported under § 101b IV StPO.



Graph 14: Number of Days Authorized in Judicial Orders under § 100c StPO and Days in Operation[1120]

Graph 14 shows that the days authorized in orders of home surveillance were only partially used. 63 % of days authorized in judicial orders were used between 2008 and 2018. During this period, orders in 29 (out of 86, 34 %) procedures were issued with

[1120] The number of days includes the days authorized in extensions.

no more than 20 days. These "short judicial orders" were normally fully executed. "Long judicial orders" authorized with more than 20 days were more likely to be only partly implemented. Judicial orders in 29 (out of 86, 34 %) procedures were extended according to Table 13.

Obviously, the statistics in 2017 were abnormal since the days in operation were more than those authorized. The original report 2017 shows that in Saarland a judicial order with one day and an extension of ten days were issued but that this order was implemented for 341 days. This case in Saarland continued to 2018 when an extension of three days was used for 107 days. This is also the longest home surveillance with 448 days in operation between 2008 and 2018. Saarland may have mistakenly reported the number of judicial orders instead of the days authorized.

Table 13
Number of Procedures with Extensions

	Number of Procedures	**Number of Procedures with Extensions**
2008	7	3
2009	8	2
2010	4	2
2011	10	3
2012	8	3
2013	7	2
2014	6	2
2015	6	1
2016	6	3
2017	12	4
2018	12	4
Total	86	29

c) Cost

The cost of telecommunication surveillance is not included in reports. § 101b IV StPO, however, requires statistics on costs of home surveillance to be reported.

According to reports on home surveillance under § 100c StPO, the costs of such a measure consist of costs for translation and other costs, such as labor costs or device costs. Costs of some cases were not shown in the reports while costs in other cases were only estimated.

Table 14
Costs of Home Surveillance under § 100c StPO

	Number of Procedures with Cost Reported	Cost (Euros)	Cost per Procedure (Euros)
2008	6	265,211	44,201.83
2009	3	34,900	11,633.33
2010	3	3,200	1,066.67
2011	6	108,437	18,072.83
2012	8	266,502.48	33,312.81
2013	2	16,180	8,090.00
2014	4	6,550	1,637.50
2015	2	134,292	67,146.00
2016	3	3,300	1,100.00
2017	1	40,000	40,000.00
2018	3	81,068.08	27,022.69
Total	41	959,640.56	23,405.87

Table 14 shows that between 2008 and 2018 one measure under § 100c StPO costs around 23,405 Euros on average. It was not rare that translation fees were the main costs. The most expensive case occurred in 2012 in Niedersachsen, which cost 102,737.93 Euros for 23 days in operation. 102,073.39 Euros of the total costs were paid for translators, including their accommodation. Another unusual case was a case investigated by the Federal General Prosecutor's Office in 2013 where the surveillance was not implemented but still carried costs of 16,000 Euros.

6. Efficiency

The statistics on telecommunication surveillance under § 100a StPO do not contain much information that reflects the efficiency of the measure. By contrast, reports on home surveillance under § 100c StPO include information on whether the results of the measures were relevant for the procedures, including procedures in other cases. In addition, if the results were not relevant, the reasons must be reported. The reports also show the number of intercepted suspects and that of third persons, which reflects the degree to which these measures had an impact on the privacy of third persons.

Table 15
Number of Intercepted Suspects and Relevant Procedures under § 100c StPO

	Number of Suspects Intercepted under § 100c StPO	**Number of Persons Intercepted under § 100c StPo (Suspects + Third Persons)**	**Rate of Suspects among All Intercepted Persons**	**Number of Revelant Procedures under § 100c StPO**	**Number of Procedures with Measures under § 100c StPO**	**Rate of Relevant Procedure among All Procedures under § 100c StPO**
2008	29	90	32.2 %	4	7	57.1 %
2009	29	33	87.9 %	5	8	62.5 %
2010	15	20	75.0 %	3	4	75.0 %
2011	21	45	46.7 %	6	10	60.0 %
2012	26	104	25.0 %	5	8	62.5 %
2013	32	57	56.1 %	4	7	57.1 %
2014	36	49	73.5 %	5	6	83.3 %
2015	29	44	66.0 %	3	6	50.0 %
2016	11	26	42.3 %	3	6	50.0 %
2017	36	41	87.8 %	5	12	41.7 %
2018	61	136	44.9 %	9	12	75.0 %
Total	325	645	50.4 %	52	86	60.5 %

The relevant procedures in Table 15 include procedures whose results were either relevant for the procedures for which the measures had been ordered or for other procedures, or both. The total rate in Table 15 shows that around 50 % of persons under home acoustic surveillance are suspects, while 60.5 % of procedures taking place led to relevant information. The most frequent reason for irrelevance cited in the reports was a lack of results. Other reasons were that the intercepted house was not used, the suspect stayed in the house only for a very short period of time, almost no conversations were conducted in the intercepted area, the quality of recording was too bad to understand, the suspect was arrested, less covert investigative measures were taken, the meeting of suspects did not take place, and the results were not admissible.

VI. Conclusions

Surveillance of telecommunication and homes as investigative measures infringe upon the right of privacy, but at the same time they are regarded as necessary and thus constitutional if certain conditions are fulfilled. The BVerfG has developed the notion

that a "core area of privacy" must be respected under all circumstances. This "core area of privacy" is not limited to a physical space but sets a limit to all investigative measures including covert surveillance.

Under the scheme of the constitution and the legislation, an independent judge should decide whether the requirements for each measure are met before the surveillance takes place. Judicial control *ex ante* is meant to limit the powers of the police and the prosecution.

The practical effect of judicial control on investigative activities is doubtful, however. Without investigating on their own, courts need to rely heavily on the information offered by the police. The courts play a role, to a large degree, like a notary. The most obvious example is the evaluation of subsidiarity clauses. Police information dominates that decision.[1121]

As for judicial control *ex post*, the courts are generally hesitant to exclude evidence. Except for core private information, there are no express rules on the exclusion of information obtained from surveillance. Courts apply a balancing theory, weighing the interests and values involved against each other,[1122] e. g., the degree of the infringement of personal rights and the purpose of the violated rules on the one side of the scale, and the general interest in truth-finding and an effective investigation, the seriousness of the crime, and the importance of the evidence on the other side.[1123]

German Courts have rejected a generally applicable "distant effect" of violations of procedural law. This means that the police can normally use evidence from illegal surveillance as a clue for further investigations.[1124] Violations have a "distant effect" only in exceptional cases where human dignity or fundamental rights have been violated, such as an intrusion into the "core area of privacy". If primary evidence from surveillance has been obtained by infringing upon the "core area of privacy", the evidence derived from the primary evidence is inadmissible.[1125]

Given the current practice of surveillance, there remains the question of how to restrict the power of the police more effectively. Some authors have suggested to reduce the scope of application of covert measures, by shortening and rendering more precise the crime catalogue provided in §§ 100a ff. StPO[1126] or by limiting the du-

[1121] Vgl. *Paeffgen*, in: Schünemann, u. a. (Hrsg.), Festschrift für Claus Roxin zum 70. Geburtstag, 2001, S. 1308 ff.

[1122] "Abwägungstheorie" has not been especially developed for evidence law but describes a general legal method; *Hubmann*, Wertung und Abwägung im Recht, 1997, S. 147.

[1123] See Section 2. c), Chapter IV, Part II.

[1124] *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung, 2003, S. 467 – 469. More suggestions to reduce the abuse of surveillance can be found here.

[1125] *Hauck*, in: Löwe/Rosenberg, StPO, Band 3/1, 27. Aufl., 2018, § 100a, Rn. 234; § 100d, Rn. 23.

[1126] *Schröder*, Beweisverwertungsverbote, 1992, S. 60 ff.

ration of surveillance permitted by each judicial order.[1127] Moreover, it has been suggested to enhance judicial control over surveillance measures in order to make possible substantial judicial review instead of a formal review, by investing greater human and financial resources to courts and to the training of judges.

[1127] *Paeffgen*, in: Schünemann, u. a. (Hrsg.), Festschrift für Claus Roxin zum 70. Geburtstag, 2001, S. 1313.

Part III

Technological Investigative Measures in the People's Republic of China

I. Telecommunication and Art. 40 of the Chinese Constitution

1. The Concept of Human Dignity in China

a) History

The People's Republic of China (hereafter referred to as PRC) was founded in 1949 by the Chinese Communist Party. The new government abolished the previous legal system, which had been introduced by the former government following the German/Japanese model (the "bad" capitalism model), and turned instead to the Soviet Union model.[1128] The first constitution of PRC was issued in 1954 (hereafter referred to as the *1954 Constitution*)[1129] with 106 articles in total. Chapter 3 with 19 articles provided the fundamental rights and obligations of citizens. Among them, Art. 90 protects the inviolability of the residence and the secrecy of communications.

At that time, the rights of citizens were regarded as a product of the political system.[1130] Therefore, the public interest and the party's interest enjoyed priority and individual rights only played a marginal role in the *1954 Constitution.* One obvious

[1128] Former Chinese President Mao Zedong had required the draft Committee of the constitutional law to read all the historical versions of the constitutions of the Soviet Union, especially its 1936 Constitution. *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 206. It was thus to be expected that the 1954 Constitution was deeply influenced by the 1936 Constitution of the Soviet Union. *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 206, Fn. 3. See also *Zhu/Wang*, in: *Zhang/Han* (eds.), 1954 年宪法研究 (the Study of the 1954 Constitution), 2005, 59; see also *Zhang*, 中国宪法史 (History of Chinese Constitutions), 2004, 332.

[1129] Between 1949 and 1954 there was a "Common Guideline" which worked as a temporary constitutional document. This is mainly because it was impossible to call upon a national-wide congress meeting directly after civil war in 1949. In 1952, the former Chairman of the Congress, LIU Shaoqi, visited Stalin. During this visit, Stalin pushed the Chinese Communist Party to call upon a congress meeting to introduce a formal constitution in 1954. See *Han*, 1954 年宪法与中国宪政 (The 1954 Constitution and Chinese constitutionalism), 2008, 35 – 51.

[1130] *Han*, 1954 年宪法与中国宪政 (The 1954 Constitution and Chinese constitutionalism) (2nd Ed.), 2008, 328.

evidence is that Article 101 of *1954 Constitution* emphasized the inviolability of public property.[1131]

The Chinese Constitution was massively modified three times after the *1954 Constitution*, in 1975, 1978 and 1982. The first two modifications were deeply influenced by extreme revolutionary thinking and made no contribution to the current discussion. The 1982 modification took place after a period of opening-up reform in China and led to the development of a new constitution (hereafter referred to as the *1982 Constitution*).[1132] On the one hand, this constitution returned, to a large degree, to the *1954 Constitution.*[1133] On the other hand, the *1982 Constitution* demonstrated that the Communist Party had rejected its more extreme policies of the previous decades. The *1982 Constitution* expanded the articles on the fundamental rights and obligations of citizens to 24 articles. The inviolability of the residence and the protection of the privacy of communications provided in Art. 90 in *1954 Constitution* were now provided in two separate articles, i.e., Articles 39 and 40. These two Articles remained unchanged by the following modifications.

The *1982 Constitution* is regarded as a correction to the former two versions of the constitution and as an improvement over the *1954 Constitution.* It is clear that individual rights receive better recognition in the *1982 Constitution*, since the Chapter about the rights and obligations of citizens has been placed ahead of the Chapter on the structure of the state institutions. Since then, the *1982 Constitution* has been modified five times, namely in 1988, 1993, 1999, 2004[1134] and 2018. With the former four modifications, the protection of individual rights was continuously improved. For example, the *2004 Constitution* recognized the inviolability of legal private property.[1135] Moreover, it introduced the term "human rights" into its text for the very first time. The *2018 Constitution* is more controversial because it established a new national institution, the Supervision Committee, with broad powers.[1136]

[1131] The ultimate aim of the Communist Party was to eliminate private property. According to the reform schedule at that time, the Party was very optimistic to believe that they can achieve this aim in the next decades. Therefore, the Party would not bother to emphasize the private ownership and then abolish it soon. The private ownership appeared only in Art. 11 and 12 under the General Guideline of *1954 Constitution.*

[1132] *Ji*, 宪法的理念与中国实践 (The Constitutional Idea and Chinese Practice), 2017, 12.

[1133] *Ibid.*; see also *Zhang*, 法学研究 (Research on Law) 3 (1982), 1; *Bao*, 张友渔学术精华录 (Memo of Scholarship of Zhang Youyu), 1988, 75.

[1134] *Ji*, 宪法的理念与中国实践 (The Constitutional Idea and Chinese Practice), 2017, 13.

[1135] The legal status of private ownership in the Constitution is a good indicator of the status of individual rights. *Id.* at 18–30. See also *Ji*, 当代中国研究 (Modern China Studies) 3 (1999), 48.

[1136] More details about supervision committees can be found in Section 2.c), Chapter III, Part III.

b) Human Rights and Human Dignity

In the current Chinese Constitution, human dignity ("人格尊严") is protected in Article 38, providing that: "The human dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directed against citizens by any means are prohibited." As the second sentence of this article shows, "human dignity" is not a general and overriding right, as it is in the German Basic Law,[1137] rather it refers to one's reputation and honor. Hence, in the Chinese Constitution, it is not clear whether "human dignity" includes the right to privacy, because insult, libel, false accusation or false incrimination do not infringe on privacy.[1138]

This article is followed by Article 101 of *General Principles of the Civil Law of the People's Republic of China* ("民法通则") (2009 Amendment, invalidated by the *Chinese Civil Code*): "Citizens and legal persons shall enjoy the right of reputation. The human dignity of citizens shall be protected by Law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited."[1139]

Art. 109 of the *Chinese Civil Code* ("中华人民共和国民法典"),[1140] however, gives a more general description: "The personal freedom and human dignity of a natural person shall be protected by law." Art. 110 follows: "A natural person enjoys the rights of life, inviolability and integrity of the person, health, name, likeness, reputation, honor, *privacy*, and marital autonomy, among others." Art. 110 can be regarded as a non-exhaustive enumeration for Art. 109. This article shows that at least in civil law, privacy is regarded as an aspect of human dignity. This clarification in civil law, however, has no binding effect on constitutional law, which has priority.

When the term "human dignity" is searched for in the national database of legal judgements, 17,101 results are shown.[1141] Among these, there are 400 criminal cases, 16,170 civil cases, 523 administrative cases and eight applications for national

[1137] *Lin*, 从宪法规范到规范宪法 – 规范宪法学的一种前言 (From Constitutional Norm to Normative Constitution – Foreword to Normative Constitution), 2017, 185.

[1138] Some scholars have argued that the term "human dignity" in Art. 38 of the Constitution covered the right to privacy before *General Provisions of the Civil Law (2017)* was issued. See *Zhang*, 宪法学导论 – 原理与应用 (Introduction of Constitution Theories – Principles and Application), 2014, 535. However, at that time, this argument had no legal basis. The opposite opinion, see *Wang*, 隐私权的宪法保护 (Constitutional Protection on the Right to Privacy), 2007, 231.

[1139] 中华人民共和国主席令第18号 (Order No. 18 of the Chinese President of the 11st Session). More legislation protecting human dignity can be found in *Liu*, 人格尊严及其实现 – 道德与法的双重考量 (Human Dignity and Its Realization – Double Considerations from Morality and Law), 2014, 249.

[1140] 中华人民共和国主席令第45号 (Order No. 45 of the Chinese President of the 13rd Session).

[1141] 中国裁判文书网(China Judgements Online): http://wenshu.court.gov.cn/, visited at 05.03.2019.

compensation.[1142] Among the criminal cases, the following criminal activities are frequently regarded as an infringement of human dignity:[1143] (1) the trafficking of children[1144] and women[1145]; (2) insulting (such as splashing excrements and urine on the body;[1146] pulling down a female victim's underwear and disclosing her intimate part in public;[1147] dragging a naked woman onto a busy street;[1148] sending messages with humiliating contents;[1149] uploading sexual videos of an individual to a chat group[1150]); (3) beating the victim in public with oral humiliation;[1151] (4) beating one's child with a jumping rope;[1152] (5) rape;[1153] (6) kidnapping;[1154] (7) molestation of women[1155] and children[1156]; (8) unlawful detention;[1157] (9) slander;[1158] (10) theft and insult to a corpse.[1159]

[1142] The cases where only one party or applicant invoked "human dignity" are included in the results. It does not mean that the judges finally confirmed that human dignity was involved.

[1143] This is an unexhaustive list.

[1144] Huang Huasheng et al., (2013) Ao High Court, Fourth Criminal Chamber, Final No. 51 (黄声华等人拐卖儿童二审刑事裁定书, (2013) 粤高法刑四终字第51号); Zhang Xianhui, Zhu Ying et al. (2016) Zhe Criminal Final No. 513 (章显辉、朱瑛等拐卖妇女、儿童罪二审刑事裁定书, (2016) 浙刑终513号).

[1145] Yang Fuxing, (2014) Gui Criminal Appeal Final No. 20 (杨兴富拐卖妇女二审刑事裁定书, (2014) 桂刑二终字第20号).

[1146] Peng vs. Chen, (2016) Xiang 04 Criminal Final No. 232 (彭某甲诉陈某侮辱案刑事裁定书, (2016) 湘04刑终232号); Deng Manfei, (private prosecution), (2018) Supreme Court, Criminal Complain No. 112 (邓满妃自诉侮辱刑事通知书, (2018) 最高法刑申112号); Yu Huan, (2017) Lu Criminal Final No. 151 (于欢故意伤害案二审刑事附带民事判决书, (2017) 鲁刑终151号).

[1147] Chen Jing and Li Chengfang (2017) Chuan 18 Criminal Final No. 16 (陈静、李成芳犯侮辱罪二审刑事附带民事裁定书, (2017) 川18刑终16号).

[1148] Li Longhe, (2014) An Criminal First Instance No. 44 (被告人李龙和强制侮辱妇女案一审刑事判决书, (2014) 安刑初字第44号).

[1149] Zhou Lingna and Zhou Guangying, (2018) Qian 0521 Criminal First Instance No. 174 (周玲娜、周光英非法拘禁一审刑事判决书, (2018) 黔0521刑初174号).

[1150] Zhao Huihui, (2018) Jin 1125 Criminal First Instance No. 99 (Ji No. 89) (赵辉辉一案刑事附带民事判决书, (2018) 晋1125刑初99号 (暨89号)).

[1151] Jiang XX and Li XX, (2016) Xiang 0726 Criminal First Instance No. 134 (江某某、李某某寻衅滋事案一审刑事附带民事判决书, (2016) 湘0726刑初134号).

[1152] Li Xjia, (2015) Pushao Criminal First Instance No. 13 (被告人李某甲故意伤害一案的刑事判决书, (2015) 浦少刑初字第13号).

[1153] Ren Wujian and Zhao Qing, (2011) Gan Third Criminal Court Final No. 73 (人武剑、赵庆犯绑架、强奸罪二审裁定, (2011) 甘刑三终字第73号); Zhang Yapeng, (2017) Chuan 0104 Criminal First Instance No. 838 (张亚鹏强奸罪(未遂)一审刑事判决书, (2017) 川0104刑初838号).

[1154] Ren Wujian and Zhao Qing, (2011) Gan Third Criminal Court Final No. 73 (人武剑、赵庆犯绑架、强奸罪二审裁定, (2011) 甘刑三终字第73号).

[1155] Feng XX, (2016) Hu 0118 Criminal First Instance No. 46 (冯某某强制猥亵妇女案一审刑事判决书, (2016) 沪0118刑初46号); Chen Anyi, (2018) E 1083 Criminal First Instance No. 200 (陈安宜盗窃罪一审刑事判决书, (2018) 鄂1083刑初200号).

From the above cases, it can be seen that simple cases of injury and killing are normally not considered as an infringement of human dignity. Children and women, however, are granted special protection. The courts follow a rather narrow concept of human dignity and relate it, to a large degree, to the feeling of humiliation experienced by the victim.[1160] In spite of this, compared to the Constitution, the courts have expanded the term "human dignity" to relate to cases such as rape and kidnapping rather than limiting the term to cases involving an insult.

Chinese courts have no right to interpret the text of the Constitution. Therefore, the Constitution cannot be directly applied and invoked in courts. This means that judges cannot interpret the constitutional term "human dignity" in their judgments. However, courts bypass this problem by discussing this terminology in a generalized way and do not connect it to any specific legislation, such as by referring to fairness.

As stated above, the sentence "[t]he state respects and protects human rights" was introduced into the preface of the Constitution in 2004.[1161] "Human dignity", on the other hand, is provided as a specific right of the citizen. In this context, the term "human rights" is not an equivalent concept to "human dignity". The former is overriding and provides the fundamental basis to all rights, while the latter is at the same level as other specific rights, such as the freedom of speech.[1162]

Lacking a broad definition and overriding status, human dignity is frequently ignored and infringed upon. Since human dignity is afforded a low value, it has a very weak position in the context of proportionality, which is often considered in public governance. Human dignity can be easily overridden by other values, such as the public interest; for instance, if the police were to use humiliation as a punishment or as a tool to maintain social order. There were also cases where the police forced prostitutes to dress up in yellow and expose themselves in public streets.[1163] In other cases, the police hung signs with the words "fraud criminal" outside houses in which

[1156] Li X.yang, (2017) Min 02 Criminal Final No. 301 (李某阳猥亵儿童二审刑事判决书, (2017) 闽02刑终301号); Li Yueqin, (2014) Baozhong, First Criminal Court Final No. 00127 (李月钦猥亵儿童二审刑事裁定书, (2014) 宝中刑一终字第00127号).

[1157] Lü Peng and other five, (2015) Kaitie Criminal First Instance No. 9 (吕鹏等六人非法拘禁一案刑事判决书, (2015) 开铁刑初字第9号).

[1158] Ding Manqin, (2018) Jin 08 Criminal Final 269 (丁满勤诽谤罪二审刑事裁定书, (2018) 晋08刑终269号).

[1159] Qin XX and Qin XX et al., (2018) E 9005 Criminal First Instance No. 170 (秦某某、秦某某等盗窃、侮辱尸体罪一审刑事判决书, (2018) 鄂9005刑初170号).

[1160] Some scholars have argued that the concept of human dignity has a broad sense and a narrow sense. See *Zhang*, 宪法学导论 – 原理与应用 (Introduction of Constitution Theories – Principles and Application), 2014, 536; *Lin*, 宪法学讲义 (Textbook on the Constitutional Law), 2015, 388.

[1161] See Section 1. a). Chapter I, Part III.

[1162] See *Zhang*, 宪法学导论 – 原理与应用 (Introduction of Constitution Theories – Principles and Application), 2014, 536, Fn. 1160.

[1163] *Lin*, 宪法学讲义 (Textbook on the Constitutional Law), 2015, 388–389; see also *Hu/Han*, 中国宪法 (Chinese Constitutional Law), 2018, 238.

the family of fraud offenders lived.[1164] Nowadays, some cities have adopted camera systems to catch the faces of pedestrians who do not follow the traffic lights and show their faces on a huge LED screen beside the road.[1165]

c) Privacy in the Constitution

It is well recognized that the right to privacy is essential to the development of the personality and the rights of the individual. For a long time, however, "privacy" carried negative connotations because it was associated with issues that people felt shame discussing within traditional Chinese culture, such as sexual relations.[1166] After the foundation of the PRC, state powers suppressed the private area and people were effectively "owned" by the state; for instance, a marriage required the permission of the government.[1167] In such a society, prioritizing individual rights or concerns was regarded as selfish.

Although the current generation focuses increasingly on their personal rights, the concept of "public first, private second", or the spirit of sacrifice, is still just as highly regarded as it was in the imperial era.[1168] This similar social attitude derives from different foundations, however; now it is based on socialist principles, formerly it was connected with traditional culture (such as Confucianism). Due to this tension, there is a heated debate regarding the right to privacy in China, and its legal protection lags behind.

The right to privacy is not expressly mentioned in the Constitution. The majority opinion is that the right to privacy is included in the "human rights" referred to in the preamble of the Constitution, in the reference to "human dignity" in Art. 38, the statement regarding the inviolability of the residence in Art. 39 and in the citation of the protection of telecommunication in Art. 40.[1169] In 1988 and 1993, the Supreme Court stated in judicial explanations that the disclosure of one's private information without permission can be regarded as a violation of the right to reputation provided in Art. 101 *General Principles of the Civil Law* (1986 and 2009).[1170] Later, the right to

[1164] Source: http://365jia.cn/news/2019-02-15/6AD22C66F888B30A.html, visited 06.03.2019.

[1165] Source: https://www.sohu.com/a/225980515_355764, visited 06.03.2019.

[1166] *Wang*, 隐私权的宪法保护 (Constitutional Protection of the Right to Privacy), 2007, 227–229.

[1167] *Id.* at 229.

[1168] *Ibid.*

[1169] *Yang*, 宪法隐私权导论 (Introduction to the Right to Privacy in the Constitutional Law), 2010, 169.

[1170] Art. 140 of *The Supreme People's Court's Opinions on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation)* ("最高人民法院关于贯彻执行《中华人民共和国民法通则》若干问题的意见(试行)") (1988) (Invalid on 24.12.2008) (法(办)发(1988)6号); Art. 7 of *the Responses of the Supreme People's Court on Several Issues about the Trial of Cases Concerning*

privacy was formally recognized in legislation, such as Art. 49 of the *Law on the Protection of Juveniles* ("未成年人保护法") (2020),[1171] and *the Chinese Civil Code* mentioned above.

2. Freedom and Privacy of Correspondence

a) Definition of "Correspondence"

Article 40 of *the Constitution* provides:

> "The freedom and privacy of correspondence ("通信") of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon citizens' freedom and privacy of correspondence, except in cases where, in order to meet the needs of state security or of criminal investigation, public security or procuratorial institutions are permitted to censor correspondence according to procedures prescribed by law."

This provision protects two different but closely related rights, namely, the freedom of correspondence and its privacy.[1172] The former focuses on the act of freely communicating with others. The latter focuses on the contents of the correspondence. The Chinese term "通信" (English translation: correspondence) has a narrower meaning than communication ("交流"). "通信" refers to communications that are not conducted face to face, such as letters, phone calls, emails, fax, online chatting, etc.[1173] The privacy of correspondence covers not only its contents but also related information, such as the addresses of the correspondents (including email addresses, IP addresses), the dialed numbers, the time and the duration of the call.[1174] In other words, Art. 40 protects the act of communicating and the contents of correspondence from illegal interference, surveillance, disclosure, withholding, and review. It imposes this obligation on the state but also on individual citizens.[1175]

One district court, however, has ruled that an employee has no right to withhold his business correspondence from the employer.[1176] In this case, lawyer W discovered

---

the Right of Reputation ("最高人民法院关于审理名誉权案件若干问题的解答") (1993) (Invalid) (法发(1993)15号).

[1171] 中华人民共和国主席令第57号 (Order No. 57 of the Chinese President).

[1172] *Zhou*, 法学 (Law) 6 (2006), 57, 58.

[1173] *Id.*, at 59.

[1174] *Ibid.* This article also argues that information on the owner of the communication device, such as ID numbers and home addresses, are also covered by the secrecy of correspondence. See also *Chen*, 全国首例起诉电信来电显示侵权案被当场驳回 (Court Rejected the Claim on Tort of Caller Display), https://it.sohu.com/20040827/n221768888.shtml, visited at 08. 12. 2020.

In this case, the court ruled that the dialing numbers belong to privacy.

[1175] *Zhou*, 法学 (Law) 6 (2006), 57, 59.

[1176] *Id.* at 60.

that a letter sent to him by his client was opened by his law firm. W sued the law firm claiming that his right to privacy of correspondence under the *Law of Mail* was violated.[1177] This claim was not accepted by the court.[1178] In China, it is widely recognized that an employer has the right to read business correspondence without the employee's permission, based on their employment contract. If the employer opens a private letter sent to a work address, however, the employer can be liable under tort law, unless the employer can demonstrate that he or she acted without fault because he or she could not have known that it was a private letter.[1179] Moreover, there is no lawyer-client privilege in China. Art. 14 of the *Lawyer Law* provides that "A law firm is a firm where a lawyer practices law". This means that the representation contract can only be concluded between the law firm and the client. Afterwards, the law firm refers to the client by the name of a lawyer representing him. Therefore, in principle, law firms can read the correspondence between clients and employees. In sum, the individual does not enjoy a right to privacy of his or her business correspondence.

b) Privacy of Correspondence and the Power of the Courts to Order Evidence

According to Art. 40 of the Constitution, the security and prosecution services are the only authorities permitted to intercept correspondence, in accordance with procedures prescribed by law; moreover, correspondence can only be intercepted for the needs of state security or criminal investigation. In practice, however, interception also may be ordered by courts in order to collect telecommunication information as evidence according to Art. 67 of the *Civil Procedure Law* ("民事诉讼法").[1180] For example, in 2003, in order to carry out an administrative judgment, a court ordered a telecommunication company to provide the call list of an individual's phone. The company refused to do so based on Art. 40 of the *Constitution* and Art. 66 of the previous version of the *Telecommunication Regulation of the People's Republic of China* (now Art. 65). The court then imposed a sanction against this company based on the fact that the company had violated its obligation under Art. 67

[1177] Because the Constitution cannot be directly applied in the trial, the legal claim has to be based on other legislation. Art. 3 of the *Law of the Mail* is almost identical with Art. 40 of the Constitution.

[1178] More details on the case can be found in *Li/Yang*, 律师请王海代理索讨通信秘密权案 (Mr. Hai WANG Represented Lawyers to Sue for the Right to Confidence of the Correspondence), 法制日报 (Legal Daily), 23.12.2002. The argument is supported by *Zhou*, 法学 (Law) 6 (2006), 57, 60.

[1179] From an interview on 08.03.2019 with Ms. Meng LI who has practiced labor law for more than five years in China.

[1180] 中华人民共和国主席令第71号 (Order No. 71 of the Chinese President of the 2nd Session). First sentence of Art. 67 *Civil Procedure Law:* "A people's court shall have the authority to investigate and collect evidence from the relevant entities and individuals, and the relevant entities and individuals shall not refuse such investigation and collection of evidence."

of the *Civil Procedure Law.*[1181] In this case, the company asked the parliament of the province to give a legislative explanation. The provincial parliament stated that the freedom and privacy of the correspondence are constitutional rights. According to Art. 40 of the *Constitution* and Art. 66 of the previous version of the *Telecommunication Regulation*, telecommunication information can only be collected by the security or prosecution services for the purpose of criminal prosecution or public security. For example, a call list contains a great deal of private information and thus its contents fall within Art. 40 of the *Constitution.* When a court collects evidence according to Art. 67 of *the Civil Procedure Law*, it should not violate the *Constitution* and should not infringe upon an individual's fundamental rights. This explanation has been confirmed by the national parliament.[1182]

In 2005, however, a similar case occurred in another province, where a telecommunication company was fined by a local court.[1183] Moreover, in another 2005 case, Ms. A sued Mr. B for sexual harassment because B kept sending her messages with sexual content. A showed the court these messages. B argued that A had sent him similar messages, so it was not sexual harassment. B, however, had not stored the messages that A had sent him, so he asked the court to order the telecommunication company to recover these messages and present them to the court. The court did so. A appealed and argued that the first instance court had violated her rights under Art. 40 of the *Constitution.* In the second instance, the court denied A's claim.[1184]

The latter two cases were both decided after the legislative explanation had been given in the first case. Some writers supported the latter two court decisions, arguing that the freedom and the privacy of correspondence are not unlimited.[1185] That argument, however, is not convincing. On the one hand, it is true that such a right should and can be restricted. On the other hand, Art. 40 of the *Constitution* provides clearly which institutions can infringe upon that right and in what situations such a right may be restricted. The court and non-criminal cases are not mentioned in the *Constitution.* Limiting restrictions to criminal cases is reasonable because fundamental human rights should only be restricted in extreme situations.[1186] As long as Article 40 of the

[1181] *Zhou*, 法学 (Law) 6 (2006), 57, 59 – 60.

[1182] *Standing Committee of the Parliament of Hunan Province and the Standing Committee of National Parliament*, 中国人大 (Chinese Parliament), Vol. 13, 2004.

[1183] *Li*, 中国电信业 (Chinese Telecommunication) 118 (2010), 46, 47.

[1184] "性骚扰"案女主角:法院取证违宪 (The Plaintiff of the Sexual Harassment Case: the Collection of Evidence by the Court is Unconstitutional), Chengdu Business Post, 21. 02. 2006. What can be argued in the above sexual harassment case is that B applied to the court to get his own chatting history. It is not clear whether the permission of other parties to a communication is needed in such a situation.

[1185] *Wang*, 巴南女教师性骚扰案宪法性分析 (Constitutional Analysis on Sexual Harassment on Female Teacher in Banan), Master Thesis in Chinese Southwest Political Science and Law, 2008.

[1186] However, it is a problem here that the criminal courts are also not qualified to order information on correspondence. This situation results from the weak position of the courts in the

Constitution is not amended, the court has no power to order a telecommunication company to disclose the correspondence of a citizen, even in a criminal case.

c) Interception of Letters of Prisoners

Art. 47 of the *Prison Law* ("监狱法")[1187] provides that prisoners can correspond with others but that their letters are to be reviewed by prison officials. Letters written to the judicial department are free from review. The constitutionality of this provision has been put into doubt by some legal experts who argue that Art. 40 of the *Constitution* does not authorize prisons to infringe upon the freedom of correspondence.[1188] Although prisons are responsible for investigating crimes committed in prison, Art. 40 of the *Constitution* makes no exception. Moreover, even if the right to intercept letters were covered by the investigation power of prisons, such measures should be limited to letters that might be related to crimes and should not extend to every letter written by a prisoner.[1189] One way to resolve this conflict is to amend Art. 40 of the *Constitution* to authorize prison administrators to intercept prisoners' letters. These measures should be permitted only in the interest of public security and criminal investigation. The other option is to amend Art. 47 of the *Prison Law* to prohibit the prison administration from reviewing prisoners' letters, but that is highly unlikely.

II. The Inviolability of the Residence and Art. 39 of the Chinese Constitution

As stated above, the inviolability of the residence and the privacy of correspondence were both provided in Art. 90 of the *1954 Constitution.*[1190] In the 1975 and 1978 Constitutions, the inviolability of the residence was provided together with the right to personal freedom. This demonstrates that, for quite some time, the legislature did not have a clear understanding of the relationship between these three rights, namely, which one falls within the category of the inviolability of the residence.[1191] Only since the *1982 Constitution* have these three rights been provided for in separate articles. By doing this, the legislature granted these rights equal status.[1192] Moreover,

---

Chinese criminal justice system. For instance, it is the prosecution, not the court, that issues warrants. The courts are not involved at all before the cases are charged.

[1187] 中华人民共和国主席令第63号 (Order No. 63 of the Chinese President).

[1188] *Tang*, 法学 (Law) 12 (2007), 13.

[1189] *Ibid.*

[1190] See Section 1. a), Chapter I, Part III.

[1191] *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 206–209.

[1192] *Id.* at 209.

it is easier to prescribe different conditions for different rights when they are provided for separately.[1193]

1. Definition of Residence

Art. 39 of the *Constitution* provides: "The residences of citizens of the People's Republic of China are inviolable. Unlawful searches of or intrusions into a citizen's residence are prohibited." The Chinese term "住宅" (residence) is used. This word consists of two Chinese characters: the first character means "living", and the second character means house or residence place. In the traditional and daily use of the language "宅" (house or residence place) refers only to private houses. So, the use of this specific Chinese character reflects the position of the legislature that Art. 39 of the *Constitution* protects only private residences used for daily life. It follows that offices and cars are not regarded as residences.

As with the term "human dignity", no cases can be found which interpret the constitutional term "residence" directly.[1194] The closest thing to an interpretation of the term by the Supreme Court can be found in three Judicial Explanations concerning the crimes of theft and robbery,[1195] i.e., Art. 3 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Theft* (2013) ("最高人民法院、最高人民检察院关于办理盗窃刑事案件适用法律若干问题的解释")[1196] (hereafter referred to as the *Interpretation on Theft*); Art. 1 of the *Opinion of the Supreme People's Court on the Application of Laws for the Trials of Criminal Cases Involving Robbery or Seizure* (2005) ("最高人民法院印发<关于审理抢劫、抢夺刑事案件适用法律若干问题的意见>的通知")[1197] (hereafter referred to as the *Opinion on Robbery or Seizure*); Art. 1 of the *Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Robbery* (2000) ("最高人民法院关于审理抢劫案件具体应用法律若干问题的解释")[1198] (hereafter referred to as the *Interpretation on Robbery*).

[1193] *Ibid.*

[1194] See Section 1.b), Chapter I, Part III.

[1195] These three Judicial Explanations explained another Chinese word "户"(living place of household), different from "住宅" ("residence") used in the *Constitution.* However, it argues that "户" is normally considered to have the same meaning as "住宅" used in Art. 254 of *CCL* (illegally intruding into others' residences) which is the same word with the one used in the *Constitution.* See *Wang*, 河南财经政法大学学报 (Review of Henan University of Business and Political Science) 2 (2016), 97, 101; *Du*, 法学家 (Legal Scholar) 2 (2015), 15, 16. The two words are often both translated as "residence" in English. For instance, http://www.pkulaw.com/en_law/c7096bf940368bd8bdfb.html, visited 10.03.2019.

[1196] 法释(2013)8号.

[1197] 法发(2005)8号.

[1198] 法释(2000)35号.

In accordance with Art. 1 of the *Interpretation on Robbery*, "intruding into another person's residence to rob" means that a person enters "a location where another person is living, which is comparatively separated from the outside (including isolated courtyards, tents of herdsmen, fishing boats used for family living, and rented houses)" to commit robbery. Art. 1 of the *Opinion on Robbery or Seizure* offered a further interpretation of the meaning of "intruding into another person's residence to rob". "The term 'residence' in this context refers to a domicile with two characteristics: a place for the family life of another person and a place that is comparatively separated from the outside." The former refers to function and the latter to location. As a general rule, a collective dormitory, a hotel, a work shed or any temporary building is not deemed a 'residence'. fic circumstances, however, a place with these characteristics may be regarded as a 'residence'. Art. 3 of the *Interpretation on Theft* provides that whoever illegally enters a residence which is for family living of others and is relatively separated from the outside and commits theft therein shall be deemed as "intruding into another person's residence to commit theft".

In the case law, it has been well established that a multi-functional place can be regarded as a residence.[1199] In a very famous case, police broke into a private clinic at around 11pm (outside business hours) because a couple was watching sex videos.[1200] The key issue was whether a clinic outside business hours is regarded as a residence or as a public place. The case was dropped for lack of sufficient evidence and the police apologized. Although the prosecutor did not directly declare that the clinic was a residence, the fact that the case was dropped suggests that the prosecutor regarded it as a residence. In another case, the victim conducted a business in his shop during daytime and lived there during the night. When a robber broke into the shop at night, this was treated as "intruding into another person's residence to rob".[1201] According to

[1199] *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 23.

[1200] See *Zhang*, 法学家 (Legal Scholar), Vol. 3, 2003, 10. In China, watching sexual video in public is punishable.

[1201] See Zhuang Baojin robbery case, (2000) Supreme Court, No. 59, 刑事审判参考 (References to Criminal Judgements), 8 (2000), 18. Other similar cases: Yin Dongjin robbery and theft case, 中国审判案例要览 (Overview of Chinese Judgements) (Criminal Volume 2001), National College of Judges and the Law School of Chinese Renmin University (ed.), 2002, 232; Du Yi Robbery and blackmail case, (2002) Yi Criminal Final No. 33 (杜义抢劫、敲诈勒索案，(2002) 宜刑终字第33号) (a personal shop was robbed in the late night and it is defined as "intruding into another person's residence to rob") ; Lin Jianbo et al. robbery case, (2002) Longxin Criminal First Instance, No. 180 (林剑波等抢劫案，(2002) 龙新刑初字第180号) (a cloth store was robbed in the late night and it is defined as "intruding into another person's residence to rob"); Li Weiqing robbery and obstruction of the public duties, (2003) Mei Criminal First Instance, No. 74 (李维清抢劫、盗伐林木、妨害公务案，(2003) 梅刑初字第74号) (the living room in a petrol station was robbed in the midnight and it is defined as "intruding into another person's residence to rob"); Wei Peiming et al. robbery case, (2002) Hu Second Middle Court Criminal Final No. 511 (魏培明等人抢劫案 (2002) 沪二中刑终字第511号) (the shop was robbed during the business hours and "intruding into another person's residence to rob" was denied); Zhang Shiming robbery case, Supreme Court No. 590, 刑事审判参考 (References to Criminal Judgements) 71 (2010), 30 (the shop was robbed in the midnight and it is defined as "intruding into another person's residence to rob").

this decision, during business hours the location was not a residence, while outside business hours it changed into a residence. Therefore, according to the courts' opinion, the function is the most important criterion for defining a residence.

Art. 1 of the *Opinion on Robbery or Seizure* has to a large degree narrowed the scope of the term "residence" by referring to "family life". Based on this element, the courts expressly excluded collective dormitories,[1202] hotels[1203] and temporary work sheds.[1204] Compared to typical private residences, these three locations provide less privacy and have a more social function. In most cases, people stay there for temporary purposes instead of living a private life. The length of stay and the intention of the inhabitant are also taken into consideration. For instance, a room that is rented by the day for the purpose of having sex is not regarded as a residence.[1205] Moreover, an apartment rented jointly by students has been ruled not to be a residence because it is not for "family life".[1206] The reasoning behind this Supreme Court ruling could be that "intruding into another person's residence to rob" is regarded as one of the most serious crimes and is punished by at least ten years imprisonment or even the death penalty, the same sentencing range as homicide. Therefore, the Supreme Court wanted to limit the application of this crime and to avoid a frequent imposition of this severe penalty.[1207] In practice, however, lower courts tend to recognize jointly rented apartments as residences. Especially for young people in big cities, living in a jointly rented apartment has become a normal way of living. In one case, the lower court argued that intruding into such an apartment is not different from intruding into a family house. Both locations enjoy privacy and excludability.[1208] It would be unfair if

[1202] See Liang Shan, (2004) Long Criminal First Instance No. 198 (梁山等抢劫案,(2004) 龙刑初字第198号) (student dormitory is not regarded as "residence").

[1203] See Yang Tingxiang et al., High Court No. 309, Shandong Province, 刑事审判参考 (References to Criminal Judgements) 39 (2005), 31 (a family hotel was robbed and "intruding into another person's residence to rob" was denied); Liu X et al., (2006) Yu Fourth Middle Court Criminal First Instance No. 15 (刘某等抢劫案,(2006) 渝四中法刑初字第15号 刑事判决书) (the "residence" is denied where own living house is operated as a hotel); Feng Yujie and Han Weiwei, (2011) Zheng Criminal Revision No. 2 (冯玉杰、韩伟伟抢劫案,(2011) 郑刑再终字第2号刑事判决书) (the hotel room is not regarded as the "residence").

[1204] See Zhou Hurong et al., 人民法院案例选·月版 (Case Selection of the Courts) (monthly version), 10 (2010), 8 (workers' dormitory is not regarded as the "residence"); Wang Zhijian, Supreme Court No. 613, 刑事审判参考 (References to Criminal Judgements) 73 (2010), 30 (workers' dormitory is not defined as the "residence").

[1205] See Deng Jianyi, (2007) Nan Criminal First Instance No. 123 (邓建义等抢劫案, (2007) 南刑初 字第123号刑事判决书).

[1206] See Han Qingdong et al., (2006) Xi Middle Criminal Final No. 96 (韩庆东等抢案 (2006) 宜中刑终字第96号); Lin Lizhu and Bi Yanting, (2006) Su Second Criminal Chamber in Middle Court, Criminal Final No. 26 (林立柱、毕研亭抢劫案,(2006) 苏中刑二终字第26号刑事判决书).

[1207] The Comments on Han Qingdong et al. robbery case, 人民法院案例选 (Case Selection of the Courts), 56 (2006), 69. Similar ideas can be found, for instance, in *Huang*, 政治与法律 (Political Science and Law) 6 (2005), 138, 139; *Du*, 法学家 (Legal Scholar) 2 (2015), 15, 23.

[1208] See Han Wei robbery case, 刑事审判参考 (References to Criminal Judgements), 59 (2008), 24.

the *Chinese Criminal Law* (hereafter referred to as *CCL*) did not protect such residences.[1209] The court further stated that a property should be regarded as a residence if it is comparatively isolated from the outside and its occupancy is relatively stable.[1210] In order to avoid a potential violation of Art. 1 of the *Opinion on Robbery or Seizure*, this court emphasized that this Article did not change the meaning of Art. 1 of the *Interpretations on Robbery* and that they follow the same standard.[1211] It cannot be denied, however, that these two judicial explanations use different terminology. This judgment has actually expanded Art. 1 of the *Opinion on Robbery or Seizure* and went back to Art. 1 of the *Interpretations on Robbery.*

Limiting the scope of "residence" to places of family life should be regarded as unconstitutional. Any unreasonable restriction of the legislation causes negative effects, especially when the Constitution cannot be directly applied. If judges find that the legislation or the judicial explanation is unconstitutional, their only choice is to consider the issue of so-called "social fairness".[1212] It is true that the punishment level for robbery should generally be lower than for homicide. This is, however, a problem at the legislative level and cannot be properly solved by an unreasonable limitation of the scope of the term "residence". This interpretation therefore violates Art. 39 of the *Constitution.*

The common understanding of "residence" among constitutional law scholars is much broader than that of the judicial explanation, although it is still much narrower compared to the German or American understanding of the term.[1213] Nevertheless, it is widely recognized by constitutional scholars that hotel rooms and dormitory rooms offered by universities are covered by Art. 39 of the *Constitution.*[1214] It is, however,

[1209] *Id.* at 23.

[1210] *Ibid.*

[1211] *Id.* at 22.

[1212] The Supreme Court has expressly prohibited the lower courts from even referring to the Constitution. See *Response of the Supreme Court regarding that the Constitution cannot be relied on as a basis for conviction and sentencing 1955* (1955年最高人民法院"关于在刑事判决中不宜援引宪法作论罪科刑的依据的批复") (Invalid); *Response of the Supreme Court regarding the Rules on the Citation of Legislation and Regulations in Documents produced by the Courts 1986* (1986年最高人民法院"关于人民法院制作法律文书如何引用法律规范性文件的批复") (法[研]复 (1986) 31号) (Invalid); *Rules on the Citation of Legislation and Regulations in Judgements 2009 by Supreme Court* (2009)年最高人民法院"关于裁判文书引用法律、法规等规范性法律文件的规定") (法释(2009)14号). See also *Du*, 法学家 (Legal Scholar) 2 (2015), 15, 26.

[1213] For example, *Zhou*, 宪法基本权利:原理·规范·应用 (Fundamental Rights in Constitutional Law: Principle, Norm, Application), 2006, 114. The author argued that the definition of residence does not require permanent occupancy.

[1214] *Huang*, 住宅不受侵犯权研究(Inviolability of Residence), 2014, 23; *Ni*, 从住宅不受侵犯权看高校对学生宿舍的检查 (Study on the Checking of Students' Dormitories by the University from the Perspective of the Inviolability of Residence), Master Thesis in Nanjing Normal University, 12.

still a common practice for universities to perform checks of dormitory rooms for different purposes, such as sanitary examination or fire control.[1215]

The best solution for guaranteeing the inviolability of residences and the privacy of telecommunication as well as other constitutional rights would be to allow a direct application of the *Constitution*. This step, however, cannot be expected in the foreseable future due to political considerations. Therefore, the best possible way to improve the constitutional protection is to ensure the constitutionality of legislation and of judicial explanations.

2. The Limited Understanding of "Illegal Search" and "Illegal Intrusion"

The second sentence of Art. 39 of the *Constitution* explains the meaning of the term "inviolability": "Any illegal search of or intrusion into a citizen's residence is prohibited." This is reflected in Art. 245 of the *CCL*, which provides that: "(1) Those illegally searching others' body or others' residences, or those illegally intruding into others' residences, are to be sentenced to no more than three years in prison or put in criminal detention. (2) Judicial workers committing crimes stipulated in the above paragraph by abusing their authority are to be severely punished." This provision includes two crimes: illegal search and illegal intrusion into another person's residence.

The Chinese word for "searching" and "search" is "搜查", the word-to-word translation is "searching and checking". In the legal context, this word is used to specifically refer to searches for the purpose of criminal investigation.[1216] For example, Art. 222 of the *Provisions on the Procedures for Handling Criminal Cases by Public Security Organs* ("公安机关办理刑事案件程序规定") (2020 Revision) (hereafter referred to as the *Procedures for Criminal Cases* 2020)[1217] provides that: "In order to collect incriminating evidence and to arrest the suspect, with the permission of the president of the county police station or above, an investigator may search the body of the suspect as well as the body of other persons, objects, residences and other places where a suspect or evidence can be found." This provision treats the human body, objects and residences in parallel, much like the 4th Amendment to the U.S. Constitution. Chinese law, however, limits searching a residence to a physical level.

[1215] If any dormitory room is found to violate the room regulations, as a "punishment", the students living in that room are normally required to write a statement apologizing for what they did and promising that they will never do it again. One university announces the results of its weekly check on dormitories on its website: http://www.pharm.sdu.edu.cn/info/1048/9079.htm, visited at 10.03.2019.

[1216] *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 228.

[1217] 中华人民共和国公安部令第159号 (Order No. 159 Ministry of Chinese Public Security).

According to academic literature and case law, searching and intruding ("侵入") in Art. 39 of the *Constitution* and in the *CCL* mean the same. Therefore, an intrusion also should be understood as a physical act. According to the explanation of Art. 254 of the *CCL*, illegal intrusion means that someone enters another person's residence illegally and forcefully without permission or refuses to leave the residence after he or she has been asked to leave.[1218] A non-physical search and intrusion, i.e., surveillance of telecommunication or conversations within the residence, is not covered.

This raises a dilemma. Given that there are no other articles in the *Constitution* referring to acoustic surveillance, citizens have no constitutional protection against such surveillance of their residence unless acoustic surveillance of a residence is regarded as an infringement on the inviolability of the residence. Compared to the privacy and the freedom of correspondence protected by Art. 40 of the *Constitution*, conversations within residences enjoy even less protection. This is inconsistent. According to common understanding, activities, including conversations, in a residence should enjoy more, or at least not less protection than telecommunication. On the other hand, if the acoustic surveillance of a residence were regarded as an infringement on the inviolability of the residence, any "invisible" surveillance of the residence, regardless of whether it is legal (with permission) or illegal (without permission), would violate Art. 39 of the *Constitution*, because such a surveillance is not a search or intrusion and thus is not legitimate under Art. 39 of the *Constitution.*

To afford true inviolability of the residence, it would be necessary for Art. 39 of the *Constitution* to cover "invisible" surveillance. As a result, such measures should be regarded as a "search" and "intrusion" provided in the second sentence of this article. This is also how case law in the U.S. developed, from purely physical intrusion to invisible surveillance. Another possible solution is to understand the physical and illegal "search" and "intrusion" as a non-exhaustive enumeration, so that any other equivalent or more severe measure, such as destroying the house, could be included.[1219] In that case, the invisible surveillance of a residence would be covered. Both solutions would need a direct explanation of Art. 39 of the *Constitution* by the Parliament; the Supreme Court cannot go so far with a judicial explanation.

It should be kept in mind in this context that the role of the Constitution in Chinese law is strictly limited. In contrast to constitutions of European countries, the *Chinese Constitution* has often been described as a book that is kept on top of the shelf,

[1218] *Criminal Law Division of the Standing Committee of National Parliament*, 中华人民共和国刑法:条文说明、立法理由及相关规定 (Criminal Law of People's Republic of China: Interpretation of Texts, Reasons of Law-making and Related Rules), 2009, 502.

[1219] See *Politics Sub-division of the Research Division of the Standing Committee of National Parliament*, 中国宪法精释 (Interpretation of the Chinese Constitution), 1996, 165.

acquiring dust. The rights provided in the *Constitution* are often violated by the government itself.[1220] If the government presents a bad example, others will follow.

Since the central government does not wish to relinquish the final authority on fundamental issues, it will in the forseeable future not grant courts the power to interpret the *Constitution.* Nevertheless, demands for judicializing the *Constitution* have been raised for decades and this issue is also a popular topic of research in constitutional law. In most textbooks and literature on constitutional law, a discussion of the possibility of a judicialization of the Constitution can be found.[1221] This would be the most effective way for the Constitution to regain credibility and respect.

Due to the inapplicability of the Constitution, the lack of protection of residences on the constitutional level makes almost no difference in practice. The acoustic surveillance of a residence and the interception of correspondence both belong to the category "Technological Investigative Measures" ("技术侦查措施", hereafter abbreviated as TIMs) regulated in Section 8 (Technological Investigative Measures), Chapter two (investigative measures) of the *Chinese Criminal Procedure Law (CCPL)*, which applies to all TIMs. Both types of measures follow exactly the same procedures for application and implementation.[1222] Moreover, the procedure for TIMs is stricter than that for conventional searches. Art. 222 of the *Procedures for Criminal Cases*[1223] only requires a permission from the president of a county police station for a house search warrant, while the permission for TIMs can only be approved by the president of a city police station or above.[1224]

The inviolability of residences is rarely respected, especially by state power in China. For example, since individuals cannot own the land on which their residences have been built, if the local government wants to use the land for other purposes (such as building a factory), the houses on the land will be destroyed regardless of whether the inhabitants support these plans.[1225] Another example of this situation occurs with administrative controls or checks.[1226] Even for the purpose of criminal investigation,

[1220] For example, it is quite common that job announcements for civil servants declare that only males are qualified to apply for the positions.

[1221] *Zhang*, 宪法学导论 – 原理与应用 (Introduction of Constitution Theories – Principles and Application), 2014, 160 and following pages; *Hu/Han*, 中国宪法 (Chinese Constitutional Law), 2018, 145; *Lin*, 宪法学讲义 (Textbook on the Constitutional Law), 2015, 405.

[1222] More procedural details can be found Chapter 0, Part III.

[1223] See Fn. 1217.

[1224] More details about the approval process of TIMs can be found Section 1, Chapter IV, Part III.

[1225] This often causes violent confrontations between the house owners and executors sent by the government. It is not rare that people are killed in such conflicts. Therefore, this practice is harshly criticized. This issue is more often discussed in the context of the right to property. See *Hu/Han*, 中国宪法 (Chinese Constitutional Law), 2018, 265.

[1226] A case reported in *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 222. The administrative institution who controls tobacco transactions searched W's residence and shop with an administrative document. According to the law, this document can only be used to examine business places. Art. 46 of the *Regulation on the Implementation of the Law of*

there is no real procedural control on issuing search warrants, since the police are omnipotent when making these decisions. Moreover, this procedure does not distinguish between residences and other places, such as business areas. This means that residences do not receive any special protection in the view of the police.

A better way to protect residences would be to limit searches to criminal investigations, excluding searches for administrative control. Secondly, procedural law should introduce more detailed procedural control on searches by the police.

Many writers confirm the close relationship between the right to privacy and the inviolability of the residence.[1227] Compared to the U.S., however, Art. 39 of the *Chinese Constitution* still retains a typical trespass theory, which only protects the two dimensions of residences instead of protecting all three dimensions of the space. This is far from sufficient for the protection of the inviolability of the residence.

III. Technological Measures in Legislation and Departmental Regulations

1. The Purpose of Criminal Procedure

The policy behind criminal procedural law in every jurisdiction influences the distribution of investigative authority. Art. 1 of *CCPL* provides "To ensure the correct enforcement of the Criminal Law, punish crimes, protect the people, protect national security and public security, and maintain the order of socialist society, this Law is formulated in accordance with the Constitution." This article shows that the direct purpose of criminal procedure is to enforce the *CCL*, and that its ultimate purpose is to (1) punish crime; (2) protect the people; and (3) protect security and social order. According to the explanation given on the *CCPL* by the Standing Committee of the National Parliament, "protect the people" here means to protect the people from crimes by punishing criminals.[1228] The protection of the rights of suspects or defendants is not mentioned here. This reveals the attitude of the legislature regarding criminal procedure: the procedure mainly serves substantive criminal law, and its own independent value is of lesser relevance; and the public interest is dominating all other purposes.

---

the People's Republic of China on Tobacco Monopoly (中华人民共和国烟草专卖法实施条例) (2016 Revision) (中华人民共和国国务院令第666号 (Order No. 666 the Chinese State Council)) (Art. 49 of the previous version).

[1227] *Huang*, 住宅不受侵犯权研究 (Inviolability of Residence), 2014, 101; *Zhang*, 宪法学导论 – 原理与应用 (Introduction of Constitution Theories – Principles and Application), 2014, 648 et seq.

[1228] *Criminal Law Division of the Standing Committee of National Parliament*, 中华人民共和国刑事诉讼法:条文说明、立法理由及相关规定 (Criminal Procedure Law of People's Republic of China: Interpretation of Texts, Reasons of Law-making and Related Rules), 2008, 1.

This position has been enhanced by Art. 2 *CCPL:* "The objectives of the Criminal Procedure Law of the People's Republic of China are to ensure the accurate and timely finding of criminal facts and the correct application of the law, to punish criminals, to ensure that innocent people are not incriminated, to safeguard the socialist legal system, to respect and protect human rights, to protect personal rights, property rights, democratic rights, and other rights of citizens, and to ensure smooth socialist construction." This provision demonstrates that the primary task of the *CCPL* is to find the truth. The phrase "protect the personal rights" was only added in 2012. In the past and even today, the goal of finding the truth guides criminal proceedings, while the protection of human rights and the rights of defendants plays only a marginal role. The emphasis on finding the truth and punishing crime has a strong influence on the investigative power and on the scope of exclusionary rules.[1229]

2. Power Distribution in Criminal Investigations

a) The Dominant Role of the Police during the Investigation

The *CCPL* divides the criminal process into five stages: opening the case, the investigation, the charge, the trial, and the implementation of judgments.[1230] In contrast to the German system, in which the prosecution is responsible for the criminal investigation, in China the police are responsible for most of the criminal cases, while supervision committees investigate the crimes committed by civil servants and other persons working for public agencies as well as other duty-related crimes.[1231] The law grants the police and the supervision committees full investigative power in cases over which they have jurisdiction. It is believed that such an arrangement can help to find the truth and thus fight crime more effectively because it can prevent "interference" by prosecution offices and courts, which can prolong the duration of the investigation. Their dominant position guarantees these authorities the possibility to decide on all kinds of warrants for investigative measures, for example, warrants on technological investigative measures, search warrants (people and places), seizure warrants (papers and objects), summons by force, sealing orders,

[1229] More discussion can be found at Chapter V.

[1230] *Chen*, 刑事诉讼法 (Criminal Procedure Law), 2013, 280 et seq.

[1231] Art. 11 I 2 *Supervision Law of the People's Republic of China* ("监察法") (中华人民共和国主席令第3号) Order No. 3 of the Chinese President of the 13rd Session): "It shall conduct investigations of duty-related violations and crimes such as suspected corruption, bribery, abuse of power, neglect of duty, power rent-seeking, tunneling, practice of favoritism and falsification, as well as the waste of state assets." The jurisdiction of the Supervision Committee can be found in Section 5. d), Chapter III, Part III. There are other organs with criminal investigation powers, i. e., military, prison, public security, and customs. But they are only for special cases which are not main topic here.

and "wanted" orders.[1232] The police execute their own warrants as well as those issued by the supervision committees.

The problems emanating from this arrangement are obvious. The lack of judicial control violates the basic principle of the rule of law. There is a high risk of abuse of police power. Moreover, the exclusionary rule is not well established in Chinese courts. Even evidence collected through abuse of power, such as by searching a residence without proper cause, is rarely excluded from trials if it is deemed important to the case.[1233] Hence, there is no effective way to punish or deter the police from abusing their power. Some arrangements even encourage the police to collect evidence by any means possible. For example, the number of cases that have been solved is an important criterion for the promotion of policemen. To be promoted, police officers therefore tend to use any means possible to "resolve" cases, including torturing suspects and even manufacturing evidence.[1234]

b) Early Participation of Prosecutors in the Investigation

Given the current criminal justice system in China, it is impossible to quickly introduce judicial control over investigative activities. On the other hand, the risk of abuse of the investigative power is too serious to be ignored. As a compromise, the early interference of prosecution office was first raised in a meeting memo of the Supreme Court in 1987 and in a Notice issued by the General Prosecution office in 1989.[1235] Finally in 2012, the *CCPL* officially decided that the prosecution service may "participate" in investigations under certain conditions.

In accordance with Art. 256 of the *Rules of Criminal Procedure of the People's Procuratorate* ("人民检察院刑事诉讼规则"),[1236] (hereafter referred as the *Rules of Criminal Procedure*), the prosecution office may appoint a prosecutor to participate in the investigative activities in important, difficult and complicated cases. The prosecutor can give legal advice on the collection of evidence and the application of the law as well as monitor the legality of investigative activities. Art. 567 of this

[1232] The arrest order has to be approved either by a prosecutor or a judge.

[1233] See Section 10. a), Chapter V, Part III.

[1234] In Lanzhou, Jiangsu Province, a policeman put heroin in the back of a taxi and later arrested the taxi driver in order to increase the number of resolved cases. See http://news.sina.com.cn/c/2003-10-20/0827952332s.shtml, visited at 13. 09. 2019.

[1235] See *Meeting Memo for Cases on Corruption, Bribery and Smuggling in the Courts in Eight Provinces* ("八省市法院审判贪污、受贿、走私案件情况座谈会纪要") in 1987: "For some serious cases, there should be early interference." In 1989, the General Prosecution Office issued *the Notice on Fighting Serious Crimes Harshly and Quickly subject to the Law* ("最高人民检察院关于坚决依法从重从快打击严重刑事犯罪分子的通知") which requires prosecutors to participate in the investigative activities of the police in serious cases and to promote the work on the approval of arrest warrants and charging, in order to get better social effect.", https://www.thepaper.cn/newsDetail_forward_2403884, visited at 13. 12. 2020.

[1236] 高检发释字(2019)4号.

regulation provides that if the prosecutor regards the behavior of the police slightly illegal, he can orally correct the fault; if the situation is more serious, he should, after obtaining the approval of the chief prosecutor, issue a written notification to the police to correct their behavior. This arrangement aims not only at improving the quality of the evidence for the prosecution but also at supervising the conduct of the police and restraining the abuse of power.[1237]

The police can apply for the participation of a prosecutor if they are confronted with legal problems.[1238] The prosecution office can also make a request to participate in the investigation. In the latter situation, the president of the police station can deny the request if he or she thinks that the case is inappropriate for early participation.[1239] Moreover, the prosecution offices are very cautious in applying this practice. They emphasize that they should only participate – not interfere – at an appropriate time and to a proportional degree. They should only give suggestions as opposed to overruling the police officers' decisions, and should give instructions rather than investigating the crime themselves.[1240]

In the draft of the *CCPL* 2012, prosecution offices were granted the power to interfere at an early phase, but this provision was deleted in the final version of the law. The present arrangement is rather experimental, since the prosecution offices do not possess any real power and only play the role of a consultant.[1241] Therefore, the new law has not changed the dominant position of the police in the investigation.

In practice, early participation of the prosecution service is rare compared to the total number of investigated cases. When the key words "early participation of prosecutors" were entered into the legal database of pkulaw.cn, 34 judgments from 2012 to 2020 appeared, 33 cases of which were relevant (see Graph 15).[1242] In the thirteen corruption cases showed in Graph 15, the prosecutors only participated after they were asked to do so by the Party's Commission for Disciplinary Inspection.[1243]

[1237] http://www.sohu.com/a/251077349_100068302, visited at 20.03.2019.

[1238] See https://www.thepaper.cn/newsDetail_forward_2403884, visited at 13.09.2019.

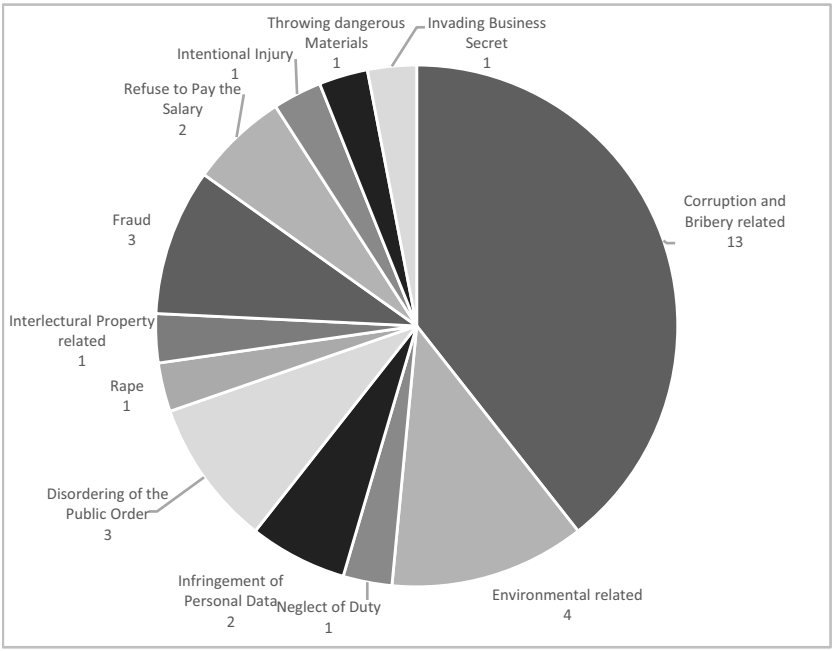
[1239] http://www.spp.gov.cn/ztk/dfld/2017dfld/dfld98_5099/ywtt/201708/t20170817_198472.shtml, visited at 20.03.2019.

[1240] http://www.spp.gov.cn/ztk/dfld/2017dfld/dfld98_5099/ywtt/201708/t20170817_198472.shtml, visited at 20.03.2019.

[1241] In a self-defense case in Laiyuan, the prosecutor suggested to the police that the case should be dropped. The police totally ignored the prosecutor's advice, kept the suspect in custody and submitted the file for charging. https://www.spp.gov.cn/spp/sp/201904/t20190402_413565.shtml, visited at 13.09.2019.

[1242] In one case among these 34 cases, the judgment recorded the testimony from a policeman who only once mentioned early participation of prosecution offices, however, no such early participation was ever considered or taken.

[1243] This department is responsible for disciplinary inspection of Party members, and it often gets the first information about corruption. In this case, the commission can investigate on its own and later pass the case on to the prosecution service. The commission and the Supervision Committee have since been merged.



Graph 15: Case Types of Early Participation of Prosecution Offices

Although this database does not collect all investigated or decided cases, such a small number among the collected cases clearly shows that early prosecutorial participation is an unpopular practice. When reading these cases in more detail, the reasons for the participation were as follows: (1) The investigation of the case attracted public attention,[1244] for instance because the investigative activities of the police caused suspicion among the public[1245] or the case met with great social interest, e. g., a corruption case[1246] or a case with a dramatic development.[1247] (2) Cases with severe circumstances or a great social impact, such as a disruption of the public

[1244] In such a situation, the police tend to ask the prosecution service for an early participation, mainly to avoid potential blame from the public.

[1245] https://www.spp.gov.cn/spp/sp/201904/t20190402_413565.shtml, visited at 13/09/2019.

[1246] Tian, (2015) Song Criminal First Instance No. 057 (田某受贿、玩忽职守案 (2015) 松刑初字第057号).

[1247] See, for example, a self-defense case in Kunshan, where a man was attacked by another man with a knife, but being a good fighter the attacked man grabbed the knife and killed the attacker. http://www.pkulaw.cn/case/pal_a3ecfd5d734f711d104211464d7ce37f0e07fcadf82d2328bdfb.html?keywords=%E6%A3%80%E5%AF%9F%E6%9C%BA%E5%85%B3%E6%8F%90%E5%89%8D%E4%BB%8B%E5%85%A5&match=Exact, visited at 14. 10. 2019.

order in a hospital[1248] or rape case.[1249] (3) The prosecutor found out about the crime first and handed the case over to the police.[1250] (4) The case was very complicated.[1251] (5) The police had difficulty with the application of the law.[1252] (5) There were special protective needs, e. g., in a case where a young girl had been raped.[1253] (6) In environmental cases were the prosecutor can file a civil or an administrative suit in the public interest alongside the criminal case; in such a case the prosecutor may wish to guide the police toward collecting evidence that will be needed for the civil or administrative proceedings.[1254] One empirical study of about 90 cases that involved early participation found that prosecutors participated often in cases of intentional homicide (10 cases) and fraud (10 cases).[1255]

Although a general tendency is observed that early participation of prosecution offices has become more frequent (see Graph 16), this practice is still numerically insignificant. A more effective way of enhancing the control over police would be for the law to reduce the investigative power of the police and to grant prosecutors and judges more influence in investigations. If the introduction of judicial control is politically unfeasible, warrants for investigative measures should at least be approved by prosecution offices, following the model of the arrest warrant.[1256] Measures in

[1248] Zhao Juntang and other seven persons, Wenfeng District Court, Anyang, Henan Province, 29.01.2015, Fabao CLI.C.6110303 (赵君堂等8人聚众扰乱社会秩序案，河南省安阳市文峰区人民法院，2015.01.29，【法宝引证码】CLI.C.6110303).

[1249] Bao, a lawyer, was suspected of raping his illegally adopted daughter. The prosecution office participated early and investigated jointly with police. At the end, no sufficient evidence was found and thus the case was dropped. CLI.C.310838608.

[1250] Li Jian, (2012), Zhungeerqi Court, Inner Mongolia Province, Fabao CLI.C.8272551 (李健侵犯著作权案，内蒙古自治区准格尔旗人民法院2012.11.19【法宝引证码】CLI.C.8272551); Han XX, (2014), Huangzhong County Court, Xining, Qinghai Province, 18.11.2014, Fabao CLI.C.6004060 (韩某某非法采矿案，青海省西宁市湟中县法院，【法宝引证码】CLI.C.6004060).

[1251] Lu, (2016) Lu 0982 Criminal First Instance No. 573 (鲁某等侵犯公民个人信息案，(2016) 鲁0982刑初573号).

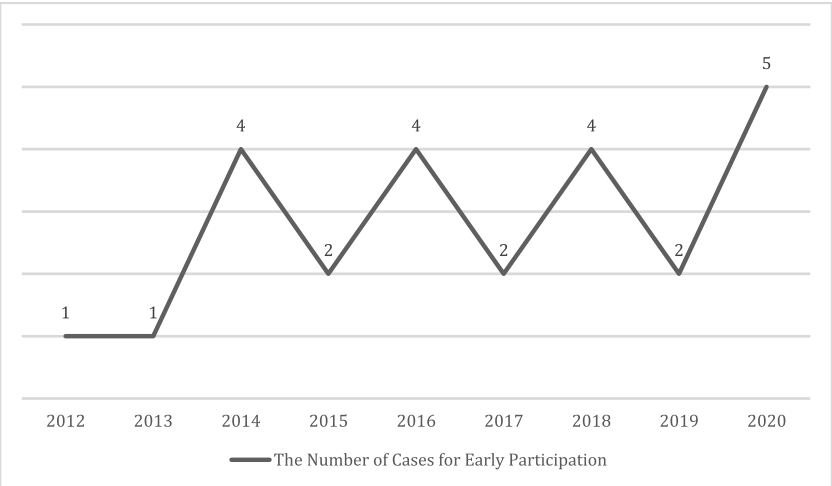
[1252] Wu Guang, (2013), Shanghai Pudong New District Court, Fabao CLI.C. 11517169(吴广侵犯商业秘密案，上海市浦东新区人民法院，【法宝引证码】CLI.C.11517169); Zhang and Yao, Huangpu District Court, Shanghai, Fabao CLI.C9036632 (张某某、姚某某侵犯公民个人信息案，上海黄浦区人民法院，【法宝引证码】CLI.C.9036632) (This was the very first case in that jurisdiction where a hacker stole personal data).

[1253] He, Fabao CLI.C. 8333561 (贺某强奸案，【法宝引证码】CLI.C.8333561).

[1254] Li, Jinghu Disctrict Court, Wuhu, Anhui Province, Fabao CLI.C. 67642852 (安徽省芜湖市镜湖区检察院诉李某等人跨省倾倒固体废物刑事附带民事公益诉讼案，【法宝引证码】CLI.C.67642852).

[1255] Other cases were: Infringement of personal data (8); environmental cases (7); intellectual property cases (6); neglect of duty (6); serious accidents with liability (5).

[1256] Although the practical control effect of the arrest warrant issued by the prosecutors is also in doubt, it still prevents the police from detaining a suspect as long as they want.



Graph 16: Number of Cases of Early Participation between 2012 and 2020

cases investigated by the prosecution offices and supervision committees should be approved by the courts.[1257]

c) The "Inspection" Power of Supervision Committees

aa) Supervision Committees

A constitutional amendment that went into effect in 2018 inserted a new Section 7 into the *Constitution*, creating supervision committees as a new national institution under the leadership of the National Supervision Committee.[1258] These committees are especially designed for the fight against corruption. The National Supervision Committee is neither an administrative nor a judicial institution;[1259] it is responsible directly to the National People's Congress and its Standing Committee. The position of the Committee is on an equal level with the central government, higher than the Supreme Court and the General Prosecution Office. Art. 125 of the *Constitution* has thus created a "fourth power" beside the existing legislative, administrative and judicial powers.[1260] Section 4 of the *Supervision Law*, which went into effect in 2018, provides details of the competence of the supervision committees. It grants the committees an "inspection power" ("调查权") together with other competences

[1257] *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 73. Compared with the Section 1, Chapter IV, Part III.

[1258] Art. 10 of the *Chinese Supervision Law.*

[1259] *Zuo/Tang*, 现代法学 (Modern Law) 4 (2018), 18, 20.

[1260] *Zuo/An*, 武汉大学学报 (哲学社会科学) (Review of Wuhan University·Philosophy and Social Science Edition) 1, (2018), 100, 101.

against duty-related illegal activities and crimes.[1261] This arrangement has been harshly criticized on the grounds that the new committees blur the boundary between the authority of the State and of the Party.[1262]

The newly established committees share personnel and premises with the Party's Commission for Disciplinary Inspection. The latter is an internal party organisation, which in principle should not have any judicial power. The *Supervision Law* thus expands the competency of the Party's Commission for Disciplinary Inspection and has transformed it from an internal institution of the Party to a semi-judicial organization. Now the supervision committees can inspect not only disciplinary issues but also criminal cases. For disciplinary infractions, the committees will impose disciplinary sanctions, such as education measures, removal from a position, recording of the misconduct in personal files, or expulsion from the party; for criminal offenses, it can collect incriminating evidence and hand it over to the prosecution office after inspection.[1263] Through this arrangement, the supervision committees are entrusted with a far-reaching power that combines the party's disciplinary authority, the power to impose administrative sanctions (such as to remove a person from his government position), and judicial power. This violates the principle of separation between the party and public authorities.

bb) The "Inspection" Power

Art. 18 of the *Supervision Law* uses the term "inspection" ("调查") in distinction from the term "investigation" ("侦查") used by the *CCPL*. The *Supervision Law* has redefined some investigative activities as "inspection activities".[1264] Regardless of the different terminologies employed, however, many measures that the supervision committees can take have almost the same characteristics as measures taken by the police in criminal investigations. Arts. 20–30 of the *Supervision Law* provide for such similar investigative measures. According to Arts. 20 and 21, the committees can interrogate the inspectee and interview witnesses. Art. 22 provides that the committees can detain a person at a specific place under certain circumstances. Arts. 23–30 provide for the power to freeze bank accounts, to search the home and the body of the inspectee when he is under suspicion of a crime in violation of a duty; to collect, seal and seize evidence; to hire experts; to order technological "inspection"

[1261] Jurisdiction is regulated in Section 5.d), Chapter III, Part III.

[1262] In order to "calm down" the criticism, public discussions on the 2018 amendments to the Constitution are currently forbidden in China. Any book drafts and journal articles on the Constitution are strictly reviewed before the publication. Some published books are not allowed to be sold anymore. For example, one textbook of Prof. ZHANG Qianfan on constitutional law, Introduction of Constitution Theories – Principles and Application) (3rd Ed.) published in 2014, academic conferences on the constitutional law, has been forbidden.

[1263] Art. 45 of the *Supervision Law*.

[1264] *Cheng*, 国家检察官学院学报 (Review of the National College of Prosecutors) 26 (2018), 125, 126.

measures; to issue "wanted person" orders; and to prohibit the person under inspection and related persons from leaving the territory. Art. 19 provides for a special inspection measure, namely to "have a talk" or require a person to give an explanation. The evidence collected from such measures can later be used before the court in a criminal process.

Under the current arrangement, two models of criminal procedure in fact exist side by side.[1265] The interpretation given by the National Supervision Committee declares that an inspection is not an investigation, hence the committees are only bound by the *Supervision Law*, not by the *CCPL*.[1266] This makes it quite clear that the committees are exempt from the procedural control of investigative activities provided by the *CCPL*.[1267] For example, Art. 34 of the *CCPL* entitles the suspect to the assistance of a lawyer from the day when he is interrogated by a criminal investigative authority for the first time or from the day when a compulsory measure is taken. The *Supervision Law* remains silent on this issue, and according to common practice the "inspectee" cannot get access to a lawyer until he is charged. Another example regards detention. The *CCPL* allows for no more than 24 hours of detention (48 hours in special cases), before the police need to request an arrest warrant from the prosecutor. Art. 43 of the *Supervision Law* allows the committees to impose three months of detention and they can prolong it for another three months.[1268]

In contrast to the view of the National Supervision Committee, the legislature's use of different terminology cannot exempt them from the scope of the *CCPL*.[1269] If it were otherwise, the investigation of duty crime cases would be totally outside of the remit of the *CCPL*.[1270] Yet, the inspection measures stated above have the same compulsory and legal effect as investigative measures[1271] and should therefore not be subject to the lower standards of procedural control provided by the *Supervision Law*.

cc) Technological Measures during Inspection

Art. 28 of the *Supervision Law* provides that if a supervision committee investigates a suspected serious duty-related crime such as corruption it may conduct strict approval formalities for taking technological inspective measures and assign these measures to the relevant institution. In accordance with this article, a supervision

[1265] *Zuo/An*, 武汉大学学报 ("哲学社会科学版") (Review of Wuhan University Philosophy and Social Science Edition) 1, (2018), 100, 101.

[1266] *Chen*, 中国人民大学学报 (Review of Renmin University) 4 (2018), 10, 11.

[1267] *Ibid.*

[1268] Even for detention, the Supervision Law uses another term than the *CCPL*.

[1269] For instance, *Chen*, 中国人民大学学报 (Review of Renmin University) 4 (2018), 10, 11.

[1270] *Liu*, 法学论坛 (Legal Forum) 6, (2017), 5, 7.

[1271] *Cheng*, 国家检察官学院学报 (Review of the National College of Prosecutors) 26 (2018), 125, 128.

committee can issue a warrant for technological measures whenever necessary and can order the corresponding police station to execute the warrant.[1272] Although the term "technological inspective measure" is used, it implies that the technological measures mentioned in the *Supervision Law* mean the same as "technological investigative measures" provided for in the *CCPL.*

d) Investigations by Prosecutors as a Supplement to Supervision Committees

Before the establishment of the supervision committees, the prosecution offices were responsible for the investigation of duty-related crimes. Under the *Supervision Law*, supervision committees conduct most of the investigative work in these cases.[1273] To comply with the *Supervision Law*, Art. 19 of the 2018 Amendment of the *CCPL* limited the investigative jurisdiction of prosecution offices to duty-related crimes committed by judicial personnel.[1274] Moreover, Art. 20 of the *Organic Law of People's Procuratorates of the People's Republic of China* (2018) provides that prosecution offices conduct investigations of relevant criminal cases in accordance with the law. This means that their jurisdiction over cases needs to be granted both by the *CCPL* and the *Supervision Law.*[1275]

Art. 34 of the *Supervision Law* further provides that when judicial institutions, including prosecution offices, or any other state organization discover any evidence of duty-related crimes committed by a public official, that organization must transfer such evidence to the corresponding supervisory institution. This provision underlines the fact that prosecution offices (and other organizations) play only a supplementary role, while the supervision committees take the dominant role if the case involves both duty-related and other crimes, regardless of which is the principal activity.[1276]

[1272] More details on the procedure can be found in Chapter IV, Part III.

[1273] *Zuo/Tang*, 现代法学 (Modern Law) 4 (2018), 18, 18.

[1274] Art. 19 CCPL 2018: "…any case regarding false imprisonment, extortion of confessions by torture, illegal search or any other crime committed by a judicial officer by taking advantage of his/her functions for infringing upon a citizen's rights and for damaging judicial justice, which is found by a people's procuratorate in its judicial supervision of litigation activities, may be placed on file for investigation by the people's procuratorate. Any other case regarding a serious crime committed by a civil servant under the jurisdiction of the public security authorities by taking advantage of his/her functions, which requires direct acceptance by a people's procuratorate, may be placed on file for investigation by the people's procuratorate upon decision by a people's procuratorate at or above the provincial level."

[1275] *Guo*, 法治研究 (Research on Rule of Law) 1 (2019), 26, 29.

[1276] Art. 34 of the *Supervision Law*: "Where the people's court, people's procuratorate, public security organ, auditing organ or any other state organ discovers in work any clue to suspected corruption, bribery, neglect of duty, malfeasance in office, or any other duty-related violation or crime committed by any public official, it shall transfer such clue to the supervisory organ, and the latter shall investigate and handle it in accordance with the law. Where the person under investigation is suspected of not only any serious duty-related violation or duty-related

To avoid jurisdiction conflicts between prosecution offices and supervision committees, the General Prosecution Office issued *Rules on the Investigation by Prosecution Offices on Duty-related Crimes Committed by Judicial Personnel* ("关于人民检察院立案侦查司法工作人员相关职务犯罪案件若干问题的规定") (hereafter referred to as *Rules on Duty-related Crimes*) in Nov. 2018. Para. 3 of this document provides that if a prosecution office, in the course of its investigation of certain offenses,[1277] finds evidence of crimes which are under the jurisdiction of the supervision committee, the prosecution office must pass this information on to the committee. In principle, it must let the committee take the leading role, with the prosecution office assisting in the investigation. If after communication between the prosecution office and the committee it is determined that it is advisable for the committee to take over the investigation, the prosecution office must retreat from the case.

According to Art. 150 2nd item of the *CCPL*, prosecution offices can take TIMs only in the investigation of crimes that imply a serious infringement on the personal rights of citizens by abusing official functions.[1278] In light of Art. 19 CCPL, however, a TIM can only be ordered in duty-related cases involving judicial personnel. Moreover, Para. 1 of the *Rules on Duty-related Crimes* provides that prosecution offices "may" investigate judicial personnel only according to the nine provisions in the *CCL*.[1279] In fact, after the *Supervision Law* came into effect, some prosecutors thought that they could no longer order such measures at all.[1280] The question of whether Para. 1 contradicts the *CCPL* has not attracted any attention, since the second category provided for in Art. 19 of the *CCPL* is of little relevance in practice. Moreover, since Para. 1 of the *Rules on Duty-related Crimes* provides a specific list and has been issued by the General Prosecution Office, it can be expected that prosecutors will just follow this list.

---

crime but also any other violation or crime, the supervisory organ shall take the lead in conducting investigation, and other organs shall provide assistance."

[1277] It refers to 14 types of crimes committed by the judicial personnel provided in Para. 1. More details can be found in Fn. 1279.

[1278] Art. 150 2nd item *CCPL:* "With regard to a case involving a major crime of serious infringement upon the personal rights of citizens by abusing functions, after placing the case on file, the people's procuratorate may, as needed for investigation of the crime and upon going through stringent approval procedures, employ technological investigative measures, which shall be carried out by the relevant authorities in accordance with applicable regulations."

[1279] Art. 238 (illegal detention); Art. 245 (illegal search); Art. 247 (torture during the interrogation and force the suspect to confess; and to collect the evidence violently); Art. 248 (torture the detainee); Art. 397 (abuse and negligence of the duty); Art. 299 I (bending the law for personal benefits; abuse the law in the civil or administrative proceedings; abuse or negligence of the duty in the execution of a judgement or rulings); Art. 400 (release the prisoner privately; let the prison escape because of the negligence); Art. 401 (offering commutation, parole, or out-of-prison enforcement because of favoritism and malpractice). The prosecutor can only investigate these crimes when they have been committed by judicial personnel.

[1280] In an interview, Mr. Song (a prosecutor) said that prosecutors are waiting for further explanation regarding technical measures from the General Prosecution Office.

3. The Covert Nature of TIMs

TIMs in China date from wartime. Radio signals of enemies were intercepted during World War II and the Civil War. In the 1950s and 1960s, TIMs were mainly used by national security agencies to detect spies from Taiwan or other countries. At that time, the vast majority of crimes were committed without the use of technology, since the population rarely had access to technical devices. In the last few decades, telecommunication technology has become highly developed and has penetrated almost every corner of daily life and business as well as the world of crime. Given this situation, the police now use TIMs more frequently than security agencies.

In 1989, to fight duty-related crimes more effectively, the Supreme Prosecution Office and the Public Security Ministry jointly issued a *Notice for the Public Security to Assist the Prosecution Offices in the Use of Technical Investigation Measures in Serious Economic Cases* ("关于公安机关协助人民检察院对重大经济案件使用技侦手段有关问题的通知"). This document stated for the first time that TIMs can be used to investigate cases. In 1993, Art. 10 of the *National Security Law* also provided for "technological investigation" in national security cases.[1281] Then Art. 16 of the *Police Law 1995* provided that the police can use TIMs in criminal investigations. In 2000, the Public Security Department issued an internal *Regulation on the Work of Technological Investigative Measures* ("公安部关于技术侦察工作的规定"), emphasizing that the information obtained from such measures can neither be directly used as evidence nor be presented in court. Such information can only be used as a clue for further investigative activities. The information needs to be transformed into forms of evidence recognized by law through the investigative measures provided in the *CCPL*. Only this evidence can be used in court.[1282]

One reason for this rule was that the former version of the *CCPL* before 2012 was silent on the issue of TIMs, and forms of evidence recognized by the *CCPL* did not include information gathered by TIMs. This shows that both the legislature and the police believed that such measures needed to be kept secret. The negative effects of that practice are obvious. The first is that this power can be abused and that the individual has no chance to obtain a remedy when his or her rights have been violated. In addition, the legality of such measures was often challenged since it was not recognized as an investigative measure by the *CCPL*.[1283] Moreover, the need for a broader use of TIMs increased as offenders relied more and more on modern

[1281] Art. 10 of *the National Security Law* 1993: Where the reconnaissance of an act endangering State security requires, a State security organ may, in accordance with the relevant provisions of the State and after going through strict approval procedures, employ technological means of reconnaissance.

[1282] *Zhu*, 国家检察官学院学报 (Review of the National College of Prosecutors) 1 (2004), 111, 116.

[1283] Report: 专家谈刑诉法修改:应避免技术侦查滥用侵犯人权 (Experts Discuss the Modification of Criminal Procedure Law: to Avoid TIMs from Infringing upon Human Rights), 人民日报 (China Daily), 12. 10. 2011.

technology. The absolute confidentiality of communications, however, prevented the efficient use of TIMs. If information from a TIM could not lead to other substantive evidence, the judge was precluded from taking the information from TIMs into account and was thus unable to convict the defendant[1284] or could only convict the defendant of a less serious crime.[1285] Therefore the police felt that their hands were tied and they were not satisfied with the covert nature of TIMs.

TIMs were first introduced into the *CCPL* in 2012, which provided that information obtained through TIMs may be used as evidence. A new section regarding TIMs, containing eight articles, was added to the Chapter entitled "Investigative measures", which detailed procedures for interrogation, interviewing witnesses, examining crime scenes, search and seizure, forensic identification and evaluation and notifications regarding wanted persons.

The new section introduced a stricter procedural control for TIMs than for the other investigative measures. For example, TIMs are limited to certain types of serious crime and must be executed in strict compliance with a warrant. The CCPL, however, does not provide further information about the procedure to be followed nor does it define the permissible types of TIMs. Many details of such measures are not disclosed and are still treated as a "national secret". As a result, the new section of the *CCPL* has only a "declaratory" function.[1286] Shortly after the enactment of the *CCPL* in 2012, the Ministry of Public Security issued a ministerial regulation, *Procedures for Criminal Cases* (2012 Version), with more procedural details.[1287] As reported by an interviewee,[1288] however, another internal handbook exists for the police to instruct officers on the operational aspects of TIMs. The content of this handbooks is strictly confidential and not accessible to the public.[1289] It could be argued that this is a violation of the principle of publicity of the law.[1290]

[1284] This is especially the case in the area of cyber crime. Opinion of Mr. Wang, a policeman.

[1285] *Zhang* et al., 新控辩审三人谈 (New Discussions among Three-the Prosecutor, Defense Lawyer and the Judge), 2014, 391.

[1286] Report: 专家谈刑诉法修改:应避免技术侦查滥用侵犯人权 (Experts Discuss the Modification of Criminal Procedure Law: to Avoid TIMs from Infringing upon Human Rights), 人民日报 (China Daily), 12. 10. 2011.

[1287] It is modified in July 2020.

[1288] A policeman, Mr. W.

[1289] Interview with Mr. Wang. In a book, it is reported that the police mainly follow an internal regulation called *Public Security Instructions on the Criminal Investigation. Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 63. The text of this regulation has not been published.

[1290] The covert nature of the TIMs is also demonstrated by the fact that I was told that I had to invalidate the Internet link to the questionnaire Model A after I made it publicly visible for three hours. The reason for this is that the police are forbidden to answer any questions about TIMs online and I am also not allowed to ask such questions online.

The fact that the police can use TIMs is a "public secret" today.[1291] Still, the police keep this issue strictly confidential and regard all information on TIMs as a "national secret", even though these measures have been included in the *CCPL* for several years. The lack of information prevents scholars from doing in-depth research[1292] and leads to general suspicion about the frequency with which such measures are used. Without official information, people tend to believe online news or rumors, for instance, that the police conduct wide-ranging surveillance of the internet and can read anyone's online communications without any restrictions. Regardless of whether such rumors are true, they prove that people are anxious and feel that their privacy is threatened. Over the long term, this may damage the credibility of public institutions.

4. Concept and Types of TIMs

Section 8 of the *CCPL* does not shed much light on the issue on TIMs, since it does not even offer a definition of the term "technological investigative measures".[1293] The legislature had originally defined this term in the first draft of the *CCPL* in 2012 and made two proposals: one was to define them as "measures that use technological methods, such as telecommunication surveillance, covertly taking photos of a residence, wiretapping and video recording, or interception of the internet information, etc., for obtaining criminal evidence." The other proposal defined TIMs as "measures that influence the right of telecommunication, the right of residence or the right to privacy of citizens through technological methods, such as telecommunication surveillance, covertly taking photos of a residence, wiretapping and video recording, or interception of internet information, etc."[1294] Given the continuous development of technology and the difficulties of giving a clear definition, however, the legislature was worried that such a definition might be too narrow. Moreover, it was quite controversial as to whether some new technological measures, such as locating an IP address, should be included in the definition.[1295] Therefore, the legislature gave up the attempt to define this core term in the *CCPL*.

The lack of a definition of TIMs in the *CCPL* has been criticized. Some argue that despite the difficulties mentioned above, no definition can be more harmful than an

[1291] Interview with policeman, Mr. Wang.

[1292] The covert nature of TIMs is also demonstrated by the fact that I was told that I had to invalidate the Internet link to the questionnaire Model A after I made it publicly visible for three hours. I learned that the police are forbidden to answer any questions about TIMs online, and I also was not allowed to ask such questions online.

[1293] See also Section 3, Chapter III, Part III.

[1294] *Chen*, 2012 刑事诉讼法修改条文理解与适用 (Interpretation and Application of the Modified Provisions in the Criminal Procedure Law 2012), 2012, 216–217.

[1295] *Li*, 秘密侦查法律问题研究 (Research on Legal Problems of Covert Investigations), 2016, 140.

imperfect definition.[1296] The lack of a legal definition also gives the police discretionary power to interpret the term "technological investigative measures". The police might also be confused about what they are allowed to do. As a supplement, Art. 264 of the *Procedures for Criminal Cases* 2020 provides that TIMs refer to the surveillance of records, of the traces of a person, of telecommunication and of places. Apparently, it lists only the categories of TIMs instead of the individual measures. Therefore, it is still not clear what measures fall within the term "technological investigative measures".

It seems that the police exercise a great deal of freedom when it comes to deciding what constitutes a TIM. According to my interview with a policeman, Mr. Wang, however, the police use TIMs as a specific legal term which refers to only eight types of measures rather than to any measure involving technologies. Not each of these eight measures requires the police to use technologies, such as obtaining a list of calls from a telecommunication company. The interviewee did not list all eight measures but mentioned checking mails (which also now includes checking logistic information), surveillance of premises and of telecommunications, surveillance of emails, surveillance of online communications, use of undercover agents with mini cameras,[1297] obtaining a list of phone calls, and using video recordings from public and private cameras. Mr. Wang divided TIMs into inquiries and surveillance measures. The former includes the collection of the call lists and the use of video recordings from public and private cameras; the latter refers, e. g., to the surveillance of telecommunication. Another interviewee also referred to tracing of suspects and counter-reconnaissance, such as interrupting telecommunication signals within a certain region.[1298]

Some scholars interpret the term "technological investigative measures" more broadly than the police. They claim that all measures that are executed covertly with the help of technology should be regarded as TIMs, such as DNA tests and IR thermographs.[1299] Given the fact that individuals enjoy a higher protection from TIMs than from other measures,[1300] to introduce a broader definition of TIMs serves to better protect individual rights. When a measure is not included in TIMs, it is subject to lesser procedural control.

From the perspective of the police, the term "technological investigative measures" is clearly comprehensible, but from the perspective of scholars it is imprecise and confusing. These contrasting perspectives on the term ultimately derive from a

[1296] *Id.* at 141.

[1297] He said this is to a large degree replaced by the records from public and private cameras.

[1298] The interview was conducted anonymously. The interviewee is a policeman working in a TIM department at a police station at the city level.

[1299] *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 3. These are expressly excluded from TIMs by the police according to Mr. W.

[1300] The TIMs have even a stricter procedural control than the search of a residence.

lack of interaction between the law in practice and academia, which is caused by the police obligation of confidentiality.

The term "technological investigative measures" is too vague to be operational and cannot instruct practice.[1301] This term should be explained and further clarified. An exact list of the measures should be provided in the *CCPL*.[1302] In addition, following each measure, the scope and conditions of application should be defined,[1303] as does the law in Germany and the United States. The advantage of such a structure is that the legislature can provide different conditions for different measures according to their intrusiveness.

Besides the lack of a definition of TIMs, another problem is that Section 8 of the *CCPL* confuses the concepts of TIMs and "covert investigative measures".[1304] For example, Art. 153 of the *CCPL* provides for the investigation by undercover agents. This is not a technological measure because it is not necessary for the undercover agent to adopt TIMs. The reason for this legislative arrangement might be that TIMs are often used by undercover agents.[1305] In fact, both belong to the category of "covert investigative measures".[1306]

5. Crime Catalogues of TIMs

a) Crime Catalogues under Art. 150 of the CCPL

Art. 150 of the *CCPL* provides certain crime categories for the application of TIMs:

> "After opening a case regarding a crime of endangering the national security, a crime of terrorist activities, an organized crime of a gangland nature, a significant drug crime, or any other crime seriously endangering society, a public security authority may, as is needed for criminal investigation, take technological investigative measures after undergoing a strict approval process."

[1301] *Chen*, 理性审视技术侦查立法 (A Rational Review of the Legislation of Technological Investigations), 法治日报 (Legal Daily), 21.09.2011.

[1302] *Ibid.*

[1303] *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 3.

[1304] *Chen*, 理性审视技术侦查立法 (A Rational Review of the Legislation of Technological Investigations), 法治日报 (Legal Daily), 21.09.2011.

[1305] Another reason might be historical. Mr. Wang said that in the past, the undercovered agents were specially trained to use mini-cameras and other technological measures. Now these measures are mainly replaced by the video cameras on the streets.

[1306] *Chen*, 理性审视技术侦查立法 (A Rational Review of the Legislation of Technological Investigations), 法治日报 (Legal Daily), 21.9.2011. See also *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 3.

It is obvious that this list is much shorter than the ones in U.S. or German law. Instead of referring to individual criminal norms, Art. 150 of the *CCPL* provides four crime categories of the *CCL* as examples, coupled with an unspecific reference to "any other crime seriously endangering society". In principle, any crime from the *CCL* could be included in this category.

"A crime of endangering national security" refers to all crimes in Chapter I of the special part of the *CCL*, covering twelve articles (from Art. 102 until Art. 113 CCL) with fourteen crimes. "A crime of terrorist activities" refers to seven articles with seven crimes under Chapter II in the Specific Part of the *CCL* as "a crime endangering public security", such as the organization, leadership or participation of terrorist groups, assistance to terrorist groups, preparation for terrorist activities, etc. Other crimes under Chapter II of the *CCL* may also be investigated with TIMs according to the questionnaire.[1307] "An organized crime of a gangland nature" refers to Art. 294 of the *CCL*, consisting of 3 crimes: organization, leadership and participation of an organization with a gangland nature, recruitment of new members for such an organization within the territory of the PRC by overseas organizations, concealment and connivance of a criminal organization of a gangland nature. "A significant drug crime" refers to all crimes in Section 7 ("Crimes of Smuggling, Trafficking, Transporting and Manufacturing Drugs") of Chapter VI ("Crimes of Disrupting the Social Order") in the special part of the *CCL*.

Art. 150 I of the *CCPL* does not limit these four categories to "serious crimes", however, the expression "any other crime seriously endangering society" should be interpreted as implying that a crime within one of these four categories should amount to the level of "seriously endangering society".

b) Art. 263 of the Procedures for Criminal Cases 2020

"Any other crime" in Art. 150 of the *CCPL* allows for the public security ministry to compile its own list of offenses. Therefore Art. 263 of the *Procedures for Criminal Cases* 2020 offers a longer list and shows what can be considered as "other crimes". It provides that crimes seriously endangering society contained in the following list can be investigated with TIMs: (1) crimes of endangering national security, terrorist activities, organized crimes of a gangland nature, significant drug crimes; (2) intentional homicide, intentional assault causing serious injury or death, rape, robbery, kidnapping, arson, explosion, poisoning with a dangerous substance, and other seriously violent crimes; (3) organized, serial and interregional serious crimes; (4) serious crimes committed via telecommunication, internet and mail, as well as serious crimes that target computer and internet systems; (5) other crimes seriously

[1307] See Question 5 Model A and Question 4 Model B in the Appendix.

endangering society which can be punished by more than seven years of imprisonment.[1308]

It is not clear whether the requirement that the crime carries a sentence of seven years of imprisonment or more is also meant to apply to the first four categories above. If the seven-year limit applied only to the fifth category, the police would be able to exercise a great deal of discretion when deciding which cases could be included within the first four categories.[1309] In order to make the rules more precise, this seven-year imprisonment requirement should be understood to apply to all categories.

c) The Use of TIMs for the Purpose of Arresting Suspects

Art. 150 III of the *CCPL* provides that the necessary TIMs for arrest may be taken for tracing a wanted person.[1310] Art. 263 II of the *Procedures for Criminal Cases* 2020 provides for exactly the same measures. Art. 228 of the *Rules of Criminal Procedure* provides that using TIMs to trace suspects is not bound by the crime catalogues. The crime catalogue is the result of a balancing of interests. Only if the suspected crime is serious enough can it justify the adoption of TIMs. Not applying the crime catalogue to arrest means that the purpose of arresting a suspect is accorded an overweighing value in comparison with any other rights. For instance, the right to the privacy of correspondence is infringed upon if a suspect is traced by the interception of telecommunication signals. Theoretically, even a person merely suspected of a theft can be traced by TIMs.[1311] This demonstrates a determined attitude of the Chinese legislature towards the safeguard of the legal order. Anyone who violates the law must not escape the punishment he deserves by fleeing. This is obviously disproportional. There is no legal basis for the absolute priority being given to the interest of arresting a suspect. Therefore, TIMs for the purpose of arrest should only be allowed in the investigation of crimes listed in the catalogue of Art. 150 I of the *CCPL*.

Even when TIMs for tracing a suspect are limited to catalogue crimes, however, this limitation could be bypassed by using other measures with more developed technology which are not defined as TIMs, such as surveillance cameras in public places. The installation of such cameras needs to be approved but their use need not because they run around the clock and mainly serve to maintain social security. If

[1308] The feedback regarding the types of cases where TIMS are used can be found in Question 5 Model A in the Appendix, and which crimes are more often investigated by TIMs will be showed in Question 6 Model A in the Appendix.

[1309] *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 30.

[1310] Art. 150 III *CCPL:* "To capture a wanted criminal suspect or defendant or a fugitive criminal suspect or defendant whose arrest has been approved or decided, technological investigative measures necessary for capture may be taken with approval."

[1311] Although this might not happen in practice when the police think it is not worth the time spent on TIMs.

necessary, the police could use a "camera network" combined with "face recognition" technology to identify wanted persons. Everyone captured by cameras could be compared with the database of facial and body features and other information of wanted persons; or a person's face can be searched in all such video records.[1312] This is more efficient than TIMs for tracing individuals and does not need "troublesome" approval procedures like TIMs. When there are no procedural controls over more developed technological practices, any controls on TIMs with similar functions are meaningless.

d) Crime Catalogue under the Supervision Law and the Rules on the Jurisdiction of the Supervision Committee (Trial)

Art. 28 of the *Supervision Law* provides that TIMs can be utilized in duty-related crimes such as serious corruption. The law thus excludes non-criminal activities and limits such measures to crimes such as serious corruption and bribery. This should be interpreted as meaning that the measures can only be considered in serious cases regardless of the types of duty-related crimes.

In accordance with Art. 11 of the *Supervision Law*, supervision committees can inspect seven categories of duty-related crimes and other non-criminal but illegal duty activities, i. e. suspected corruption and bribery, abuse of power, neglect of duty, illegal transaction of public power, illegal transfer of benefits, practice of favoritism and falsification, and wasting state assets.[1313] Four of these categories (corruption and bribery, abuse of power, neglect of duty, and practice of favoritism and falsification) are defined as crimes in the *CCL*.[1314] In order to specify which crimes can be inspected by supervision committees, the National Supervision Committee issued *Rules on the Jurisdiction of the Supervision Committees* ("国家监察委员会管辖规定") (Trial)[1315] in April 2018. These Rules list six categories which include 88 duty-

[1312] This technique might not be operated all year round, but definitely for busy seasons, such as in train stations during the spring festival. There are news reports every year on how many wanted persons are caught in train stations by such a technique. News report: https://www.sohu.com/a/213129184_100017896, visited 23. 3. 2019. A "face recognition system" technique is widely used in China, not only by police. For example, companies and universities use it to check attendance. The efficiency of this system is restricted due to the lack of a network of camera records among different regions. The local police have access only to the camera records in their jurisdiction. The process for obtaining camera records from other jurisdictions can be extremely cumbersome.

[1313] Art. 11 No. 2: "A supervisory commission shall, in accordance with the provisions of this Law and relevant laws, perform the duties of supervision, investigation and disposition: …(2) It shall conduct inspection of duty-related violations and crimes such as suspected corruption, bribery, abuse of power, neglect of duty, illegal transaction of public power, illegal transfer of benefits, practice of favoritism and falsification, as well as the waste of state assets."

[1314] *Yao/Yi*, 上海政法学院学报 (Review of Shanghai College of Political Science and Law) 6 (2018), 23, 25.

[1315] 国监发 (2018) 1号.

related crimes: (1) corruption and bribery (17 crimes); (2) abuse of power (15 crimes); (3) neglect of duty (11 crimes); (4) practice of favoritism and falsification (15 crimes); (5) serious liability accidents (11 crimes); (6) other duty-related crimes (19 crimes). This covers almost all duty-related crimes in the *CCL.* All these crimes can be inspected with TIMs, whenever a crime is deemed serious and the supervision committee believes that such measures "are needed".

6. Degree of Suspicion

Section 8 of the *CCPL* does not require any special degree of suspicion but follows the general standard for investigating a crime. Art. 109 of the *CCPL* provides this standard for initiating a case: "A public security authority or a prosecutor who discovers any facts of a crime or a criminal suspect shall initiate a case for criminal investigation according to their jurisdiction." The first sentence of Art. 115 of the *CCPL* provides that: "After initiating a criminal case, a public security authority shall conduct a criminal investigation and gather and require submission of evidence to prove the guilt or innocence of a criminal suspect or the pettiness or gravity of a crime." This shows that once a case is initiated, the police automatically start an investigation and decide which investigative measures are suitable for the case. Art. 115 of the *CCPL* does not demand any specific level of suspicion for starting an investigation and indeed for implementing TIMs.

7. "For the Needs of the Investigation" and "as Needed"

Art. 150 of the *CCPL* provides that police may use TIMs for the needs of the criminal investigation of certain crimes. One author who has participated in drafting the *CCPL* (2012) has given his interpretation of the phrase "for the needs of the investigation" in Art. 150 of the *CCPL:* it does not mean that TIMs can be used in all cases, but such measures can only be taken if conventional investigative measures have failed to achieve a successful outcome of the investigation.[1316]

The expression "as needed" in Art. 28 of the *Supervision Law* has more or less the same meaning as "for the needs". The National Supervision Committee has published its interpretation of the phrase "as needed" on its official website, stating that the supervision committees have the right to take TIMs, however, they cannot take TIMs in every case but only if such measures are deemed necessary after careful consideration. TIMs can thus only be taken if conventional measures cannot achieve a successful outcome of the investigation.[1317]

[1316] *Lang* (ed.), (中华人民共和国刑事诉讼法) 修改与适用 (Modification and Application of Chinese Criminal Procedure Law), 2012, 277.

[1317] http://www.ccdi.gov.cn/toutiao/201808/t20180806_177261.html, visited at 26. 07. 2019.

These two interpretations show that TIMs should only be regarded as a last resort. This restriction, however, cannot be found in the relevant legal texts.[1318] Both expressions "for the needs of the investigation" and "as needed" are rather misleading. They seem to indicate that the police or the supervision committees can take TIMs whenever they need, regardless of the existence of other alternatives. According to the wording of the statute, it is up to the police and the supervision committees to decide what is the most effective way to investigate a case. Since TIMs can only be executed by TIM departments,[1319] however, applying for a TIM might delay the arrival of the desired information to the responsible investigator. Therefore, the investigator or the inspector might prefer to take alternative measures to ensure a faster result whenever possible.

Another problem concerns Art. 151 of the *CCPL*, whose first sentence provides: "A decision on approval of the types of technological investigative measures to be adopted and the parties to which such measures apply shall be made based on the needs of the criminal investigation." This provision makes it clear that the type of measure and the targeted persons should be subject to "the needs of the criminal investigation." It is not clear, however, whether telecommunication can be recorded only for "the needs of the criminal investigation" or whether the police can record any conversation of the targeted persons around-the-clock once a warrant has been issued. For instance, if the police know that the wife of the suspect is not involved in the crime, can they still record the conversations of the couple? None of the legal texts or the two interpretations mentioned above[1320] answer this question. Moreover, the information included in a warrant is quite limited and does not describe what kind of conversation can be intercepted.[1321] A further explanation or detailed standards should be issued to interpret the meaning of the phrase "directly related to criminal activities". An arbitrary surveillance, a "fishing expedition", should be forbidden and certainly any evidence collected during an arbitrary surveillance should be excluded.[1322]

8. Targeted Persons

The second sentence of Art. 255 of the *CCPL* provides: "The targets of technological investigative measures are suspects, defendants and persons directly related to criminal activities." This provision shows that TIMs can be taken even after charging since defendants are named as possible targets. Secondly, the statute affords the police discretion to select targets other than suspects and defendants, for example,

[1318] See *Sun*, 环球法律评论 (Global Law Review) 4 (2013), 33, 35.

[1319] More information on the TIM Department can be found in Section 1, Chapter IV, Part III.

[1320] Fn. 1316 and Fn. 1317 and accompanying text.

[1321] *Wang*, 知与行 (Knowledge and Practice) 19 (2017), 67, 67.

[1322] See Section 2, Chapter IV, Part III.

relatives of the suspects or defendants. Even witnesses or victims can be defined as being "directly related to criminal activities". According to one interviewee, some police forces permitted and even recommended placing witnesses and victims under surveillance as an effective investigation method. This practice has now been forbidden. However, if the police believe that a witness has something to do with the suspect or with criminal activities, this witness may quickly become a suspect and his/her conversations can be intercepted.[1323]

Communications between suspects and their lawyers are not expressly excluded from surveillance. Art. 33 of the *Law of Lawyers* provides: "… A meeting between a defense lawyer and a criminal suspect or defendant shall not be intercepted." The word "meeting" here refers only to a situation where a lawyer meets a client in custody.[1324] A general client-lawyer privilege is not recognized in China. Art. 33 of the *Law of Lawyers* provides only a partial right. Defense lawyers normally join a case only after a suspect has been arrested. At that time, TIMs have normally already been terminated and the investigation is approaching completion. If the suspect calls his lawyer before he has been arrested, the communication is regarded as a normal communication and enjoys no special protection. In addition, if the police learn that the lawyer is aiding the suspect, for instance, by concealing evidence, the lawyer is likely to become a suspect himself.[1325] The fact that there is no protection of lawyers' communications with their clients sometimes makes it difficult for lawyers to obtain their clients' trust.[1326]

This topic has not caused much debate.[1327] The right to a defense lawyer is now widely recognized, but it is still a sensitive topic and its reach is quite controversial. Since scholars and lawyers are still fighting for lawyers' basic rights, such as free access to the client and free access to the case file, many lawyers have no expectation that their telecommunications are free from surveillance. This is not a singular

[1323] Addressed by Mr. W, a policeman.

[1324] Even in such a meeting, the communication between the lawyer and the client can be overheard and be used as evidence against the lawyer. According to a case report, defense lawyer, Mr. Xiong, met his client in police custody and a policeman overheard the communication. Based on the testimony of the defendant and of the policeman, Mr. Xiong was accused of "fabrication of evidence". There was no tape recording. The testimony was admitted into evidence. https://chinadigitaltimes.net/chinese/2019/09/%E6%96%AF%E4%BC%9F%E6%B1%9F%EF%BC%9A%E8%A2%AB%E7%AA%83%E5%90%AC%E5%85%A5%E7%BD%AA%E7%9A%84%E5%8D%97%E6%98%8C%E7%86%8A%E6%98%95%E5%BE%8B%E5%B8%88/, visited at 21.09.2019.

[1325] Interview with Mr. W, a policeman.

[1326] Interview with Ms. Li, a lawyer.

[1327] The keywords "technological investigative measures" and "interception of lawyers" were fed into one of the biggest databases of journals http://www.cnki.net/, visited in 26.3.2019. No results appeared. Some scholars claim that surveillance of the communications between the suspects and his lawyers and family members should be forbidden unless there is sufficient evidence to prove that the communications are crime-related. *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 71–72.

problem but is closely related to the general status of lawyers in the justice system. As long as a lawyer-client privilege is not generally recognized, it is too early to argue for the protection of the privacy of telecommunications between lawyers and their clients.[1328]

9. Privacy Clause

The first sentence of Art. 152 II of the *CCPL* provides: "Investigators shall keep confidential any state secret, trade secret, or personal privacy they have come to know in the course of taking technological investigative measures." Art. 270 I of the *Procedures for Criminal Cases* 2020 and Art. 18 of the *Supervision Law* also contain this provision. Art. 270 II of the *Procedures for Criminal Cases* 2020 further provide that individual and legal persons have an obligation to cooperate with the police in regard to TIMs and that they must keep all related matters confidential. Art. 230 of the *Rules of Criminal Procedure* provides that protective measures should be taken to avoid disclosing the identity of persons or the way in which the measures were taken, if using evidence from TIMs could endanger the safety of certain persons, involve a national secret, an investigative secret, a trade secret, or personal privacy. If necessary, a prosecutor can ask for the evidence not to be discussed in court and can ask judges to confirm evidence *in camera.*[1329] In addition to restating Art. 152 II of the *CCPL*, Art. 231 of the *Rules of Criminal Procedure* provides that if materials obtained from TIMs are irrelevant to the case, they should promptly be deleted and the deletion should be recorded. Evidence, clues, and other materials can be used only for the criminal investigation, prosecution, and trial; their use for other purposes is forbidden. It has been argued that judges are obliged to maintain the confidentiality of national secrets, investigative secrets, trade secrets and personal privacy, although the legal texts refer only to the police and prosecutors. This argument is based on the fact that judges can in principle get access to secrets and private information by reading the files and conducting the trial.[1330]

The law does not explain what is meant by "personal privacy", and there exists no common understanding of that term. Before any concept of privacy could be firmly established in Chinese society, the wide-spread use of e-payments (such as Alipay and WeChat) and face recognition systems (for payment or boarding a train, etc.) in daily life has greatly reduced the scope of privacy. In China, where people disclose a great deal of private information during daily life, this may give the police the wrong impression that such information is no longer private.

[1328] Question 4 Model A in the Appendix.

[1329] More discussion about the *in-camera* confirmation can be found in Section 3, Chapter V, Part III.

[1330] *Wang*, 知与行 (Knowledge and Practice) 19 (2017), 67, 67.

When the keywords "technological investigative measures" and "privacy" are entered into the database of judgements,[1331] no results appear. This shows that, until now, no cases have addressed the issue of whether a TIM infringes on privacy. This is quite understandable. As stated above, the need to find the truth is given total priority in the Chinese criminal justice system. Therefore, if a piece of information is useful for the investigation, the police are unlikely to treat it as private. If, on the other hand, the information is not needed, the police will not include it in the file.

The process of conducting TIMs requires a high level of confidentiality, hence normally all information collected through such measures, including private information, is highly protected. According to the internal police rules, only the chief of the police station at the city level and the policemen who carry out the measures get access to the information collected from such measures. Even the investigator responsible for the case and who applied for the TIM cannot always get the original information but may receive only a report from the TIM department.[1332] Although the main purpose of such a strict rule is to preserve "national secrets" rather than individual privacy, in practice there is a very low risk that private information may be leaked. The protection of private information is only a byproduct of this rule but is nevertheless a positive consequence. This is one of the reasons why the concept of TIMs should be understood broadly.[1333] Private information collected by other measures has a much higher likelihood of being leaked.[1334]

IV. Procedural Requirements

1. The Approval Procedure of Police, the Supervision Committees and the Prosecution Offices

The approval procedure for TIMs is not a judicial one but is subject to an administrative process. The highest-ranking officer of each institution authorized to conduct TIMs must approve the application.[1335] Although it is an internal process, it can be quite cumbersome, especially for police in the countryside. Their applications need to be signed four times before the measure is carried out by the special de-

[1331] http://wenshu.court.gov.cn/Index, visited on 23. 3. 2019.

[1332] Question 21 Model A in the Appendix.

[1333] See Section 4, Chapter III, Part III.

[1334] For example, in China, many policemen carry mini cameras on their bodies when on duty to record any confrontation. In a case, a policeman saw a car parking beside the road at night with someone inside. He approached the car and saw two lovers having sex inside the car. This scene was recorded by his camera. Later he spread this piece of video among his colleagues and somehow it went online. The woman in that video committed suicide because of it. https://www.sohu.com/a/358456685_351144, visited at 10. 04. 2021.

[1335] Interview with Mr. W, a policeman.

partment responsible for the execution of TIMs (the TIM department).[1336] If internal rules were violated, the measure can be regarded as illegal.[1337] These rules are not described in Section 8 of the *CCPL* but are contained in regulations or internal handbooks. Under the rule of law, the procedure should be established by legislation and made public.[1338]

a) Police

As stated above, three institutions may approve TIMs in cases in which they have jurisdiction. Approval procedures, however, are slightly different with each institution.

Section 8 of the *CCPL* regulates neither application nor approval procedures for TIMs. Art. 264 I of the *Procedures for Criminal Cases* 2020 states that the city-level police must have a special department responsible for the execution of TIMs (TIM department). Art. 265 provides that if TIMs are considered necessary, documents on the application should be prepared and submitted to the director of the city-level police. Yet it does not provide who has the authority to submit an application. According to Question 7 Model A of the Questionnaire (see Appendix), both the investigator directly in charge of the case and the section chief of the police department that investigates the case may do so. If the director of the city-level police approves the application, he or she will issue the warrant. One interviewee added the information that the application is first submitted to the chief of the TIM department to check whether the current technology can realize the desired outcome. Only thereafter does the application go to the director of the city-level police for his approval.[1339]

Since the investigator needs to rely on the TIM department to carry out the measures,[1340] he or she submits all case-related information, such as the background, how far the case has been investigated, what information is expected, information on the targets, their circle and their location. Since the investigator must give many details to the TIM department, it can be expected that the approving director will also be quite well informed about the case.

[1336] *Chen*, 理性审视技术侦查立法 (A Rational Review of the Legislation of Technological Investigations), 法治日报 (Legal Daily), 21/9/2011.

[1337] Question 10 Model B in the Appendix.

[1338] See also Section 3, Chapter III, Part III.

[1339] An anonymous policeman (hereafter Mr. X) who works at the TIM Department at a city-level police station.

[1340] It can also happen that the investigators collect the evidence directly during their search activity. For instance, to output the online chatting and payment history from the suspect's computer during the search. Li and others, (2017) Jin Criminal Final No. 21 (李某林等人犯贩卖毒品罪，山西省高级人民法院刑事裁定书 (2017) 晋刑终21号).

One interviewee criticized this arrangement for its low efficiency.[1341] He complained that investigators do not get sufficient support from TIM departments. The investigative department cannot give orders to the TIM department, since they are on the same administrative level. Therefore, measures may be delayed and important information may be missed if personnel in TIM departments do not understand what the investigators are looking for. The policeman suggested that TIM departments should be reorganized to only assist investigators and carry out their orders.

Another interviewee reported that applications are rarely denied.[1342] All persons who answered Model A said that there were applications denied[1343] but estimated that percentages varied between 0–20 % and 40–60 %.[1344] Although due to the low number of completed questionnaires the responses are not representative, they at least indicate that some applications are denied.

As to what elements or criteria play a role in the approval or denial, the questionnaire offered 6 choices: monetary costs, labor costs, time consuming, the legality of the applied measures, whether the measure can get the desirable results, other elements. All the first five options were selected. No one filled in "other elements".[1345]

b) Prosecution Offices

Art. 150 II of the *CCPL* grants prosecution offices approval power, but they need to rely mainly on TIM departments of the police for implementation, because prosecutors do not have the necessary technical devices. The first sentence of Art. 229 I of the *Rules of Criminal Procedure* provides that according to the needs of the investigation, prosecution offices can decide on the types and targets of TIMs. Art. 265 II of the *Procedures for Criminal Cases* 2020 provides: "If the prosecution offices decide to take technological investigative measures, the city level or above police station allocates this task to the TIM department. The results must be handed over to the prosecution offices." One interviewee confirmed this procedure and said that the general prosecutor of a city approves the application from the districts of a city or from his own investigation department. Then the prosecutor will send this warrant to the police station at the city level or above for implementation.[1346] Another interviewee reported, however, that the prosecutor at the city level needs to present the application to the TIM Department to check the operability and that the police president of the city level can reject the warrant.[1347] The two interviewees came from

[1341] Interview with Mr. W.
[1342] Interview with Policeman, Mr. X.
[1343] Question11 Model A in the Appendix.
[1344] Question 12 Model A in the Appendix.
[1345] Question 10 Model A in the Appendix.
[1346] Interview with Mr. Song.
[1347] Interview with Mr. X.

different regions and might therefore follow different rules. The former system seems more logical. The prosecution offices should supervise the behavior of the police, not the other way round.

Interestingly, some prosecutors complained that the process of approving TIMs is too complicated and that due to delays the prosecutors often fail to make the most of these investigative opportunities.[1348] Even police investigators complained that they do not get sufficient support from their colleagues in the TIM departments; "out-of-house" warrants from prosecution offices may confront even more bureaucracy.

After the Supervision Committee System was established in 2018, it was no longer clear whether the prosecution offices can still make decisions regarding TIMs.[1349] Art. 150 II of the *CCPL* still expressly grants the prosecution offices such authority, however, it is likely that new rules will be introduced to further clarify this situation.

c) Supervision Committees

The formulation of Art. 28 I of the *Supervision Law* is very similar to the rule for prosecution offices.[1350] Since the supervision committees took over the jurisdiction of duty-related crimes and also the corresponding personnel from the prosecution offices, it is not surprising that the committees also adopted the procedural rules and practices of the prosecution offices for a certain time.

Art. 28 of the *Supervision Law* refers only to a "strict approval process" without regulating the details, i. e., who gives the approval. Based on case reports released by local supervision committees, the inspector responsible for the case needs to fill in two forms, i. e., the application form for TIMs and the notification of the use of TIMs. Both forms require information on the targeted persons, the name of the case, the grounds for applying the measures and the duration of the measure. Both forms need the signatures of the department manager, the branch leader, and the main leader. After all signatures have been collected, three copies of the notification will be numbered and stamped, one is for storage, one is put into the file, and the third one is handed over to the police office for execution.[1351] The process can slightly differ from place to place, but they all more or less follow the model used by the prosecution offices in the past. In the context of the supervision committees, however, the inspection and the approval take place within one institution. It is common that the main leader orders an inspector to take TIMs and then the inspector initiates the

[1348] Question 22 Model B in the Appendix.

[1349] See Section 2. d), Chapter III, Part III.

[1350] See Section 2. c) cc), Chapter III, Part III.

[1351] http://www.lnsjjjc.gov.cn/yw/system/2019/06/11/030002610.shtml (Wan'an County, Jiangxi Province and Chenggong District, Kunming City, Yunnan Province) and http://www.moj.gov.cn/news/content/2018-06/20/460_36959.html (Jiamusi City, Heilongjiang Province), visited at 26. 07. 2019.

application process; or the inspector asks for the oral permission from the main leader before he submits the application form.[1352] If the main leader of a committee can decide to inspect a case and to take TIMs, the control process is weak.

After the introduction of the supervision committee system, very few changes have been observed in the process.[1353] In the long term, developments are to be expected. When prosecution offices were responsible for duty-related cases, they were cautious about taking TIMs,[1354] since their targets (some of whom were in high positions in the government hierarchy) were potentially more influential and powerful than the prosecutors. Now the supervision committees enjoy the total support of the central government and the Party. Compared to the "weak" figures in the prosecution offices, the committees are tougher and, as a consequence, employ TIMs more frequently.

[1352] http://www.moj.gov.cn/news/content/2018-06/20/460_36959.html (Jiamusi City, Heilongjiang Province), visited at 26. 07. 2019.

[1353] One difference is that the technological measures can only be approved by the city level (or above) of the prosecution offices, but the county level of the supervision committees can already decide on such measures.

[1354] Opinion of Mr. Song.

2. Contents of the Warrant

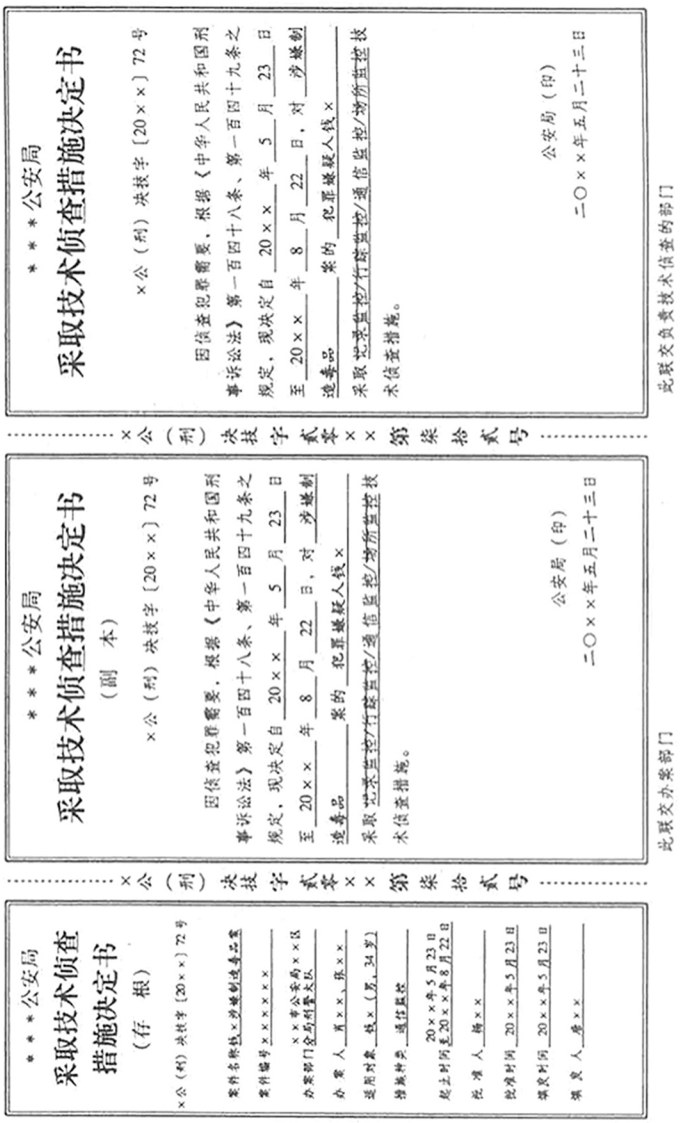


Photo 1: Warrant (Police) of the Technical Measures[1355]

[1355] *Sun*, 公安机关刑事法律文书制作指南与范例 (Instructions and Examples of Legal Documents in Criminal Issues used by Public Security), 2015, 417.

Photo 1 shows a warrant issued by the police. It consists of three parts. The far left part is to be stored in the file for later checks. The blanks detail are (from top to bottom): the name of the case (Suspect A for drug dealing crime); the case number; the name of the investigation department (such as the criminal department of XX county XX city); the names of the investigators; the targets (suspect A, male, 34-year old; or locations to be intercepted), the measure (such as telecommunication surveillance); duration (from DD/MM/YY till DD/MM/YY); the approval person (B); the date of the approval; the date of filing the document; and the person submitting the document (C).

The middle section is a duplicate of the right part and is sent to the investigation department. The investigation department will put it into the investigation file of the case. If the information obtained through this measure is used as evidence, this part is included in the charging file and handed over to the prosecution office according to Art. 154 of the *CCPL*.[1356]

The right part is given to TIM departments as a warrant. It states: "For the needs of the investigation, according to Art. 148 and Art. 149 (now Art. 150 and Art. 151) of the *CCPL*, we now decide to install telecommunication surveillance against Suspect A in a drug dealing case from DD/MM/YY to DD/MM/YY." At the very bottom is the time of issue and the stamp of the police station for approval.

3. Implementation

No matter which institution issues the warrants for TIMs, it is the TIM department that implements them. If it is an "in-house" warrant, the TIM department will implement the measures based on the warrant in Photo 1 Warrant (Police) of the Technical Measures. If the warrant comes from the prosecution office or a supervision committee, the police will issue an "execution order". Both the warrants in Photo 1 Warrant (Police) of the Technical Measures and the "execution order" can only be used once. When the targets need to be changed or another measure is needed, a new warrant needs to be issued following the same procedure as the first one.[1357]

Art. 152 of the *CCPL* provides: "Where technological investigative measures are taken, such measures must be executed in strict accordance with the approved types, scope of application and terms." Art. 267 of the *Procedures for Criminal Cases* 2020 has adopted the same provision.

The warrants play a role in determining the legality of TIMs later. According to the questionnaire, when persons not covered by the warrant are intercepted, these TIMs can be regarded as illegal.[1358]

[1356] *Id.* at 415.

[1357] *Id.* at 416 and 420.

[1358] Question 10 Model B in the Appendix.

4. Duration and Extension of TIMs

The second sentence of Art. 151 of the *CCPL* provides:

> "An approval decision shall be valid for three months from the date of issue. When technological investigative measures are no longer necessary, they shall be terminated in a timely manner; or if it is necessary to continue to take technological investigative measures in a complicated or difficult case after the term of validity expires, the term of validity may be extended with approval, but each extension must not exceed three months."[1359]

Any extension needs to be approved by the person/department that issued the original warrant.[1360] For an extension, the case must be too complicated and difficult to be solved within three months, and further TIMs must be needed. By an extension, the targets and the form of the measure cannot be changed. If they are to be changed, a new warrant is needed. An extension may not exceed three months, but a measure can be extended several times. Theoretically, TIMs can continue forever if the police think that it is necessary.[1361] According to the interview, the percentage of prolongations is not high.[1362]

It is not clear what the phrase "the case is complicated and difficult" means. All warrants have the same form with vague phraseology, such as "for the needs of the investigation" and "the case is complicated and difficult". Neither the police nor the prosecutors give reasons for the existence of investigatory needs or for the case being complicated and difficult. The substantive grounds for the warrant therefore cannot be reviewed and its legality cannot be challenged. It would be better if more information were offered. For example, the reports made by the investigation department should be attached to the warrant if investigators wish to use the materials from TIMs as evidence. Moreover, the legislation should require applicants to present sufficient evidence to support their application, for example, concerning the evidence against the person to be placed under surveillance and the expectation that surveillance will produce relevant evidence. Warrants should be issued only if the applications are based on sufficient evidence.

On the warrant form, space should be made available for information regarding the legal justification for the measures to be taken. As an alternative, applicants could be required to attach certain documents such as the application materials, the report to the TIM department, and a detailed statement of justifications.

[1359] The second sentence of Art 229 of the *Rules of Criminal Procedure* provides: "With respect to difficult and complex cases, if the technological investigative measures are still required upon expiry of the time limit, their term of validity may be extended upon approval, subject to a maximum of three months per extension."

[1360] *Sun*, 公安机关刑事法律文书制作指南与范例 (Instructions and Examples of Legal Documents in Criminal Issues used by Public Security), 2015, 422. See also Question 18 Model A in the Appendix.

[1361] *Sun*, 环球法律评论 (Global Law Review) 4 (2013), 33.

[1362] Question 17 Model A in the Appendix.

5. Termination of the Measure

In addition to the requirement of termination in Art. 151 of the *CCPL*, Art. 266 II of the *Procedures for Criminal Cases* 2020 provides more procedural details:

> "If within the term of validity it is no longer necessary to continue the technological investigative measures, the investigation department should immediately inform the TIM department in writing to terminate the measure. If the TIM department thinks it is necessary to terminate the measure, it should apply to the application approver to terminate the measure, who can then promptly inform the investigation department."

Possible grounds for a termination of TIMs include a finding that the situation has changed or that the measure is no longer appropriate.[1363] In order to terminate measures promptly when they are no longer needed, the TIM department and the investigation department should be in regular communication. The TIM Department should also inform investigators immediately when the situation has changed or the desired information has been collected.

6. Obligation to Delete Information

Art. 152 II of the *CCPL* includes a privacy clause[1364] and imposes an obligation to delete information obtained via TIMs that is irrelevant to the case. Such information must be destroyed in a timely manner. This shows that the deletion of irrelevant information primarily serves to protect privacy. In the *Procedures for Criminal Cases* 2020, the obligation to delete and a privacy clause have been provided separately. Art. 269 II prescribes: "Irrelevant information collected by technological investigative measures should be deleted in a timely manner and the deletion should be recorded."[1365] Art. 231 I of the *Rules of Criminal Procedure* provides the same. The legal texts, however, neither provide a clear period for the deletion, nor do they name the person responsible. In the interview questionnaires, these options were proposed: (1) The TIM department deletes irrelevant information immediately after collection; (2) the investigator decides when to delete information; (3) all information is deleted after the case has been decided; (4) information is deleted after a fixed period; and (5) the chief officer decides when to delete information. Three of the interviewees chose No. 3, the other four options were chosen by one or two interviewees each.[1366]

[1363] *Sun*, 公安机关刑事法律文书制作指南与范例 (Instructions and Examples of Legal Documents in Criminal Issues used by Public Security), 2015, 425.

[1364] The discussion about the private clause can be found in Section 9, Chapter III, Part III.

[1365] Art. 261 I of *The Rules of Criminal Procedure* is about the privacy clause. See Section 9, Chapter III, Part III.

[1366] Question 20 Model A in the Appendix.

V. Admissibility of Information from TIMs

The negative effect of excessive confidence in TIMs as evidence has already been discussed in Section 3 of Chapter III in this Part. In the course of the judicial reforms between 2008 and 2012, the Central Political and Law Committee issued an opinion stating that in order to legally combat serious crime, the procedures and the scope of TIMs and covert measures as well as the legal status of evidence from TIMs should be clarified.[1367] In 2010, in order to improve the quality of death penalty cases, the Supreme Court and the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security and the Ministry of Justice jointly issued *Provisions on Several Issues Concerning the Examination and Judgment of Evidence in Death Penalty Cases* ("关于办理死刑案件审查判断证据若干问题的规定") (hereafter referred to as *Provisions of Evidence in Death Penalty Cases*).[1368] Article 35, as a forerunner of Art. 152 of the *CCPL* in 2012 (now Art. 154 of the *CCPL* 2018), provides:

> "Physical evidence, documentary evidence or any other evidence obtained by an investigative institution through special investigative measures under the relevant provisions may be used as a basis for deciding a case if it has been verified by the court. The court is prohibited by law to disclose the execution process and the method of the special investigative measures."[1369]

Here the term "special investigative measures" includes TIMs, and "any other evidence" includes information from TIMs, such as recording tapes. This was the first time that information from TIMs was recognized as evidence in the criminal justice system.[1370] In many cases, especially in drug cases, the death penalty cannot be supported without materials collected from TIMs.[1371] The breakthrough for the legal recognition of TIMs, therefore, occurred due to death penalty cases. The legislative history demonstrates that the idea of recognizing materials from TIMs as evidence was originally designed to combat crime more effectively and to make capital punishment easier to obtain. Nevertheless, the development was a positive one.

[1367] Opinions on Several Issues on the Further Reform on Judicial System and Mechanism ("关于深化司法体制和工作机制改革若干问题的意见"), 2008. This opinion was prompted by the Supreme Court. More details on the historical background can be found in *Zhang* et al., 新控辩审三人谈 (New Discussions among Three-the Prosecutor, Defense Lawyer and the Judge), 2014, 391.

[1368] 法发 (2010) 20号.

[1369] The *Provisions of Evidence in Death Penalty Cases* in 2010 went beyond the provisions of the *CCPL* at that time.

[1370] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153.

[1371] *Zhang* et al., 新控辩审三人谈 (New Discussions among Three-the Prosecutor, Defense Lawyer and the Judge), 2014, 395.

1. Art. 154 of the *CCPL* 2018: New Legislation Concerning Evidence Gathered via TIMs

Art. 154 of the *CCPL* provides:

> "Information collected by means of technological investigative measures under this Section (Section 8) may be used as evidence in the criminal process. If the use of such evidence may endanger the personal safety of relevant persons or may cause other serious consequences, protective measures shall be taken, for example, non-disclosure of the identity of relevant persons or of relevant technical methods. If necessary, evidence may be verified by judges outside the courtroom."

The phrase "may be", instead of "should be", grants investigators discretion to decide whether to use such information as evidence. According to an empirical study, information from TIMs was used as evidence in 73 among 1433 cases (5 %) in which TIMs were taken. In other cases, information was used as a mere clue for identifying a suspect, justifying further investigation, or locating suspects.[1372] In only 72 cases, results of telecommunication surveillance were used (including for locating the suspect).[1373] In my police questionnaires, one respondent said they would hand over information from TIMs to prosecutors, another said that they would not, the third said that "it depends".[1374] In the questionnaire for judges and prosecutors, seven respondents said that there are on average one or two out of every ten cases where the information appears in the files as evidence. One respondent chose four to six out of every ten cases, and another chose eight to ten out of every ten cases.[1375] This shows that after 2012, information from TIMs have been submitted as evidence, but with a relatively low frequency.

The second sentence of Art. 154 of the *CCPL* is normally used by the police as grounds for not submitting such information, claiming that doing so would "endanger the personal safety of relevant persons or may cause other serious consequences". This vague expression does not effectively restrict the discretion of the police since they are not required to explain why the situation "endangers the personal safety" or what serious consequences could occur. The police only need to give a general declaration on the warrant form.[1376] The legality of TIMs is also taken into consideration when the police decide whether to hand over the information from the measures.[1377] If the police are not sure whether the TIMs were legal or if the measures could be challenged in court, they tend not to include the information in the files as evidence.

[1372] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 156.

[1373] *Ibid.*

[1374] Question 13 Model A in the Appendix.

[1375] Question 7 Model B in the Appendix.

[1376] See Section 2, Chapter IV, Part III.

[1377] Question 15 Model A in the Appendix.

In fact, the second sentence of Art. 154 of the *CCPL* applies only to "evidence". Information becomes "evidence" only when it is included in the file and submitted to the prosecutors. This clause cannot turn the "original information" into "evidence". The law should provide that the information from TIMs should in principle be included in the file as evidence and that its exclusion should be exceptional. Since the second sentence already offers protection measures in special cases, the words "can be" in the first sentence should be changed to "should be".

2. The Interpretation of "Other Serious Consequences"

According to the responses of prosecutors and judges, they accept the following situations as "other serious consequences": (1) the measure is needed for further investigation in related cases. For example, Suspect A is charged but the investigation against his partner B continues. Once B knows that A was intercepted, he will be very careful, and it will be more difficult for the police to intercept B; (2) the safety of relatives of the related persons; (3) a national secret could be leaked; (4) the identity of the undercover agent could be disclosed, such as in a drug dealing organization.[1378] The drafters of the *CCPL* held the same opinion.[1379]

The dilemma here is how to interpret the phrase "national secret". If TIMs are *per se* defined as "national secrets", none of the information gathered by such measures could be presented in court. Yet, the confidentiality of TIMs should be interpreted in a limited way, especially when the investigation has been closed. TIMs should not generally be regarded as a "national secret", and an arbitrary use of "national secret" as an excuse to decline disclosure of TIMs must be avoided. Whether TIMs and information therefrom should be disclosed should be decided in individual cases by courts, not by police or prosecutors. To realize this goal, courts should receive the complete files regarding TIMs and then decide whether and to what degree to disclose information to the defense. This could also improve the transparency of TIMs.

3. Three Forms of Evidence

Another problem is the question in what form the information is to be submitted to the courts. The evidence from TIMs can be submitted in three forms. According to the empirical study mentioned above, in 29 out of 73 cases only the transcripts of the intercepted communications were submitted; a report was filed in 25 cases; and the

[1378] Question16 Model B in the Appendix.

[1379] *Lang* (ed.), 〈中华人民共和国刑事诉讼法〉修改与适用 (Modification and Application of Chinese Criminal Procedure Law), 2012, 284.

original tape recording was submitted in 7 cases.[1380] The results of my questionnaire answered by the prosecutors and judges show a similar tendency. One interviewee said that he used to receive the original information from the TIMs, such as tape recordings. Three interviewees said that they received only transcripts or reports. Five interviewees said that they saw only the final evidence, without any information about the TIMs.[1381]

The original information is more reliable than the other two forms and should be submitted as evidence whenever possible. According to the above empirical study, however, this is in fact exceptional. Due to the fact that surveillance reports can be easily manipulated, their reliability is often challenged by the defense if no other evidence can demonstrate their reliability. Tape recordings as the original evidence should be in principle be handed over to the prosecutors and judges. The defense should also have the right to challenge the original evidence. Reports should be used as rarely as possible, and this option should be abolished as soon as the police have gotten used to handing over the original information.[1382]

4. Examination of the Reliability of TIM Evidence *in Camera:* A Challenge to the Defense Right

Art. 154 of the *CCPL* offers three ways of confirming the reliability of surveillance evidence at trial. The first one is the regular method, by presenting the evidence in court and giving the defense an opportunity to challenge it. The second way is to present the evidence at the trial but to take certain protective measures, such as to blur the sound or image. The third method is to verify the evidence *in camera* by the judge "if necessary".[1383] Art. 63 of the 2012 version of the *Explanation of the Application of the CCPL*[1384] provides that in principle all evidence must be presented in court, "unless the legislation and the judicial explanation provide otherwise." This phrase "provide otherwise" is regarded as a reference to the examination *in camera* as provided by Art. 154 of the *CCPL*.[1385] Due to the so-called "confidential" nature of

[1380] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 157. A report is written by the TIM department or the investigator to summarize or describe the useful information of the intercepted telecommunication.

[1381] Question 6 Model B in the Appendix.

[1382] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 169.

[1383] *Dong*, 四川大学学报 (哲学社会科学版) (Review of Sichuan University·Philosophy and Social Science) 3 (2012), 151, 152; *Gao/Xing*, 警察法学 (Law of Police), 2017, 340–341.

[1384] 法释 (2012) 21号.

[1385] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 155–156; *Zhang* et al., 新控辩审三人谈 (New Discussions among Three - the Prosecutor, Defense Lawyer and the Judge), 2014, 391.

TIMs, examination *in camera*, done in an arbitrary way,[1386] became a widespread practice.

Art. 36 II of the *Provisions on Court Inquiry during the First Instance of the Criminal Cases* provides that if judges decide to examine TIM evidence *in camera*, he or she may ask the prosecutor and the defense lawyer to be present.[1387] The persons present have to sign a commitment to confidentiality and comply with it. In theory, judges can order the police to show the original materials to the defense lawyer, however, this happens very seldom.[1388] If police refuse to show the evidence, the prosecutor or the police only need to explain in court why presenting evidence is not feasible and how they obtained the evidence which could lead to disclosure of the identities of affected persons.

In the opinion of a former Supreme Court judge, after examination *in camera*, the judge only needs to declare in court that he is convinced of the reliability of the evidence.[1389] This view, however, makes defense work extremely difficult. Defense lawyers argue that judicial examination *in camera* cannot be a substitute for the presentation of the evidence in court, where it can be examined. If the presentation of the evidence in court can endanger the safety of persons and is refused by the prosecutor, the evidence should not be admitted at all.[1390] Defense lawyers see a conflict here between procedural rights and the criminal policy interest in fighting crime.[1391]

The lack of rules on how to do examination *in camera*, such as on the initiation of such an examination or on the persons present, leads to further arbitrariness. An empirical study of drug-related cases found that currently defense lawyers, prosecutors as well as the police can request an *in camera* review and that in the latter case the examination takes place at the police station. The judge may also initiate an examination on his own initiative or decline a suggestion by the defense lawyer or the police.[1392]

Until recently, if the police insisted that presenting the evidence in court would be dangerous, the judge had no other choice but to go to the police station to examine the

---

[1386] *Li*, 法治论坛 (Nomocracy Forum) 50 (2018), 105, 106.

[1387] *Opinions of the Supreme Court on Comprehensively Promoting the Reform of the Trial-Centered Criminal Procedure System* ("最高法关于全面推进以审判为中心的刑事诉讼制度改革的实施意见", 法发 (2017) 5号) (hereafter referred to as the *Notice on the Promotion of the Reform*), para. 13.

[1388] In fact, when the police refuse to cooperate, not even the judge can examine the evidence.

[1389] *Zhang* et al., 新控辩审三人谈 (New Discussions among Three-the Prosecutor, Defense Lawyer and the Judge), 2014, 393.

[1390] *Id.* at 392–393.

[1391] *Id.* at 400.

[1392] *Li*, 法治论坛 (Nomocracy Forum) 50 (2018), 105, 115. See also Art. 230 II of the *Explanation of the Application of the CCPL* (2021).

evidence *in camera*, namely, to listen to the original tapes or to watch the videos and take notes, which were later placed in the file.[1393] Sometimes the police even declined to show the original tape or video to the judge; in that situation, the judge was restricted to listening to oral reports given by the police.[1394]

This state of the law may change significantly due to the new *Explanation of the Application of the CCPL* (2021), which provides more procedural details on the submission and admissibility of evidence from TIMs and has deleted the expression "unless the legislation and the judicial explanation provide otherwise." This change emphasizes the importance of presentation of evidence at trial at a general level; however, its later provisions still allow examination *in camera* for TIM evidence.

According to Art. 36 of the *Provisions on Court Inquiry during the First Instance of the Criminal Cases* (Trial Version) ("人民法院办理刑事案件第一审普通程序法庭调查规程 (试行)")[1395] and Art. 120 of the *Explanation of the Application of the CCPL* (2021), whenever TIM evidence is to be admitted, the presentation of such evidence in court should be the principle and examination *in camera* the exception if necessary. This can also be concluded from Art. 152 of the *CCPL*. In order to guarantee judges a better access to TIM evidence, Art. 116 of the *Explanation of the Application of the CCPL* (2021) provides that such evidence should be submitted to the court along with the file in order to be used as evidence. Moreover, the first sentence of Art. 122 of this Explanation provides that judges can order prosecutors to submit TIM evidence to them if prosecutors have not done so. As long as judges have evidence in their hands, even if they cannot present it at trial, they can at least review the evidence *in camera* whenever they want.[1396] In order to further "deter" the prosecutors and eventually the police, the second sentence of Art. 122 of this Explanation provides that if the evidence is not submitted after judges have so ordered, judges should decide on the facts based on the evidence already in the files. This could make police think twice whether they would take the risk that TIM evidence not submitted is not considered by judges.

With this new *Explanation of the Application of the CCPL* (2021), the Supreme Court shows its determination to improve the quality of the courts' work in reviewing TIM evidence. Since this Explanation went into effect only on 01.03.2021, more time is needed to observe to what degree such a rule will influence actual practice and whether the police will respect it. In any case, the intention of the police to conceal the details of TIMs in order to maintain its discretionary power or to conveniently cover up illegal conduct will not change in a short time. Moreover, Art. 268 of the *Pro-*

[1393] *Li*, 法治论坛 (Nomocracy Forum) 50 (2018), 105, 115; *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 168, Fn. 68.

[1394] *Li*, 法治论坛 (Nomocracy Forum) 50 (2018), 105, 115.

[1395] 法发(2017) 31号.

[1396] Wu and others, (2015) Nantie Middle Criminal Final No. 3 (吴绍团、吴木同贩卖运输毒品、吴某某非法持有毒品案,(2015) 南铁中刑终字第3号). In this case, the judge wished to examine the evidence *in camera*, but the police and the prosecutor refused to cooperate.

cedures for Criminal Cases 2020 still only require the surveillance warrant, not the evidence itself, to be placed in the prosecutor's file, if information from TIMs is to be used as evidence.[1397] Since this regulation is issued by the Ministry of Public Security, it can be reasonably assumed that police would prefer to follow this regulation instead of the new rules in the *Explanation of the Application of the CCPL* (2021).

5. Defense Strategy

Currently, if TIM evidence is presented in court, it is often in the form of transcripts and reports; in that case the effect of any examination is reduced.[1398] For instance, if only a transcript is presented the defense lawyer cannot determine whether the voice that had been recorded is his client's.[1399]

In spite of this difficulty, defense lawyers challenge the legality of TIM evidence more frequently than any other evidence. According to an empirical study, the defense challenged the legality of TIM evidence in more than 70 % of the cases in which such evidence was presented.[1400] An empirical study on drug cases, however, shows that defense lawyers challenged TIM evidence only in 12.7 % of the cases. This ratio is lower than that of challenges of testimonial evidence.[1401] According to yet another empirical study, motions for excluding any evidence were made in only 5 % of all cases.[1402] Comparing the results from different empirical studies, we can see that TIM evidence is challenged more frequently than any other form of evidence.

Some legal challenges concern alleged violations of Art. 150 of the *CCPL* regarding procedural requirements such as the approval process, the crime catalogue, or the qualification of the person executing the warrant. Most frequently, lawyers argued that transcripts and reports are not the legal form of evidence and asked for the original tapes.[1403] Other lawyers challenged the admissibility of evidence only examined *in camera.*[1404] The relevance of the evidence is also often challenged,[1405] especially in drug or organized crime cases where suspects often use code words in their communications.[1406]

[1397] The same for the cases investigated by prosecutors with TIMs, according to Art. 229 II of the *Explanation of the Application of the CCPL* (2021).

[1398] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 158.

[1399] *Li*, 法治论坛 (Forum of Rule of Law) 50 (2018), 105, 111.

[1400] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 158.

[1401] See *Li*, 法治论坛 (Forum of Rule of Law) 50 (2018), 105, 113 – 114 and Fn. 6.

[1402] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151.

[1403] In the empirical study on drug cases, the challenges in 26 among 33 cases concerned the legality of the transcripts and the requests of the original tapes. *Li*, 法治论坛 (Forum of Rule of Law) 50 (2018), 105, table 1.

[1404] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 158.

[1405] Such as the cases referred in Fn. 1498 and Fn. 1499.

[1406] *Cheng*, 法学研究 (Legal Research) 5 (2018), 153, 158.

The convert nature of TIMs makes them vulnerable to this type of challenges. The police therefore try to avoid such "trouble" and refrain from presenting information from TIMs as direct evidence.

6. A Practical Example: Evidence from TIMs in Drug Cases

Drug cases are being used as an example here for two reasons. First, TIMs are often used in drug cases because the covert nature of this criminal activity makes it more difficult to obtain evidence in traditional ways. Second, the police have a strong interest in protecting the identity of witnesses or undercover agents in drug or organized crime cases. This fact leads to a higher number of instances of *in camera* examination of TIM evidence.[1407]

In an empirical study of TIM evidence in drug cases, 334 judgments with the keywords "drug" and "technological measures" were examined. TIMs were used more frequently in drug transaction (77.5 %) and drug transportation (28.1 %) cases than in drug production and drug possession cases. In the latter cases, it is easier to prove the offense by seizing evidence.[1408] Another finding of this study is that severe sentences, including the death penalty, are more likely to be imposed in cases where TIMs were used. Of 545 defendants, 70 % received sentences of more than ten years; 21 % were given life sentences, and 3 % received the death penalty.[1409] The study also showed that the defense is largely deprived of the possibility to challenge TIM evidence since it is not placed in the prosecution file and the defense lawyer cannot review it. In some cases, the defense lawyer was aware that a TIM was conducted but no evidence was presented in court, or the judge had inspected the evidence *in camera* without the lawyer present.[1410] Even where defense lawyers did challenge TIM evidence,[1411] these challenges were rarely successful.[1412]

In a conference on evidentiary rules in drug cases,[1413] Judge Gao Guijun of the Criminal Division of the Supreme Court described the purposes for which TIM evidence can be used in drug cases: for the determination of guilt or innocence, for uncovering which crime was committed, and for sentencing, especially regarding the death penalty. He also explained the requirements for introducing such evidence: (1) the process of gathering the evidence should be explained; (2) the meaning of code

[1407] *Li*, 法治论坛 (Forum of Rule of Law) 50 (2018), 105, 106.

[1408] *Id.* at 107.

[1409] *Ibid.*

[1410] *Ibid.*

[1411] See Section 5, Chapter V, Part III.

[1412] *Li*, 法治论坛 (Forum of Rule of Law) 50 (2018), 105, 108–111, table 1. Judges excluded challenged TIM evidence only in 2 out of 33 cases.

[1413] http://www.dz64.com/xsfalvzhishi/2296.html, visited at 25. 12. 2020.

words or dialects recorded on the tape should be explained; and (3) the identity of the speaker should be proved by voice recognition technology whenever necessary.

Judge Gao also pointed out that judges should review the evidence both formally and substantively. Formal review concerns the approval process of the warrant; whether the warrant has been carried out properly with regard to its duration and targeted persons, and whether there is an explanation attached to the evidence. As to the latter, the judges should compare TIM evidence with other evidence to ensure that they do not conflict with each other; the judges should review the voiceprint to ascertain the identity of the speaker. Art 119 of the *Explanation of the Application of the CCPL* (2021) states similar requirements.

Judge Gao confirmed that evidence can be reviewed in court and *in camera* but the former is the principle, while the latter should only be used in exceptional cases. For *in camera* review of evidence, the judge can summon the prosecutor, the investigator and the defense lawyer to be present. Judge Gao suggested that examination of evidence *in camera* should be further restricted. He reported that judges have specific guidelines for reviewing TIM evidence. The regulations contain a clear indication to the police, the supervision committees and the prosecutors as to which materials should be submitted regarding TIM evidence.

7. The General Rule on Exclusion

The exclusion of TIM evidence follows the general rules. Art. 54 of the *CCPL* 2012 (now Art. 56 of the *CCPL* 2018) officially established, for the first time, an exclusionary rule on the level of legislation. This is regarded as an achievement of the *CCPL* 2012. Art. 56 of the *CCPL* 2018 provides:

> "(1) A confession of a criminal suspect or defendant extorted by torture or obtained by other illegal means and a witness or victim statement obtained by violence, threat, or other illegal means shall be excluded. If any physical or documentary evidence is not gathered under the statutory procedure, which may seriously affect justice, correction or justification shall be provided; otherwise, such evidence shall be excluded. (2) If it is discovered during the criminal investigation, prosecution, or trial of a case that any evidence should be excluded, such evidence shall be excluded and not be used as a basis for a prosecution proposal, a prosecution decision or a judgment."

Art. 56 of the *CCPL* distinguishes between absolute and relative exclusion of evidence. "Absolute" exclusion means that evidence is to be excluded whenever the described situation occurs. Absolute exclusion is required when oral evidence has been obtained by torture or other equivalent methods. This rule is based on several reasons: (1) Such practices are serious violations of human rights and have always been harshly criticized; (2) Such practices have been prohibited and the exclusion of resulting evidence has been demanded for some time, although exclusion was not provided for in the *CCPL*; (3) The reliability of oral evidence is more deeply affected

by illegal methods of interrogation than the reliability of physical or documentary evidence, although illegal methods of obtaining such evidence may also violate important constitutional rights. This is the main reason for the mere "relative" exclusion of physical evidence, which means that illegally obtained evidence can still be admitted after certain corrections or justifications. For instance, when a house was illegally searched without a warrant and drugs were found, the drugs themselves still constitute reliable evidence. In accordance with Art. 56 of the *CCPL*, if the police can subsequently obtain a warrant, the evidence is admissible ("correction or justification").[1414] If there was only a slight violation of the rules, which "may not seriously affect justice", the police do not even need to apply for a correction.[1415]

This exclusionary rule is not complete. Normally, excluding evidence mainly serves to protect human rights and criminal justice. The difference between the rules concerning oral and physical evidence, however, shows that considerations of finding the truth and the need to fight crime play an important role. The definition of exclusionary rules is thus, to a certain degree, oriented towards truth-finding.[1416]

Art. 56 of the *CCPL* 2018 grants judges broad discretion in deciding whether to exclude evidence. Judges are in fact very hesitant to exclude evidence and rely on the defense lawyer to prove that evidence was illegally obtained. Proof can be extremely difficult with regard to oral evidence because suspects or defendants are detained and interrogated by the police without the presence of a lawyer. When the police obtain oral evidence by using illegal methods, they will be careful to avoid "getting caught".

Judges will normally not exclude physical or documentary evidence if it is important to convict the defendant, but they may ask for a correction.[1417] If the evidence plays a minor role, they will usually not expressly exclude it but will not use it in the judgment.[1418] This is a result of the principle that the finding of truth has priority.[1419]

[1414] More discussion about the correction of the evidence can be found in Section 10. c), Chapter V, Part III.

[1415] Arts. 123 – 126 of *the Explanation on the Application of the CCPL (2021)* provide similarly. Art. 123 and Art. 125 excludes confessions of suspects and testimony from witnesses or victims obtained through torture, threaten or illegal detention. Art. 126 provides a "relative" exclusion for physical or documentary evidence. A correction can be done first before the exclusion.

[1416] See Section 10. c), Chapter V, Part III.

[1417] See Section 10. c), Chapter V, Part III.

[1418] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151.

[1419] *Wang/Ma*, 中国法学教育研究 (Research on Chinese Legal Education) 3 (2013), 148, 151.

8. Exclusion of Evidence during Investigation, Prosecution or Inspection

In accordance with the second paragraph of Art. 56 of the *CCPL* and Art. 33 of the *Supervision Law*,[1420] the police, prosecutors and supervision committees may also exclude illegal evidence if a case falls within their jurisdiction. All three institutions have responsibility to review the legality of the evidence collected before the files are passed on to the next stage and must make sure that inadmissible evidence does not enter the next stage.[1421] This means that exclusion of evidence can occur at any time from the beginning of the investigation until the final judgment. Neither the police, prosecutors, nor inspectors make formal decisions on excluding evidence but handle this matter in a "soft" way.

a) Police

When the police think that certain material has been collected illegally and would not be admitted by prosecutors or judges, the police will refrain from using this evidence. Art. 56 of the *CCPL* does not provide any process for the exclusion of evidence but only provides that the police and the prosecutor shall exclude illegal evidence. If exclusion need not be recorded, the police can easily cover up their former illegal conduct by just "forgetting about" the evidence. In that situation, no one can find out or prove what happened and there are no negative consequences for the police.

b) Prosecutors

Art. 57 of the *CCPL* provides that a prosecutor, after discovering, receiving a report, accusation, or any indication that evidence has been obtained illegally shall investigate the situation. Prosecutors have two opportunities to exclude illegal evidence, one is when they decide on an arrest warrant, the other is when they decide on the charge. They should make these decisions without considering illegal evidence.[1422] Prosecutors can initiate the review of the legality of evidence on their own motion or upon an application by the defense.[1423] However, it is rare that prosecutors exclude evidence on their own initiative.[1424] Normally prosecutors require the police to "supplement the evidence"[1425] only if the defense lawyer challenges the evidence

[1420] Art. 33 III of the *Supervision Law:* "Evidence collected by illegal means shall be excluded in accordance with the law and shall not be taken as a basis to handle the cases."

[1421] *Chen/Nie*, 中国人民大学学报 (Review of Chinese Renmin University) 4 (2018), 2, 8.

[1422] *Hu*, 基于实证观察的我国非法证据排除规则研 (Empirical Research on Chinese Exclusionary Rule of Illegal Evidence), 2018, 156–159.

[1423] *Id.* at 159.

[1424] *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 187.

[1425] *Ibid.*

and offers sufficient materials to prove its illegality.[1426] In most situations, the prosecutor will just define the evidence as "defective"[1427] and request the police to make an explanation or to submit more materials in order to "repair" the defective evidence. It is common practice that the police just submit a sheet of paper as an explanation. If the illegality is serious, the prosecutor will send the case back to the police for further investigation.[1428] The prosecutor may also introduce the evidence but suggest a much lighter sentence as a compensation for the faulty evidence.[1429]

According to a report delivered in 2014 by Mr. Cao, the National General Prosecutor of the Supreme Prosecution Office, prosecutors declined to issue arrest warrants against 750 persons from January 2013 to October 2014, due to illegal evidence.[1430] In 2014, a total of 19.4 % of applications for arrest warrants were denied, but only 0.2 % of applications were denied because prosecutors identified illegally obtained evidence.[1431] In the same time period, prosecutors required the police to make corrections of the evidence against 494 defendants.[1432] This was regarded as a positive achievement for the new evidentiary rules in the *CCPL* 2012.[1433] Compared to the total number of arrestees during this period, however, the numbers of declinations or demands for correction were insignificant. In practice, prosecutors are unable to effectively supervise the conduct of the police, although this is one of the principal functions of prosecutors according to the *CCPL*.[1434]

c) Supervision Committees

Art. 33 of the *Supervision Law* provides that supervision committees shall follow the same standards for the collection of the evidence as provided for in the *CCPL* and that illegally obtained evidence shall be excluded.

As stated above, inspection activities of supervision committees resemble police investigations. Exclusion of evidence by supervision committees therefore poses similar problems.[1435] Moreover, supervision committees have multiple tasks, i. e., duty-related crimes as well as disciplinary and administrative cases.[1436] This makes

[1426] See Section 10. b), Chapter V, Part III.

[1427] See Section 10. c), Chapter V, Part III.

[1428] *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 188.

[1429] *Wu*, 现代法学 (Modern Law Science) 36 (2014), 121, 125. See also Section 11, Chapter V, Part III.

[1430] *CAO Jianming*, 关于人民检察院规范司法行为工作情况报告 (Work Report on the Standardization of Judicial Behavior of Prosecutors), 29/10/2014.

[1431] *Yuan*, 人民检察 (People's Procuratorial Semimonthly) 6 (2015), 26, 27.

[1432] *Ibid.*

[1433] *Ibid.*

[1434] *Luo*, 政法学刊 (Journal of Political Science and Law) 28 (2011), 71, 73.

[1435] See Section 8. a), Chapter V, Part III.

[1436] *Jiang*, 法学杂志 (Law Science Magazine) 3 (2017), 1, 2.

the definition of "illegal" evidence more complicated. It is not clear whether the term "illegal" in the *Supervision Law* refers only to the violation of criminal procedure law or whether it also includes the violation of administrative rules or even of Communist Party Discipline. In addition, Art. 33 of the *Supervision Law* does not distinguish between criminal cases and disciplinary or administrative cases, hence all cases dealt with by the supervision committees follow the same evidentiary standards regarding collection and review. It would be preferable, however, that standards of evidence in criminal cases were higher than in disciplinary cases.[1437] The supervision committees were established primarily to fight corruption. Given this overriding political mission, truth-finding plays an even more essential role than in normal criminal cases.

The National Supervision Committee is placed at the same hierarchical level as the Office of the Prime Minister, higher than the Supreme Court and the Supreme Prosecution Office. The overriding position of the supervision committees at each administrative level is more obvious in local governments, since the leader of the local supervision committee normally has a higher position in the Party than the presidents of the court and the prosecution office of that level.[1438] Moreover, judges and prosecutors are also "civil servants" and thus under the supervision of the supervision committees. Therefore, they all wish to have "good relations" with the supervision committees. It is therefore unlikely that the court or prosecutors will exclude evidence collected by supervision committees.[1439] The supervision committees are hence more or less autonomous regarding accepting or excluding evidence, free from external supervision.

9. Exclusion of Evidence by Judges

Compared to the investigation, inspection or prosecution phases, where the law does not provide for a particular process for the exclusion of evidence, the exclusion of evidence by judges after charging follows certain rules or patterns. This includes the pre-trial hearing and the trial. According to practice, the pre-trial hearing focuses on the legality of the evidence, while its reliability and relevance are mainly dealt with at trial.[1440]

[1437] *Liu*, 证据科学 (Evidence Science) 26 (2018), 410, 415.

[1438] *Zheng*, 证据科学 (Evidence Science) 26 (2018), 420, 424.

[1439] *Id.* at 425.

[1440] *Li*, 法治论坛 (Forum of Rule of Law) 50 (2018), 105, 112.

a) Exclusion of Evidence at the Pre-trial Hearing

Art. 182 of the *CCPL* 2012 (now Art. 187 of the *CCPL* 2018) introduced the pre-trial hearing as a part of the preparation for the trial.[1441] According to this provision, the judge has discretion to hold a hearing, either on his own initiative or on an application from one of the parties.[1442] The judge chairs the hearing, with the prosecutor and the defense lawyer present. The defendant also can be present if necessary.[1443] Exclusion of illegal evidence can be one of the topics of a pre-trial hearing.

According to an empirical study, 20 out of 28 pre-trial hearings were held due to a defense application to exclude evidence. In another city, the ratio was 19 out of 52 pre-trial hearings,[1444] and according to two further empirical studies, the percentage was 30 %[1445] and 46 %, respectively.[1446] All three empirical studies showed that a defense application for the exclusion of evidence is the most frequent grounds for calling a pre-trial hearing. Including the statistics of main trials, an empirical study of pre-trial hearings and judgments in 2013 in one province similarly shows that judges frequently initiate the examination of the legality of the evidence in response to applications from the defense. For instance, High Court judges of this province conducted investigations in 11 out of 27 applications (40.7 %).[1447] The percentages for the courts at city level and at district level are between 41.2 % and 53.4 %.[1448]

In 2016, the Supreme Court, the Supreme Procuratorate and the Ministry of Public Security delivered the *Opinions on Advancing the Reform of the Trial-Centered Criminal Procedure System* ("关于推进以审判为中心的刑事诉讼制度改革的意见") in order to advance the on-going judicial reform towards a "Trial-Centered Criminal Procedure System".[1449] Para. 10 of the *Opinions* emphasizes the need for the presentation of evidence at the pre-trial hearing. This mechanism offers the defense lawyer a chance to get to know the prosecution evidence and to apply for the ex-

[1441] *Wei*, 北大法律评论 (Beijing University Law Review) 17 (2016), 2, 3. Art. 187 of *the CCPL* 2018: "Before a court session is opened, the judges may summon the public prosecutor, the parties concerned, defenders, and agents ad litem to gather information and hear opinions on trial-related issues, such as challenges, a list of witnesses to testify in court, and exclusion of illegally obtained evidence."

[1442] Of 52 cases with pre-trial hearings, 36 were initiated by the judge on his own motion; the other 16 were held on applications of the prosecutor or the defense lawyer. *Wei*, 北大法律评论 (Beijing University Law Review) 17 (2016), 2, 5.

[1443] According to an empirical study, the defendant attended the pre-trial hearing in 11.8 % of the cases. *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 63.

[1444] *Wei*, 北大法律评论 (Beijing University Law Review) 17 (2016), 2, 5.

[1445] *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 62.

[1446] *Zuo*, 中外法学 (Beijing University Law Journal) 27 (2015), 469, 474.

[1447] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 155.

[1448] *Ibid.*

[1449] 法发 (2016) 18号。

clusion of evidence if necessary.[1450] In practice, however, the regulation on the presentation of evidence does not achieve the desired results because prosecutors sometimes do not hand over all evidence to the court at the pre-trial hearing.[1451]

In 2017, two further guidelines were issued, the *Notice on the Promotion of the Reform*[1452] and *The Notice of the Supreme People's Court*, *the Supreme People's Procuratorate*, *the Ministry of Public Security and Other Departments on Issuing the Provisions on Several Issues concerning the Strict Exclusion of Illegally Collected Evidence in the Handling of Criminal Cases* ("关于办理刑事案件严格排除非法证据若干问题的规定") (hereafter referred to as the *Notice on Illegally Collected Evidence*).[1453] Both provide more details on the organization and function of the pre-trial hearing.[1454]

The title of Chapter two of the *Notice on the Promotion of the Reform*, "to improve the preparatory work before trial and to guarantee a continuous trial process", explains the purpose of the pre-trial hearing, namely, to promote an uninterrupted trial process. This means that the pre-trial hearing mainly deals with procedural issues, including the admissibility of evidence. In a significant improvement, this *Notice* provides for the possibility of resolving evidentiary issues at the pre-trial hearing, based on agreements between the prosecutor and the defense. According to Para. 7, if the defense challenges the legality of evidence and applies for its exclusion, the judge can verify the situation and hear the opinions of the parties. The prosecutor can decide to withdraw certain evidence at the pre-trial hearing. After withdrawal, such evidence cannot be presented at the trial, unless the prosecutor can offer convincing reasons. The defense can also withdraw its application after an explanation or correction has been made by the prosecutor. Without new materials, the application cannot be made again. Para. 8 provides that the judge, after hearing the opinions of the parties, may suggest that the prosecutor further investigate the case or withdraw it. The judge should try to resolve the legality of the evidence at the pre-trial hearing, by legitimating defective evidence through corrections by the prosecutor, by the prosecution withdrawing the evidence or even the whole case, or by the defense lawyer withdrawing his challenges. The judge plays a mediating role here. The ultimate purpose of the pre-trial hearing is to ensure that the trial can focus on truth-finding without any interruption by procedural issues.

[1450] *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 61.

[1451] *Id.* at 64. According to Art. 28 of *the Regulation of the Pre-trial Meeting in Criminal Cases (Trial)* ("人民法院办理刑事案件庭前会议规程(试行)" 法发 (2017) 31号), the prosecutor shall hand over all the evidence to the court before the pre-trial hearing.

[1452] See Fn. 1387.

[1453] 法发(2017) 15号。

[1454] See also *Chen*, 丰富庭前会议功能助力法庭集中审理 (To Promote the Concentration of Trials by Enriching the Function of Pre-trial Meetings), 人民法院报 (People's Court Daily), 24.02.2017.

Art. 25 of the *Notice on Illegally Collected Evidence* requires that the judge shall (not "may") hold a pre-trial hearing if the defense submits sufficient materials and indications[1455] for an application for the exclusion of certain evidence. The prosecutor should then explain the legality of the evidence. Art. 26 states that when the parties cannot agree on the legality of the evidence at the pre-trial hearing and the judge suspects its possible illegality, the judge shall examine the evidence at the trial. If the judge is convinced that the evidence is admissible, he may decide not to conduct an examination.

The *Explanation on the Application of the CCPL* (2021) further encourages all parties to deal with exclusion issues at pre-trial hearings in order not to delay the main trial hearings. According to its Art. 132, the defense must give an explanation if the defense did not apply for the exclusion before trial but only at the trial. Art. 133 provides the same as Art. 26 of the *Notice on Illegally Collected Evidence*. This indicates that the judge may exclude the evidence at pre-trial hearings and that applications and decisions made at pre-trial hearings are valid for the trial.[1456]

From this development of the rules on the pre-trial hearing, it is clear that the legislature and the Supreme Court have made great efforts to promote the pre-trial hearing, and scholars have reacted with great applause.[1457] The arrangement of the pre-trial hearing has become very similar to a trial and thus has been called "a trial before the trial".[1458] According to an empirical study, however, among all criminal cases decided in 2016 open to the public (1,116,00 cases), there were only 309 cases (0.027 %) in which pre-trial hearings were conducted.[1459] The low percentage has been confirmed in two further empirical studies. In 2015, in a court at city level, pre-trial hearings were conducted in 18 cases (0.64 % of charged cases);[1460] at a different court at a city level and its eleven lower courts pre-trial hearings were held in 0.3 % of all cases in 2013.[1461] The extremely low percentage (0.027 %) in the first study may result from the fact that courts at the district level conduct pre-trial hearings much less frequently than higher courts.[1462] These statistics show that this system does not work

[1455] See more information on "the sufficient materials and clues" in Section 10. b), Chapter V, Part III.

[1456] *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 60.

[1457] *Zuo*, 中外法学 (Beijing University Law Journal) 27 (2015), 469, 469.

[1458] *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 61.

[1459] *Zhou* (the president of the Chinese Supreme Court), 最高人民法院工作报2017 (Work Report of the Supreme Court 2017), 2017, 23; *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 66.

[1460] *Wei*, 北大法律评论 (Beijing University Law Review) 17 (2016), 2, 4.

[1461] *Zuo*, 中外法学 (Beijing University Law Journal) 27 (2015), 469, 471.

[1462] *Ibid.* This empirical study shows that the percentage of pre-trial hearings in the courts at district level is 0.2 % and in courts at city level is 0.7 %. The reason can be that the courts at district level deal with simpler cases compared to the higher courts and that those cases do not meet the requirements for holding a pre-trial hearing.

as well as the legislature and the Supreme Court had expected. Many judges do not wish to increase their workload, when they are already overworked.[1463] In addition, some judges misunderstand the purpose and the function of the pre-trial hearing. They use it as a rehearsal of the trial and deal with substantive issues. This makes the trial lose its meaning. Sometimes the agreements made during the pre-trial hearings are ignored and the same issues are proposed again at the trial.[1464] With the enactment of the *Explanation on the Application of the CCPL* (2021), more pre-trial hearings are expected.

b) Exclusion of Evidence at Trial

As outlined above, if a pre-trial hearing is held, most issues regarding the legality of evidence are to be resolved there. This reduces the need to exclude evidence at the trial. However, if the legality of evidence cannot be decided at a pre-trial hearing, it has to be reviewed during the trial. Before the *Explanation on the Application of the CCPL* (2021), the judge reviewed it together with all other issues and then decided whether to initiate an examination on the legality of the evidence. In one case, the defense lawyer applied to exclude evidence before trial, but the judge did not initiate an examination before the trial started. At the trial, the lawyer again applied three times to exclude certain evidence (after the reading of the charging statement, before and after the examination of that piece of evidence). The judge, however, insisted on examining the admissibility of the evidence only after the substantive part of the case had been finished.[1465] Such a practice eliminates the effect of any exclusion, since the trial has already been deeply influenced by the evidence. Art. 134 of the *Explanation on the Application of the CCPL* (2021) states the principle that the legality of evidence should be reviewed at the beginning of the trial. However, there is a "but" clause: if there is a risk that the process of the trial can be extremely delayed, such review can also be done before closing the trial. This provision grants judges the authority to decide when to review the legality of evidence.

Judges can also implicitly exclude evidence. In an interview, one judge said that when there are five pieces of evidence and one of them cannot be admitted, he would only rely on the other four pieces of evidence in his judgment. He would not exclude the inadmissible evidence expressly but would not mention it in the judgment.[1466]

[1463] *Ma/Zhang*, 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59, 66.

[1464] *Ibid.*

[1465] *Du*, "河南非法证据排除第一大案"庭审纪实" (Trial Record of "Very First Case on the Exclusion of Illegal Evidence in Henan Province"), 法制日报 (Legal Daily), 14. 10. 2013.

[1466] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 152, Fn. 2.

10. Reasons for the Infrequency of the Exclusion of Evidence

Although the exclusionary rule is a heated topic in academic debate and has been actively encouraged by the Supreme Court, it is still a rare practice in local courts. For instance, an empirical study reported that in a district court 1550 cases were decided in 2013. Defense lawyers applied for exclusion in 17 cases, and judges examined the legality of the evidence in only 7 of these cases. Finally, the evidence was excluded in only one case.[1467] Therefore, the exclusionary rule is sometimes described as "dead".[1468] This actually encourages the police to collect evidence by illegal means.[1469]

Several factors explain the rare occurrence of the exclusion of evidence by judges in China.

a) Exclusion of Evidence and the Emphasis on Truth-finding

As stated above, Art. 56 of the *CCPL* provides for a relative exclusionary rule, which gives way to truth-finding as the main purpose of Chinese criminal procedure.[1470] This attitude is inherent in the applicable statutes and also influences judges. This can be seen in the arguments used by judges when they decline to exclude evidence. As well as using vague expressions, such as that "no evidence to prove that the challenged evidence is illegal" or "the challenge is not true", some judges declined to exclude evidence by arguing that the evidence is reliable.[1471] Judges wrote, for example, that, "the defendant has confessed naturally and objectively"; or "the defendant confessed again after his release from custody".[1472] These examples show that exclusion of evidence is still regarded as exceptional.[1473]

The fundamental idea of the exclusionary rule is that certain evidence should be excluded because of the illegal way in which it was obtained, regardless of its reliability. The exclusionary rule has a procedural function that must be evaluated separately from the reliability of the evidence.

Connecting exclusion and a lack of reliability of evidence is a special phenomenon in China.[1474] This is a consequence of the problematic distribution of power

---

[1467] *Id.* at 156.

[1468] *Wu*, 现代法学 (Modern Law Science) 36 (2014), 121, 121; *Wang*, 政治与法律 (Political Science and Law) 6 (2013), 142, 150–151.

[1469] *Hu*, 基于实证观察的我国非法证据排除规则研 (Empirical Research on Chinese Exclusionary Rule of Illegal Evidence), 2018, 127.

[1470] See Section 7, Chapter V and Section 1, Chapter III, Part III.

[1471] *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 182.

[1472] *Wu*, 现代法学 (Modern Law Science) 36 (2014), 121, 126; Li, (2019) Xiang 09 Criminal Final No. 128 (李某某虚开增值税发票案，(2019) 湘09刑终128号).

[1473] See Fn. 1467; *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 156.

[1474] *Wu*, 现代法学 (Modern Law Science) 36 (2014), 121, 126.

between the police, prosecutors, and the courts. The authority to exclude evidence at trial as a procedural sanction confers upon judges a *post-factum* supervisory role. Exclusion can be regarded as a negative comment on the conduct of the police and prosecutor, or even as a challenge to the well-established "police culture" as a whole.[1475] In practice, judges lack independence and the court system is too weak to supervise or challenge the police and the prosecution.[1476] It is possible that bad relations with the police or the prosecution have a negative impact on the personal interests of individual judges; they may not get promoted, lose their job, or may even be charged with "intentional abuse of the law". Furthermore, Chinese courts are organized like administrative agencies, which means that individual judges must follow orders from judges higher up in the court hierarchy.[1477] For instance, the chief of the police station can give pressure to the chief judge and in turn, the chief judge can give orders to the judge directly in charge of the case. Given such pressures from inside and outside, judges normally expressly exclude evidence only if they are absolutely sure that the evidence is not reliable.

This situation refers especially to TIMs. Tape recordings and videos are normally more reliable than confessions. As a result, TIM evidence is hardly ever excluded even if it has been obtained illegally. In that case, the judge will normally ask for a correction and then admit the tape.

b) The Heavy Burden of Proof on the Defense and the Lack of Impact of an Exclusion on Convictions

Another problem is that the defendant must prove that the evidence was obtained illegally or at least offer sufficient materials and indications. Art. 5 of the *Rules on the Exclusion of Illegal Evidence in Criminal Cases* (2018) (Trial) ("人民法院办理刑事案件排除非法证据规程(试行)")[1478] provides that "indications" may refer to illegal information, the identities of the investigator, the time and the location of the collection of the evidence, and illegal methods. "Materials" refer to photos of injuries, medical reports and files, transcripts, audio or video records of the interrogation, or the testimony of the defendant's cellmate in custody. Art. 127 of the *Explanation on the Application of the CCPL* (2021) provides the same.

Investigation and interrogation activities are normally done confidentially under the control of the police.[1479] Therefore, it is difficult for the defense lawyer to get sufficient material or indications, as mentioned above, to persuade the judge to in-

[1475] *Id.* at 128.
[1476] *Id.* at 129.
[1477] *Id.* at 128.
[1478] 法发(2017) 31号.
[1479] *Luo*, 政法学刊 (Journal of Political Science and Law) 28 (2011), 71, 72.

itiate an examination of the challenged evidence.[1480] This was confirmed by some of the judges interviewed.[1481]

There are normally two situations in which judges will consider a review of the legality of the evidence: if the defendant has obvious wounds on his body which cannot be explained;[1482] or the contents of the file show a clear procedural violation.[1483]

Even if a judge initiates an examination and orders the police or the prosecutor to present additional information, however, the examination can only be successful if these agencies cooperate. Obviously, the police and prosecutors have no desire to assist the judge or the defense lawyer in proving the illegality of their own conduct. Judges therefore are often unable to determine whether the challenged evidence was obtained illegally. As a result, judges have no choice but to accept the explanation of police or prosecutors.[1484]

Given such difficulties, defense lawyers sometimes just give up. They know that their challenges will probably lead nowhere. They will either not be supported by the judge, or it will make no difference even if the evidence is excluded, as in the case that a confession is later repeated.[1485] Defense lawyers even fear that challenging the evidence will make the police or prosecutors angry, and in turn their clients may be treated worse, or a more severe sentence may be imposed. For example, if the defense lawyer argues that his client was tortured and that his confession should be excluded, this may be regarded as a lack of remorse for the crime and the sentence will not be mitigated.[1486]

c) The Possibility of Correcting Defective Evidence

Art. 56 of the *CCPL* provides that physical or documentary evidence obtained illegally, which may seriously affect justice, is admissible if a correction or justification can be provided. Such evidence is called defective evidence. This arrangement was first provided by the Supreme Court and other five organs in the *Provisions of Evidence in Death Penalty* and *The Rules on Several Issues on the Exclusion of Illegal Evidence in Criminal Cases* ("关于办理刑事案件排除非法证据若干问题的规

[1480] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 158; *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 186.

[1481] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 158.

[1482] However, if the trial is conducted a long time after the torture occurred, no wounds can be seen any more. See *Luo*, 政法学刊 (Journal of Political Science and Law) 28 (2011), 71, 72.

[1483] *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 186.

[1484] *Wu*, 现代法学 (Modern Law Science) 36 (2014), 121, 128–129.

[1485] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 157. Exclusion may have a greater impact on sentencing than on the conviction, 156.

[1486] *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 186; *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 154.

定")[1487] in 2010. The drafter of these two documents[1488] arrived at a compromise solution in order to make the exclusionary rule more acceptable to the police and prosecutors. A similar rule was later introduced into Art. 56 of the *CCPL*.

It is not clear what evidence belongs to the category of "defective evidence". Some scholars distinguish between illegal evidence and defective evidence. The former refers to cases in which the rights of the defendant or substantive procedural rules were seriously violated, whereas defective evidence connotes the violation of technical rules, such as typing mistakes.[1489] Some judges argue, however, that defective evidence is a special type of illegal evidence.[1490]

According to Art. 28 of the *Rules on the Review of the Evidence*, audio-visual materials shall be excluded if their reliability cannot be confirmed or if the time, location and methods of their production cannot be reasonably explained or proved. From this wording, it follows that the rules on defective evidence mainly serve the goal of truth-finding. If the defect has no impact on the reliability of the evidence, it can be corrected. For example, if TIMs were taken without a warrant, the judge will probably ask the police to "correct" this defect by subsequently producing a warrant. If the police or the prosecutor fail to correct the defective evidence and the judge cannot confirm the reliability or the relevance of the evidence, it may be excluded.[1491]

Given the weak position of the court and the truth-finding considerations stated above,[1492] it is no surprise that judges will ask for a correction before they decide to exclude evidence.[1493] According to an empirical study on defective evidence, corrections were accomplished in most cases (705 out of 799 cases, 88.2 %).[1494] The most frequent ground for a correction was a "writing mistake", followed by "negligence".[1495]

11. Review and Exclusion of Evidence of TIMs

Evidence from TIMs is not mentioned in the exclusionary rule established in Art. 56 of the *CCPL*, which applies only to oral confessions and physical or documentary evidence.[1496] In practice, TIM evidence is regarded as audio-visual materials

[1487] 法发 (2010) 20号.

[1488] *Chen*, 法学家 (Legal Scholar) 2 (2012), 66, 67.

[1489] *Id.* at 68; *Yan*, 法制与社会发展 (Law and Social Development) 2 (2014), 182, 185.

[1490] *Chen*, 法学家 (Legal Scholar) 2 (2012), 66, 73.

[1491] See the case in Fn. 1498 and accompanying text.

[1492] See Section 10. a), Chapter V, Part III.

[1493] *Zuo*, 法商研究 (Studies in Law and Business) 3 (2015), 151, 152.

[1494] *Yi*, 环球法律评论 (Global Law Review) 3 (2019), 19, 28.

[1495] *Id.* at 29.

[1496] The transcripts and reports are sometimes defined as documentary evidence. However, this classification has often been criticized.

and digital data, whose examination and admissibility is regulated in Section 7 of the *Explanation on the Application of the CCPL* (2021). Art. 108 lists the elements to be reviewed for audio-visual materials,[1497] while Art. 110 concerns digital data, such as emails, online chatting, blogs, Weibo (Chinese twitter), SMS, digital signature, etc. The requirements for these two types of evidence have many similarities. The main criteria are the originality, the reliability, the legality of the collection process, the relevance to the case, and the completeness. In principle, judges should review the legality of TIMs. According to the questionnaires, the prosecutors do the same.

Art. 109 provides two "compulsory" causes for the exclusion of audio-visual materials and digital data: (1) their reliability cannot be verified; and (2) there are unexplainable doubts as to the time, location, and methods for producing or collecting the evidence. For instance, in a drug trafficking case, the prosecutor did not manage to provide a voiceprint identification of a telecommunication tape recording after the defense lawyer argued that the voice in the recording was not his client's. As a result, the court excluded this recording. Since the reliability of the contents of the tape could not be verified, the defendant was convicted of a lesser crime, i. e., illegal ownership of a drug instead of drug trafficking.[1498]

In another drug trafficking case, the investigator copied the online chats and the payment records from the suspect's computer. The defense lawyer argued that such copies should be excluded since they were not original. The court denied this motion stating that the data was not stored in the computer and that it would have been inappropriate for the investigator to seal the server that stored the data. Moreover, the use of copies instead of originals as evidence did not seriously impair the administration of justice.[1499] The court implied that the origin of the data was clear although only copies were shown in court. In another drug case, the court excluded the defendant's phone conversations as evidence, stating that neither the evidence-producing process nor the origin of the evidence was clear.[1500]

[1497] Art. 108 of *the Explanation on the Application of the CCPL* (2021) emphasizes that the following issues regarding audio-visual materials should be reviewed and verified: (1) whether there is an explanation of the process of obtainment, and whether the source is legal; (2) whether the materials are the original version, whether there are other copies; (3) whether the materials are produced in violation of the legislation and regulations, such as by threatening or cheating; (4) whether the time, location, conditions and methods used to produce the materials are explained; (5) whether the contents are reliable, whether they are edited, supplemented or deleted; and (6) whether the contents are relevant to the case. If there exists doubt as to these issues, the judge should order an expert to review the materials.

[1498] Najiriri, (2014) Cheng Criminal First Instance No. 188 (纳吉日日,(2014) 成刑初字第188号刑事判决书). A similar case: Li, (2015) Second Middle Court, Beijing, Criminal First Instance No. 476 (李方印非法持有毒品案,(2015) 二中刑初字第 476 号刑事判决书).

[1499] Li, (2017) Jin Criminal Final No. 21 (李某林等人贩卖毒品,(2017) 晋刑终21号). http://www.scdplaw.com/fanmaidupinzui/caipanwenshu/2791.html, visited at 14. 10. 2019.

[1500] Yang, Shang, Zhang Xjun and Zhang, (2016) Jin 02 Criminal First Instance No. 29 (杨某、尚某、张某军、张某犯贩卖、制造毒品,(2016) 晋02刑初29号).

The application of the two clauses of Art. 109 in these cases clearly shows that the rules are more concerned about ensuring the reliability of the evidence than the legality of their collection. One reason is that TIMs are generally considered as advanced measures with little negative effect on human rights. That is understandable if compared to the torture scandals that have become known. Hence the main task of the legislature and the courts is regarded as ensuring the reliability of TIM evidence, whereas the impact of surveillance on human rights is largely ignored.

Responding to Question 8 of Model B, 6 prosecutors and 1 judge said that they review the legality of TIMs; one prosecutor and one judge answered in the negative. Among the seven persons who reviewed the legality, only one said that he had ruled a TIM to be illegal, six said that they never had done so. This shows that judges and prosecutors are very hesitant to rule TIMs illegal in view of the high reliability of the evidence. If the reliability of the evidence cannot be verified, as in the case described above,[1501] the judges will not immediately rule the measure illegal but will put it aside or ask for an explanation. Only if this fails will they consider excluding the evidence.[1502]

In the questionnaires, the following elements are considered to be criteria for the illegality of TIMs: (1) the warrant has been issued without the approval procedure, (2) a national secret, trade secret or private information are leaked, (3) the TIM exceeded its duration, (4) the TIM was applied to non-catalogue crimes, and (5) a person not named in the warrant was intercepted.[1503] This result shows that although TIMs are rarely ruled illegal, prosecutors and judges do comprehensively review the measures whenever possible.

If prosecutors and judges find that the evidence from TIMs violates the law, they have several options. They can return the evidence to the police or prosecutor for further investigation,[1504] they can put it aside, they can accept it, or they can communicate with the investigators. The last option is the most common in practice.[1505] This shows that prosecutors and judges favor softer solutions rather than ruling measures illegal and excluding evidence.[1506] This practice itself is not problematic since judges and prosecutors have a right to ask for more details when they have doubts, but "conspiracies" among judges, prosecutors, and the police to cover up illegal conduct should be prevented. Communications between judges, prosecutors, and the police should be put on record and be subject to discovery by the defense. If possible, the defense lawyer should be present at any discussion or pre-trial hearing concerning the evidence.

[1501] Fn. 1498 and accompanying text.

[1502] See also Section 10. a), Chapter V, Part III.

[1503] Question 10 Model B in the Appendix.

[1504] This means that police or prosecutors should offer new evidence.

[1505] Question 11 Model B in the Appendix.

[1506] See Section 9. a), Chapter V, Part III.

12. The "Legitimization" of Evidence: the Move from "Illegal" to "Legal"

The American "fruit of the poisonous tree" doctrine is a popular topic among Chinese criminal justice scholars. In principle, however, such a far-reaching effect of exclusionary rules is not recognized in China.

It is common practice for police to transform illegal information into "legal" evidence. Three approaches are being used. First, the police may correct defective evidence and thereby make it admissible.[1507] The other two approaches, i. e., repeated confessions and the "delicious" fruits of the poisonous tree, will be discussed in this Section.

a) Admissibility of Repeated Confessions

The term "repeated confession"[1508] refers to the situation that a suspect made a confession under torture or other forbidden method and later was interrogated by the police again and repeated the same confession "voluntarily". In a case report, the first confession of the suspect was excluded, however, four further statements with similar contents were accepted by the court.[1509] Art. 1 of the *Rules on the Exclusion of Illegal Evidence in Criminal Cases* (2018) (Trial)[1510] issued by the Supreme Court constitutes some progress in this regard. Art. 1 provides that if a confession has been brought about by torture, a repeated confession made due to the impact of the former confession with the same contents shall be excluded along with the former confession, save for exceptional situations. This rule, however, is not provided in the *CCPL* 2018. In order to correct this flaw, Art. 124 of the *Explanation of the Application of the CCPL* (2021) provides for the exclusion of a repeated confession influenced by the confession obtained by torture.

b) Indirect Admissibility: the "Delicious" Fruits of the Poisonous Tree

Another way of legitimizing illegal evidence is to use information for further investigations. This is especially common regarding TIM evidence. For example, the investigator may play an illegally recorded tape to the suspect in the course of the interrogation, and as a result the suspect confesses to the crime. Such a confession is probably admissible. The violation here is not regarded as a "threat" as mentioned in Art. 1 of the *Rules on the Exclusion of Illegal Evidence in Criminal Cases.* Therefore, it does not reach the threshold for exclusion of oral evidence. Due to the prioritization

[1507] See Section 10. c), Chapter V, Part III.

[1508] See also Fn. 1485 and accompanying text.

[1509] *Zhang*, 北京开审非法证据排除第一案 (First Case on the Exclusion of Illegal Evidence in Beijing), 新京报 (New Beijing Daily), 14. 09. 2012.

[1510] Fn. 1478.

of truth-finding, physical or documentary evidence discovered through using information from inadmissible TIMs is admissible as long as it is *per se* reliable. In practice, the police will only submit the final results, such as the physical or documentary evidence discovered, if they have doubts as to the legality of TIMs[1511] or if they think that the final results are already sufficient to prove guilt. This was standard practice before information from TIMs was recognized as evidence by the *CCPL* 2012.[1512] In such a situation, once the police obtain physical or documentary evidence in a legal way, the judge might not even know that TIMs were taken.[1513]

Although the CCPL 2012 allows TIM evidence to be directly presented in court, it is still a routine practice for police to not disclose the use of TIMs to prosecutors or judges. The new *Explanation of the Application of the CCPL* (2021) requires police to submit TIM evidence if police want it to be considered, however, it still does not solve the problem that the police tend to cover up TIMs and only submit the "legal fruit" produced by TIM evidence. Even if defective TIM evidence were submitted, it will probably be repaired by correction. Then further TIM evidence will be admitted without any problem.

c) Incidentally Discovered Evidence

The *CCPL* does not clearly rule on how information incidentally collected through TIMs can be used. Art. 152 III of the *CCPL* provides: "Materials obtained by technological investigative measures shall only be used for the investigation, prosecution and trial of criminal cases, and shall not be used for any other purposes." It restricts the use of such materials to purposes of criminal cases, but it does not explain whether the materials collected for the purpose of crime A can be used for proving crime B, either as a clue for the investigation or as evidence. In the interview Question 25 Model A, all three interviewees said that there were no problems in using materials collected for one crime for prosecuting another crime, even if the latter does not fulfil the criteria for TIMs.[1514] This opinion was supported by Interviewee Mr. W. He argued that the adoption of TIMs takes up judicial resources. Therefore, once the materials are collected, they should be used at their greatest value. Moreover, he said that as the police are not at fault in collecting this material, it is right that they should make good use of it. Mr. W even likened this situation to the proverb of when "a cannon is used but only a mosquito is killed". He reflected that "we cannot say that this is wrong".[1515]

[1511] Question 15 Model A in the Appendix.

[1512] *Xue/Xiong*, 技术侦查的规范适用 (Proper Application of Technological Investigation), 人民法院报 (People's Court Daily), 19.09.2018.

[1513] See also Section 3, Chapter V, Part III.

[1514] Question 25 Model A in the Appendix.

[1515] Interview with Mr. W.

This is another example of the prioritization of "truth-finding" in Chinese criminal procedure. If evidence or clues are in the hands of the police, they cannot accept that they should not be permitted to use it to investigate other crimes. This idea is in line with the notion that the fight against crime is the main purpose of the *CCPL*.[1516] Following this logic, it can be concluded that if the police incidentally obtain information on a person who is not the original target of the investigation, such information can also be used against this person.

This practice extends the application of TIMs and allows TIM evidence to be used in a case for which it was not originally meant to be used. The doctrine of incidental findings should be strictly interpreted in order to control such unregulated extensions.

Problems such as indirect admissibility and incidental results from TIMs do not draw much attention, because the exclusion of TIM evidence is rare. The exclusionary rule in China is just beginning to be recognized, hence more fundamental issues are waiting to be resolved, such as the scope of exclusion, the result of exclusion and the exclusion of repeated confessions. If legislation, theory and practice relating to the exclusionary rule develop further, it can be expected that the issues concerning TIMs will also be further discussed and that the rules will become more detailed and concrete. The rules need to be clarified further and the use of materials from TIMs needs to be more strictly regulated.

13. Admissibility of Evidence Collected by Private Persons in Criminal Proceedings

a) Legality of the Collection of Evidence by Private Persons

Reacting to the rapid development of private detective agencies in China, in 1993 the Public Security Ministry issued a Notice prohibiting private detective agencies. It declared that this business has no legal basis and partially executes public authority, causing certain problems.[1517] Due to the high demand for such services, however, detective agencies have started describing themselves as "consulting agencies" in order to circumvent the regulations prohibiting their activities.[1518] There are even professional associations of private detectives. Such businesses run legal risks, however. In some cases, "private detectives" have been convicted of disclosing or selling private information.[1519]

In 1997, the Supreme Court explained that only evidence obtained in a legal way can be used. Privately recording conversations without the consent of all speaking

[1516] See Section 13, Chapter V, Part III.

[1517] 公安部关于禁止开设"私人侦探所"性质的民间机构的通知 (Notice by the Public Security Ministry on the Prohibition of "Private Detective Agencies"), 07.09.1993.

[1518] https://www.zhihu.com/question/20035246, visited at 27.12.2020.

[1519] *Ibid.*

persons is illegal and such recordings cannot be used as evidence.[1520] This does not absolutely exclude private recordings from evidence, but admission presupposes that all speakers had consented to the recording. There are many activities not foreseen by law, however, which makes it difficult to decide whether they are legal or illegal.[1521]

Art. 106 of the *Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law* ("最高人民法院关于适用<中华人民共和国民事诉讼法>的解释")[1522] provides that "[e]vidence formed or acquired by a serious infringement upon the lawful rights and interests of others, a violation of legal prohibitions or a serious breach of public order and good custom shall not be deemed a basis for deciding the facts of a case." Unfortunately, the words "infringing upon the lawful rights and interests of others" are too vague to be applied in practice. This rule is, nevertheless, evidence of the Supreme Court's skepticism about the private collection of evidence. Criminal evidence, however, may follow different standards from those of civil evidence. Therefore, the admissibility of privately collected evidence in criminal proceedings is still not clarified.

Art. 54 of the *CCPL* provides that courts, prosecutors, and public security institutions have the authority to collect or obtain evidence from the units and individuals concerned. Art. 43 grants defense lawyers the limited right to collect evidence, namely, with the consent of witnesses or other entities and individuals concerned. The lawyer may also apply to the prosecutor or the court to collect specific evidence. There is a controversy on whether private persons are qualified to collect evidence in criminal cases. Some argue that the *CCPL* grants such authority only to judges, prosecutors, police, and lawyers;[1523] while others argue that the *CCPL* does not prohibit private persons from collecting evidence.[1524]

Art. 283 of the *CCL* prohibits the production and sale of special espionage devices and of professional eavesdropping or secret photographing devices. Art. 284 prohibits the illegal use of such devices, and these crimes carry serious sanctions. These two articles, however, are limited to "professional devices". Normal devices (such as a cellphone or a normal camera) do not fall within this category. The National Security Department and the police have the authority to use such professional devices, but they should follow the procedures discussed in III.9. of this Part.

[1520] *Response by the Supreme Court that Private Recordings of Conversations without Consent of Other Speaking Partners Cannot be Used as Evidence* ("最高人民法院《关于未经对方当事人同意私自录制其谈话取得的资料不能作为证据使用的批复") (Invalid), 法复 (1995) 2号. This is a response to the question submitted by a lower court about whether tapes that were privately recorded without the consent of the other speaking party can be admitted as evidence. This document has since been superseded by other rules.

[1521] *Zhou/Zhou*, 广西警官高等专科学校学报 (Journal of Guangxi Police Academy) 5 (2011), 14, 17.

[1522] 法释 (2020) 20号.

[1523] For instance, *Zhou/Zhou*, 广西警官高等专科学校学报 (Journal of Guangxi Police Academy) 5 (2011), 14, 17.

[1524] For instance, *Li*, 河北法学 (Hebei Law) 11 (2005), 7, 8.

b) Legitimization of Private Evidence

In practice, evidence collected by victims or witnesses is normally not used in court.[1525] The exclusionary rule provided in the *CCPL* does not apply to private evidence because it regulates only the public activities of judges, prosecutors, and police. Due to the emphasis placed on truth-finding, however, judges usually follow the same standards as they do with regard to evidence collected by the police.[1526] It is also quite common that private evidence is "legitimized" by the police. That means that private evidence is given to the police as a clue, then the police convert it into their own evidence if they think it is necessary.[1527] This has been criticized as a waste of police resources because the evidence must be collected "repeatedly".[1528] This practice resembles the "clean hand" doctrine in the U.S. If the police take evidence with a clean hand, the evidence is admissible even if a private person had originally acted illegally in obtaining the evidence.

The issue of the admissibility of evidence collected (legally or illegally) by the defendant or a defense lawyer, who by doing so violated a restriction imposed by Art. 43 of the *CCPL*, is even less clear. Unlike the police, the defense lawyer cannot legitimatize private evidence. Art. 43 of the *CCPL* strictly limits the ability of defense lawyers to collect evidence. If a strict standard for admission of such evidence is applied, that further weakens the defense in comparison with the prosecution. The *CCPL* or *the Law of Lawyers* should grant defense lawyers more authority to collect evidence for their clients, or it should impose certain obligations on the police or prosecutors to cooperate with lawyers.

VI. Conclusions

Art. 40 of the *Chinese Constitution* permits the surveillance of correspondence by the police or prosecutors for the purpose of state security or criminal investigation in accordance with procedures prescribed by law. Art. 39 of the *Constitution* guarantees the inviolability of the residence; however, many commentators believe that it prohibits primarily physical invasion, while the acoustic surveillance of conversations in a residence is not covered. This suggests that the use of TIMs in China has a weak constitutional foundation.

Starting in the 1980s and 1990s, legal documents and legislation expressly authorized the police and prosecutors to carry out TIMs to investigate criminal cases. The information obtained from such measures, however, was not allowed to be directly used as evidence nor to be presented in court. Such information could only be

[1525] *Ibid.*

[1526] See Section 10. a), Chapter V, Part III.

[1527] *Li*, 河北法学 (Hebei Law) 11 (2005), 7, 8. See also Section 12, Chapter V, Part III.

[1528] *Li*, 河北法学 (Hebei Law) 11 (2005), 7, 9.

used as a clue for further investigative activities. Given the increasing need to fight crime more efficiently and to improve the quality of evidence, the *CCPL* 2012 declared that information obtained through TIMs may be used as evidence. The new rules on TIMs in the *CCPL 2012* introduced a stricter procedural control for TIMs than for other investigative measures. The *CCPL*, however, fails to define TIMs and does not fully explain what necessitates strict procedures. This gives the police broad discretion and essentially allows them to maintain their former practices. Therefore, the new rules on TIMs in the *CCPL* are merely "declaratory" and their impact on the use of TIMs is limited.

In China, there is no requirement for a judicial order for TIMs. They may be issued by the director of the police station at the city level or above.[1529] The police decide what type of measures to carry out and provide details of the implementation, such as the duration and the targeted persons. The police thus have a dominant role in the implementation of TIMs. This intensifies concerns regarding the abuse of TIMs.

The far-reaching authority of the police regarding TIMs seems more understandable when placed within the wider context of the Chinese criminal justice system. The Chinese police force has an avowedly political function; they guarantee and boost the authority of the government. Therefore, the police are granted more power than prosecutors or courts. They are the final decision-makers on most investigative issues. The original aim of these rules was to exclude prosecutors and judges from intervening in investigative issues. Such interventions were believed to delay the investigative process and to obstruct truth-finding, which is the primary goal of Chinese criminal procedure.

The lack of supervision over police activity can lead to serious abuse of police power. Police corruption is currently coming under increasing public scrutiny. To restore the credibility of the judicial system, the early participation of prosecutors in investigations has been made possible. Still, prosecutors very rarely request to participate in investigative activities. More effective measures should be designed to restrict police power. It may not be realistic to introduce judicial control over police, but prosecutors could be given more authority to oversee investigative activities, such as the issuing of warrants. The mechanism which enables the early participation of prosecutors is already a good start.

The *CCPL 2012* permits information obtained from TIMs to be used as evidence in court. According to various empirical studies, however, it is quite unusual for such information to be presented at trial. In most cases, only transcripts and reports are presented instead of the original recordings. The reasons for this are numerous. First, the *CCPL* does not require the police to hand over such information to prosecutors or judges. Second, the police tend not to include evidence from TIMs in case files, so as to avoid possible challenges from defense lawyers. This is certainly the case when TIMs have been carried out illegally. In that case, police prefer to turn illegally

[1529] Only in exceptional cases are warrants issued by prosecutors or supervision committees.

obtained evidence into legal evidence, for example, by using an illegally obtained recording for extracting a confession from a suspect. As an improvement, Art. 122 of the *Explanation of the Application of the CCPL* (2021) grants judges the authority to order prosecutors to hand over original recordings obtained from TIMs to the court. If the prosecutor does not comply in time, the judge should decide the case without considering the TIM evidence. More time is needed to see whether this judicial explanation will make police or prosecutors to hand over original recordings more often or will push them in the opposite direction, namely, to cover up TIMs and only submit legal evidence extracted from TIMs to avoid any "trouble".

Defense lawyers have become more active in challenging the admissibility of evidence obtained from TIMs when such evidence is presented at trial. Such efforts have, however, seldom been successful, and evidence from TIMs is rarely excluded. In light of the great emphasis placed on truth-finding, Chinese judges are hesitant to exclude reliable evidence from TIMs even if the evidence was obtained illegally. In addition, defense lawyers not only carry a heavy burden to prove the illegality of TIM evidence but also have no access to the details of TIMs. Even if the legality of such evidence is doubtful, judges will first ask prosecutors to "repair" the defect rather than simply excluding evidence.

To sum up, the current rules on TIMs in China are far from sufficient to protect the privacy and procedural rights of individuals. Evidence obtained illegally from TIMs is frequently admitted at trial, either directly or indirectly. More measures to improve the transparency of TIMs and to enhance the practice of excluding evidence are required for promoting the rule of law.

Part IV

Conclusions with Horizontal Comparison

It is well recognized that there are two basic models of the criminal process, namely, the adversarial model in the common law systems and the inquisitorial model in the civil law systems, including the People's Republic of China.[1530] Numerous differences can be observed between these two traditions; for instance, different roles of prosecutors, judges and defense lawyers in the criminal process, and the organization of the trial. On the one hand, despite these differences, the two legal models agree on some basic legal principles and take a similar approach to various issues.[1531] On the other hand, even though they follow the same model, different jurisdictions have their own characteristics and adjust their justice system to suit their own social needs or political purposes,[1532] such as in Germany and China, the U.S. and England. The three jurisdictions discussed in this study, the U.S., Germany, and China, in fact combine features of both models.[1533]

To discuss surveillance measures in a systematic way, the first three Parts of this study have focused on the U.S., Germany and China respectively. This conclusion provides an overarching comparison of the three jurisdictions, and the advantages and disadvantages of each legal solution will be analyzed. Furthermore, the conclusion aims at contributing to the ongoing discussion of possible reforms in the PR China.

I. "Reasonable Expectation of Privacy" vs. "Core Area of Privacy"

1. Different Constitutional Approaches to the Right to Privacy

A country's constitution is commonly regarded as the highest level of the law, which guarantees the basic rights of citizens. All other legislation and regulations

[1530] See *Spencer*, in: Delmas-Marty/Spencer (eds.), European Criminal Procedures, 2005, 635.

[1531] *McEwan*, in: Duff et al. (eds.), The Trial on Trial – Volume 1: Truth and Due Process, 2004, 51 – 52.

[1532] *Fabri*, Four Criminal Procedure Case Studies in Comparative Perspectives: China-Italy-Russia-U.S.A., 2016, 2.

[1533] *Ibid.*

should comply with the constitution. Given the different political, social, historical, and cultural contexts, however, constitutions are formulated with various structures and interpreted in different ways from country to country.[1534] It is no surprise, therefore, that the constitutional approaches to the protection of privacy in the U.S., Germany, and China are also quite different.

The *Declaration of Independence* of the U.S. and the enactment of its Constitution in 1789 was the starting point of its constitutional system. The *Bill of Rights* left much space for interpretation, and therefore courts applied the basic rights in different ways. The U.S. Supreme Court ruled that interceptions of telephone conversations conducted by law enforcement officers are searches and fall within the protection of the 4th Amendment. Based on the 4th Amendment, the Supreme Court in the *Katz* case[1535] developed the doctrine of "reasonable expectation of privacy", which replaced the traditional "trespass doctrine" as the main test for the legality of warrantless interceptions.

In Germany, the GG was enacted after World War II. Due to the shadow cast by the Nazi regime, GG guarantees human dignity in its very first article and the free development of personality in Art. 2. The BVerfG defined certain individual rights on the basis of these two articles[1536] and declared that citizens have a right to a private space where they are left alone, can enjoy privacy, and act with autonomy.[1537] Through further case law, the BVerfG developed the concept of the "core area of privacy", which is limited to highly personal matters and does not interfere with the personal sphere of others or with the interests of society. The core area of privacy includes the expression of the inner consciousness of a person, such as their emotions, feelings, thoughts, opinions and other highly personal experience, as well as the expression of their sexuality, which is essential for the free development of their personality.[1538] According to BVerfG case law, telecommunication and activities in the home belong to the "core area of privacy", except where criminal information is involved.[1539] This concept established an absolutely protected area of privacy that must be totally free from interception by the State.

The U.S. Supreme Court never attempted to define "privacy" directly and did not state what specific information is protected by the 4th Amendment. The "reasonable expectation of privacy" focuses on protected spheres rather than information and to a large degree concerns the legality of police activities and the admissibility of certain evidence in criminal proceedings.[1540] By contrast, the BVerfG has defined the scope

[1534] *Hu/Han*, 中国宪法 (Chinese Constitutional Law), 2018, 6.

[1535] *Katz v. United States*, 389 U.S. 347 (1967).

[1536] BVerfGE 54, 148, 153; 27, 1. 6.

[1537] BVerfGE 27, 1. 6; 34, 269, 282.

[1538] BVerfGE 109, 279, 313, 314. See also Fn. 604 and the companying texts in Chapter I, Part II.

[1539] See Section 1. b) aa), Chapter I, Part II.

[1540] *Herrmann*, in: Vogler (Hrsg.), Festschrift für Hans-Heinrich Jescheck, 1985, S. 1298.

of "privacy" from different legal perspectives, such as the right to one's spoken word, the right to data autonomy, and the right to the integrity of information systems. From this perspective, U.S. law protects a formal "sphere" of privacy, whereas German courts care more about substantial contents.

In China, modern constitutional concepts, such as a parliamentary system and the concept of democracy, were first introduced at the end of the 19th century when China was still a monarchy. This period is regarded as the beginning of the modernization of the Chinese legal system. Due to wars and political unrest, however, it took some time for a modern concept of the rights of citizens to be well established in the Chinese legal system. The Chinese Constitution of 1982 marked a huge progress concerning the rights of citizens. Art. 39 and Art. 40 protect the inviolability of the residence and of telecommunication, respectively. Chinese scholars regard these two articles as the most important constitutional basis for the right to privacy. Since the Chinese Constitution cannot be directly applied by courts, the Chinese Supreme Court cannot offer an interpretation of its provisions or of the relationship between these two articles and the right to privacy. Therefore, in practice, the Constitution plays a quite limited role in the protection of the right to privacy. It can only be applied indirectly through other legislation. In the context of TIMs, the strict procedural requirements for such measures provided in the *CCPL* can be understood to comply with Art. 39 and Art. 40 of the Chinese Constitution.

Compared to the U.S. and Germany, China lacks a systematic interpretation or a core concept of the right to privacy. Meanwhile, the wide-spread use of e-payments and face recognition systems in daily life has influenced citizens' understanding of their privacy. The fact that people are increasingly disclosing more and more private information during their daily lives might give the police the misleading impression that all such information is no longer deemed private. This problem is similar to the issue of the "reasonable expectation of privacy" in the U.S., where the scope of protected privacy is contracting. With the increasingly fast-paced development of technology, the definition of what constitutes a reasonable expectation of privacy in both the U.S. and in China is changing, with the result that less and less private space is being protected. This may lead to a worse situation in China than in the U.S., because in China the rapid development of technology occurs before a concept of privacy has been firmly established. At present, the concept of privacy is in China mainly discussed with regard to civil law, not criminal law. There is still no unified standard for determining whether legal provisions or investigative measures infringe upon the right to privacy. Even if the right to privacy has been violated in the course of an investigation, that fact would normally have no influence on the later stages of a criminal process. Evidence from TIMs is rarely excluded on the grounds of a violation of the right to privacy, although the *CCPL* requires that the right to privacy should be protected. In China's criminal justice system, the need to protect the individual's right to privacy is not prioritized.

2. "Reasonable Expectation of Privacy" and "Core Area of Privacy"

Unlike China, which does not have a systematic approach to the right to privacy in criminal procedure, "the reasonable expectation of privacy" in the U.S. and the "core area of privacy" in Germany have been widely discussed.

As stated in Part I, the "reasonable expectation of privacy" under U.S. law requires "an actual (subjective) expectation of privacy" that society is prepared to recognize as "reasonable". Under this doctrine, the right to privacy of a person is protected by the 4th Amendment only if that person has a subjective expectation of privacy and if that expectation is supported by larger society. By contrast, the German BVerfG in a case concerning a diary developed a different three-factors-test, asking (1) whether the concerned person has the will to keep the information secret, (2) whether the information is highly personal, and (3) whether it interferes with the personal sphere of other persons or with the interests of society.[1541]

a) The Subjective Element of the Reasonable Expectation of Privacy

Despite different formulations, the first factor under German law is comparable to the subjective expectation of privacy under the U.S. doctrine of "reasonable expectation of privacy". The individual must express his desire to keep an information private.[1542] In a case involving a recording of the defendant's talking to himself when alone in his car, the BGH held that since the speaker felt unobserved ("sich unbeobachtet fühlt" in German), his monologue should be regarded as being protected by the right to the freedom of thought.[1543] His monologue was held to fall within the "core area of privacy" and hence to be inadmissible as evidence. The expression "he felt unobserved" describes the subjective judgment of the person who believes that he is in total privacy, which is indicative of the protection of words spoken as "core" private.

In another BGH case, the defendant and his wife conducted a conversation in the visiting room of a jail. The investigator had made the defendant "feel unobserved" while talking to his wife although in fact the conversation was intercepted.[1544] The BGH ruled the recording to be inadmissible but made it clear that the evidence would have been admissible if the defendant had known or could have known that he was

[1541] BVerfGE 80, 367. See also Section 1. b) aa), Chapter I, Part II.

[1542] See Section 1. b) aa), Chapter I, Part I.

[1543] BHG, NJW 2012, 945, 946 ("Die Gedankeninhalte des inneren Sprechens treten vor allem in Situationen, in denen der Sprechende sich unbeobachtet fühlt, durch Aussprechen hervor. Das möglicherweise unbewusste 'laute Denken' beim nichtöffentlich geführten Selbstgespräch nimmt sodann an der Gedankenfreiheit teil…Es bestand aus der Sicht des Angekl. SK nicht die Gefahr, dass andere Personen den Inhalt seiner Äußerungen im Selbstgespräch erfassten.").

[1544] BGH 53, 294, Rn. 45 ff.

under surveillance.[1545] Consequently, if a person could have known that he was under observation, his false assumption that he was unobserved does not lead to a violation of his right to privacy. However, any covert surveillance normally is designed to make the concerned persons "feel unobserved".[1546]

Using a similar criterion of reasonable expectation, the BVerfG ruled that a conversation that is conducted within a home in such a loud voice that it can be heard from outside is not covered by Art. 13 GG, because the speakers themselves made it possible for their conversation to be overheard.[1547] The BVerfG does not, however, explain in general terms under what circumstances a person may have expressed his expectation to keep certain information secret. The U.S. Supreme Court would probably have reached the same conclusion as the BVerfG in the case of the noisy conversation, since it requires a person to take certain measures to demonstrate his expectation of privacy, such as closing the door of the telephone booth in the *Katz* case. In subsequent case law, however, U.S. courts failed to apply a consistent standard and sometimes required precautions that were very difficult to meet, thus strongly reducing the protective effect of this subjective requirement.[1548]

b) The Objective Element of the Reasonable Expectation of Privacy

The second prong of the "reasonable expectation of privacy" test differs from that in the "core area of privacy". "Reasonable expectation of privacy" requires an objective element, while no similar expression can be found in the doctrine of the "core area of privacy". German courts do not consider the opinions of society on what is covered by the "core area of privacy". German courts nevertheless rejected the view that a person's subjective will to keep certain information private is by itself sufficient to place that information within the core sphere of privacy.[1549] For example, in the jail case discussed above the BGH pointed out that visiting rooms and cells of custodial facilities may generally be entered by officers without the agreement of detainees, who therefore have no right to privacy in such areas even if they would like to enjoy privacy there.[1550] This demonstrates that German courts take objective elements, such

[1545] BGH 53, 294, Rn. 55 ("Gegen die Zulässigkeit einer solchen Maßnahme bestehen dagegen keine Bedenken, wenn der Untersuchungsgefangene weiß oder jedenfalls – etwa durch entsprechende Hinweise – wissen kann, dass Besuchskontakte generell oder im konkreten Fall – auch akustisch – überwacht und aufgezeichnet werden. So gewonnene Erkenntnisse wären nach den dargelegten Maßstäben verwertbar.").

[1546] BGH 53, 294, Rn. 46 ("Zwar ist die Anwendung einer kriminalistischen List auch bei Ermittlungsmaßnahmen in der Haftanstalt nicht unzulässig; auch ist es gerade das Charakteristikum von heimlichen Überwachungsmaßnahmen, dass der Überwachte sich unbeobachtet fühlt.").

[1547] BVerfGE 109, 279, 327. See also Fn. 838 and the companying texts in Chapter II, Part II.

[1548] See Section 4. b), Chapter I, Part I.

[1549] See the diary case, BVerfGE, 80, 367, 374.

[1550] BGHSt 53, 294, 300. See also Section 1. a), Chapter II, Part II.

as legislation and prison rules, into consideration[1551] when deciding whether certain information belongs to the "core area of privacy". U.S. courts likewise consider legislation and regulations when determining the objective "reasonableness" of a subjectively held expectation of privacy.[1552] Given the criticism directed against the stringent objective requirements under the "reasonable expectation of privacy" clause in the U.S. and the difficulty for courts to establish the opinion of "society",[1553] the German model, which applies a subjective standard modified by the reasonableness of the person's expectation, might be the preferable solution.

c) The Minimum Expectation of Privacy

In order to safeguard privacy from being eroded by police technology, the U.S. Supreme Court developed the concept of the "minimum expectation of privacy".[1554] Although both the "minimum expectation of privacy" and the "core area of privacy" reach beyond a physical intrusion and create a sphere of protected private information and human activities, they offer different levels of protection. If a conversation falls within the sphere of "minimum expectation of privacy", the police need a warrant to intercept that conversation. If a conversation belongs to the "core area of privacy", this conversation must not be intercepted at all. To obtain a judicial warrant, German prosecutors need to overcome the assumption that what occurs in a residential "home" falls within the "core area of privacy".

In practice, however, the results of applying these two concepts are quite similar. To obtain a search or interception warrant, police or prosecutors in both jurisdictions need to submit evidence sufficient to show that the activities in question are crime-related. Intercepted conversations belonging to the "core area of privacy" would probably also be excluded by a U.S. court, such as in *U.S. v. Lucht*, where the warrant prohibited the interception of conversations in bathrooms and bedrooms.[1555]

3. Constitutionally Protected Spaces in the Three Jurisdictions

Although the "trespass doctrine" was in the 1960s replaced by the doctrine of "reasonable expectation of privacy", the trespass doctrine had a significant influence on the definition of "reasonable expectation of privacy" in the U.S.[1556] Violations of the 4th Amendment no longer presuppose a physical trespass, but the location where conversations are conducted is still important for the issue of a reasonable expect-

[1551] See Fn. 883 and the companying texts in Chapter II, Part II.

[1552] See Section 4. b) aa), Chapter I, Part I.

[1553] See Section 4. b), Chapter I, Part I.

[1554] See Section 5, Chapter I, Part I.

[1555] *U.S. v. Lucht*, 18 F.3d 541 (8th Cir. 1994).

[1556] See *Note*, Michigan L. Rev. 76 (1977), 154, 172 – 173.

ation of privacy. For instance, under the "trespass doctrine", the curtilage of dwellings is protected by the 4th Amendment. This includes "all buildings in close proximity to a dwelling, which are continually used for carrying on domestic employment; or such place as is necessary and convenient to a dwelling and is habitually used for family purposes".[1557] In Germany, Art. 13 GG uses the German word "Wohnung" ("home"), which the BVerfG has interpreted as a "spatial private area",[1558] meaning a space for activities of private life. Besides the dwelling itself, areas attached to the house, such as a private garden, cellar, stairs, terrace, and garage, are also regarded as part of the "home". Moreover, hotel rooms, motor homes and holiday homes have the same residential function and are also protected by Art. 13 GG. A second category, "Wohnung im weiteren Sinne", refers to spaces for business, work, or social purposes.[1559] The BVerfG made it clear that the "core area of privacy" does not refer to a particular physical space but to highly personal activities taking place in a home.[1560] There exists therefore an assumption that a "home" falls within the "core area of privacy", but this assumption can be overcome. If there is sufficient evidence to believe that conversations in a private home are probably crime-related, surveillance of that home may be conducted.

A similar conclusion can be reached under the U.S. doctrine of "reasonable expectation of privacy".[1561] In addition, motel and hotel rooms also enjoy the full range of the protection of the 4th Amendment.[1562] Vehicles, business and commercial premises are also protected against unreasonable searches and seizures. If a person is residing at one of the places mentioned above, their expectation of privacy tends to be recognized as reasonable. Locations falling outside the protection of the 4th Amendment can still be protected under the "reasonable expectation of privacy" test, but that question must be decided on a case by case analysis.[1563]

The corresponding term used in Art. 39 of the *Chinese Constitution* is "residence".[1564] Due to the fact that the Chinese Supreme Court is not allowed to interpret the *Constitution*, the Supreme Court issued three judicial explanations to interpret the term "residence" in the *CCL*.[1565] According to these judicial explanations, "residence" in criminal law refers to "a place of people's living that is comparatively

[1557] *United States v. Potts*, 297 F.2d 68 (6th Cir.1961).

[1558] BVerfGE 32, 54, 72. See Section 1.a)bb), Chapter II, Part II.

[1559] BVerfGE 32, 54, 68 ff. See Section 1.a)bb), Chapter II, Part II.

[1560] BVerfGE 109, 279, 314. See also Section 1.b)ff), Chapter II, Part II.

[1561] One difference exists in regard of cars. In Germany, cars that serve only for travelling are not regarded as "Wohnung". (However, a soliloquy in a car can fall within the "Kernbereich der privaten Lebensgestaltung".) By contrast, U.S. courts have granted cars the same status as houses with regard to the protection of privacy.

[1562] *Lewis v. US*, 385 U.S. 206, 211 (1966) ("Without question, the home is accorded the full range of Fourth Amendment protections.") (Warren, C.J., opinion of the Court.).

[1563] *LaFave* et al., Criminal Procedure, 2020, § 3.2(c).

[1564] See Chapter II, Part III.

[1565] See Section 1, Chapter II, Part III.

isolated from the outside, including isolated courtyards, tents of herdsmen, fishing boats used also for family living by fishermen, and rented houses". The term "residence" in the criminal context refers to a domicile with two characteristics: a place for family life that is comparatively isolated from the outside. The scope of protection of Art. 49 of the *Chinese Constitution* is much narrower than that of the 4th Amendment in the U.S. and Art. 13 GG. In Chinese law, a "residence" is limited to a place of family life; a collective dormitory, a hotel, a work shed, or a temporary building is not, in principle, deemed a "residence".[1566] A broader definition of the term "residence" might possibly provide a better protection for personal privacy; however, the definition of a "residence" has only a limited effect on the practice of TIMs, because any TIM needs a warrant and the criteria for issuing a warrant remain the same regardless of where it takes place.

4. Values behind Different Constitutional Approaches

In the U.S., surveillance of conversations is permitted under the "reasonable expectation of privacy" doctrine if one party to the conversation agrees that it is to be recorded. The conversation can then be monitored by police without a warrant or the consenting person can himself record the conversation without consent of the other parties. This recording can then be admitted at trial.[1567] The U.S. Supreme Court stated that individuals must accept the risk of prosecution and the loss of the expectation of privacy if they pass on information to others who have no obligation to preserve secrecy. This ruling has been recognized by *Title III*, which expressly excludes consensual surveillance from the warrant requirement.[1568] This rule emphasizes that individuals must bear the personal risk arising from their trust in other persons. Moreover, the 4th Amendment protects against "unreasonable searches and seizures" and has been interpreted to protect privacy in procedural rather than substantive ways.[1569]

In Germany, a judicial order is needed in most situations involving interception.[1570] A conversation may be recorded without an order only if all parties agree. § 201 I and II StGB even makes it a crime to record or intercept a non-public conversation without proper authority, to make use of such a recording or to disclose

[1566] See Section 1, Chapter II, Part III.

[1567] Section 2, Chapter III, Part I.

[1568] Section 2, Chapter III, Part I.

[1569] *Colb*, Columbia L. Rev. 98 (1998), 1642.

[1570] In a special case, the BGH excluded a recording although an undercover agent had a judicial order, because the agent had abused the trust of the suspect and entrapped him into making incriminating statements; BGHSt 52, 11, 15.

its contents.[1571] This legislation demonstrates that in Germany individuals should feel free to communicate with others without fear of the conversation being recorded.

The different practices in the U.S. and Germany can result in different outcomes in similar cases. For instance, the BGH excluded the tape recording of a conversation between a prison administrator and an inmate that had been recorded without a judicial order.[1572] Under *Title III* in the U.S., such a situation is categorized as consensual surveillance so that a warrant is not needed.

In China, a warrant is needed for any TIM. This resembles the situation in Germany. Arts. 39 and 40 of the *Chinese Constitution* prohibit illegal searches but do not require warrants to be issued by courts. According to the *CCPL*, search warrants and warrants for TIMs are approved by high-ranking police officers following an internal administrative process. This reflects the fact that investigative activities in China prioritize effectiveness in finding out the truth. This theory is also supported by Arts. 1 and 2 of the *CCPL*.[1573] Another reason for this practice is that investigative activities should be kept secret from the public, including the courts, until the investigation is closed. The police do not deem courts to be "trustworthy". Given the traditionally powerful status of the police in China, any interference from outside would be regarded by the police as "problematic" and as a challenge to its dominant position.

5. Different Methods of Legal Interpretation

In both adversarial and inquisitorial theory, judges do more than simply apply the law. To a certain degree, judges also develop the law through their interpretation.[1574] The legal interpretation adopted by judges is specific to the legal system and the allocation of competence between the judiciary and the legislature in each jurisdiction.[1575]

In the U.S., according to the common law tradition substantial rules have been generated, to a large degree, by case law.[1576] Many important principles of criminal justice have emerged from the U.S. Supreme Court's interpretation of the Constitution.[1577] Since the provisions of the U.S. Constitution are partly formulated in ambiguous language, the U.S. Supreme Court has much leeway in developing the

[1571] Public interest may justify the recording; BayObLG NJW 1994, 1671; OLG Frankfurt NJW 1967, 1047, 1048.

[1572] BGH 31, 304.

[1573] Section 1, Chapter III, Part III.

[1574] *Edlin*, Judges and Unjust Laws, 2011, 193. See also *Brenncke*, Judicial Law-making, 2018, 68–69.

[1575] *Brenncke*, Judicial Law-making, 2018, 4.

[1576] *Greenawalt*, Statutory and Common Law Interpretation, 2013, 178, 197.

[1577] *LaFave* et al., Criminal Procedure, 2020, § 2.1.

law, which makes it possible for constitutional provisions to evolve as a consequence of changing social conditions.[1578] One example is the doctrine of "reasonable expectation of privacy" based on the 4th Amendment, which was first developed by the U.S. Supreme Court in the *Katz* case and later recognized by *Title III.*

Because U.S. courts are bound by precedent, courts need to make strong arguments if they want to overrule a precedent. This is the reason why wire communications were excluded from the protection of the 4th Amendment for decades after the Supreme Court decision in *Olmstead.*[1579] The conflict between the need to protect privacy and the *Olmstead* case became evident in the *Silverman* case, where the U.S. Supreme Court was forced to make distinctions on the basis of small technical differences in order to protect the right to privacy without formally overruling *Olmstead.* Even after the introduction of the doctrine of "reasonable expectation of privacy", U.S. law enforcement staff tend to use new technology without a warrant, while courts have no clear standards with which to establish the grounds for a "reasonable expectation" of privacy regarding that new technology.[1580] This also increases the workload of courts because the use of new technology without a warrant is frequently being challenged in court.

The chapter of the GG on civil rights is more extensive than the relevant amendments to the U.S. Constitution. For instance, Art. 10 GG expressly protects telecommunication, which has advanced the evolution of case law. The BVerfG interprets the GG based on the wording of its provisions[1581] but also makes direct references to substantive justice.[1582] Relying on a mixture of constitutional provisions and general rules, the BVerfG developed the concept of a general personality right and declared that the GG preserves an area of private life for every individual, which further developed into the doctrine of the "core area of privacy".[1583] The protection of a "core area of privacy" is one aspect of the personality right, while the "reasonable expectation of privacy" in U.S. jurisprudence is a collection of standards that can be used to determine the protective scope of the 4th Amendment, not a specific right in itself. Although case law in Germany, especially cases decided by the BVerfG and the BGH, plays an important role, German courts are not officially bound by precedents. Courts nevertheless show a high loyalty to the decisions of the highest courts. Courts in both jurisdictions thus play an essential role in developing legal doctrines.

The Chinese Supreme Court cannot interpret the *Chinese Constitution*; judges only apply and interpret statutes and regulations. From this perspective, Chinese courts have a limited ability to develop law and cannot declare laws to be inapplicable because they are deemed unconstitutional. Chinese courts nevertheless have various

[1578] *Greenawalt*, Statutory and Common Law Interpretation, 2013, 293.

[1579] See Section 1, Chapter I, Part I.

[1580] See Section 4, Chapter I, Part I.

[1581] *Goldsworthy*, in: Rosenfeld/Sajó (eds.), Handbook, 2013, 701.

[1582] See *Brenncke*, Judicial Law-making, 2018, 70.

[1583] Section 1. b) aa), Chapter I, Part II.

strategies to "make law". The most important tool of the judiciary is the Supreme Court's authority to issue judicial explanations of statutes. The legislature sometimes intentionally leaves space in the text of statutes for the Supreme Court to add details, such as in the *Explanation of the Application of the CCPL.* In both its content and length, this Explanation is semi-statutory. In this case, the legislature and the Supreme Court acted as collaborators. The former set up principles and guidelines, while the latter added practical detail. In practice, lower courts tend to apply judicial explanations issued by the Supreme Court directly rather than the corresponding statutes.

Given the powerful influence of judicial explanations, the Chinese Supreme Court sometimes uses them as a tool to apply pressure for legislative reform. One good example of this situation is the evolution of the exclusionary rule in China. The very first exclusionary rule for confessions obtained by illegal measures was established by the Supreme Court in a judicial explanation in 1998.[1584] The Supreme Court has in fact been the main conduit for the development of the exclusionary rule, while the legislature incorporated the exclusionary rule into the *CCPL* only in 2012 by merely copying the rules established by the Supreme Court. After 2012, the Supreme Court made continuous efforts to push for the application of the exclusionary rule and encouraged judges in the lower courts to exclude, for example, evidence illegally obtained through TIMs in drug cases.[1585] The most recent effort is the *Explanation of the Application of the CCPL* (2021). In addition, if courts believe that a provision of a statute is unconstitutional, or they cannot reach a reasonable conclusion by applying the statute as it currently stands, courts can turn to other more suitable provisions if they exist, or else to the ideas of social fairness or general social values to decide the case and ignore the improper provision. The concepts of social fairness or social values can, to a certain degree, be used to express the courts' understanding of constitutional values.

6. Reasonableness, Balancing od Interests, and Proportionality

The U.S. Supreme Court has adopted a reasonableness approach to the 4th Amendment of the U.S. Constitution, which expressly prohibits "unreasonable searches and seizures".[1586] A warrantless search is *per se* unreasonable and is prohibited unless it falls within one of a few exceptions to the warrant requirement,[1587]

[1584] *Yi*, 当代法学 (Contemporary Law Review) 1 (2017), 38, 38–39.

[1585] See Section 6, Chapter V, Part III.

[1586] The U.S. Supreme Court concluded that the "ultimate touchstone of the Fourth Amendment is reasonableness." See *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006).

[1587] *Bourdeau* et. al, Searches and Seizures - § 14 Reasonableness of warrantless searches and seizures, American Jurisprudence 2d, Vol. 68, updated in 2021; U.S.C.A. Const. Amend. 4. *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018).

such as a search by consent or the existence of exigent circumstances.[1588] A more controversial issue is how courts can establish whether a specific interception constitutes a search. The "reasonable expectation of privacy" doctrine aims to resolve this problem. Once a person's expectation of privacy is found to be reasonable, a warrantless interception by the police is unreasonable. To decide whether a search or seizure is reasonable, the U.S. Supreme Court often uses an interest-balancing approach, weighing the effectiveness of the search or seizure against the degree of the intrusiveness of the measure.[1589]

In Germany, a doctrine comparable to interest-balancing is the proportionality principle. The interest-balancing doctrine in the U.S. was originally derived from the continental private law school of thought, while the proportionality principle in Germany first emerged in administrative law and then further developed into constitutional law.[1590] In addition, proportionality has become a central tenet of constitutional law and is applicable to all types of rights and interests.[1591] The interest-balancing doctrine in the U.S. has never gained such a high status. Despite these differences, the two doctrines share common features.[1592] Both are applied in a constitutional review process where the legality of governmental action is challenged.[1593] Both require judges to decide on conflicts between different rights and interests, for instance, weighing an individual's right to privacy against the public interest in prosecuting crime.[1594] They both impose a balance on the process of analyzing competing interests. The doctrines can, however, lead to different outcomes. In the context of interception, interest-balancing is often used by courts to limit individual rights. U.S. courts tend to prioritize the public interest in criminal investigation for legitimatizing warrantless surveillance. By contrast, in Germany the proportionality principle aims to prevent excessive infringements upon personal rights. This means that the individual rights provided for in Art. 10 GG may be restricted only to a proportional degree. A disproportional restriction of the right to privacy in telecommunication would be unconstitutional.

II. Statutory Protections

Statutes, specifically *Title III* in the U.S., §§ 100a ff. StPO in Germany, as well as the *CCPL* and other regulations in China provide detailed rules for surveillance and are thus highly significant for legal practice.

[1588] See Chapter III, Part I.

[1589] *Colb*, Columbia L. Rev. 98 (1998), 1642.

[1590] *Cohen-Eliya/Porat*, Proportionality and Constitutional Culture, 2013, 11, 15.

[1591] *Id.* at 3.

[1592] *Id.* at 10, 16.

[1593] *Id.* at 16.

[1594] *Id.* at 2.

1. Different Statutory Approaches to Regulating Surveillance

In the U.S., 18 U.S. Code § 2511 categorizes three different groups of interceptions: interceptions of wire, oral, and electronic communications. The protections relating to these three types of communication are subject to the same standard, "the reasonable expectation of privacy", and follow similar procedures provided for in 18 U.S. Code § 2518. Although the location of the communication is an important issue when establishing a "reasonable expectation of privacy", the legislation *per se* does not provide different rules for different locations. Courts are to define the "reasonable expectation of privacy" in individual cases.

The StPO differentiates between telecommunications, acoustic surveillance, online searches, and other measures (§§ 100a ff. StPO) and takes into account the location where the communication took place. For instance, § 100c StPO regulates acoustic surveillance in the home, whereas § 100f StPO provides for acoustic surveillance outside of the home. § 100c StPO sets higher standards for intercepting communications in a home, reflecting the "core area of privacy" doctrine under which a home is granted special protection. Statistics show that warrants are issued under § 100c StPO much less frequently than under § 100a StPO.[1595]

Rules on TIMs in the *CCPL* make no distinction between different types of communication or location. All provisions for TIMs fall under the category of "technological investigative measures". All measures follow the same standards and procedural rules. The type of measure to be adopted and the form of communication to be intercepted are to be described in the warrant, but nothing else is required.

German legislation provides more detail for each type of measure; this makes the application of the provisions more practical for police, prosecutors, and judges. Moreover, since judicial orders are needed for almost all interceptions, police and prosecutors are unlikely to conduct warrantless interceptions. Compared to Germany, *Title III* in the U.S. provides a unified standard and various procedural rules for both wire and oral communications. Although this might seem to simplify the rules, in practice this can cause difficulties for police who struggle to predict the rulings of judges. If judges interpret the rules differently from police, the evidence may eventually be excluded. This can lead to a massive waste of investigative resources. The rules provided by the *CCPL* are often too simple to have much practical meaning. Chinese police, prosecutors and judges rely too much on the regulations issued by the ministry, the Chinese Supreme Prosecution Office, or judicial explanations. More detailed and clearly formulated rules are required to improve the practical implementation of TIMs and to protect the rights of the defense.[1596]

[1595] Statistic source: Bundesamt für Justiz https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Wohnraum/Wohnraumueberwachung_node.html;jsessionid=DD1F601722E93979048097805630C61A.1_cid393 and https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html, visited on 30.04.2021.

[1596] More discussion can be found in Chapter VI, Part IV.

2. The Relationship to Other Constitutional Rights

As one of many investigative measures, interceptions infringe not only upon the right to privacy but can also touch upon other constitutional rights.

a) Self-incrimination

The 5th Amendment of the U.S. Constitution prohibits compelling persons to incriminate themselves.[1597] According to case law, interceptions under *Title III* do not amount to "compulsion". In the case of surveillance by undercover agents, suspects are deemed to engage in incriminating conversations voluntarily with such agents or police informers. Moreover, the 5th Amendment applies only to interrogation situations. Interception, by its very nature, must be conducted covertly and therefore is not equivalent to an interrogation. Therefore, the 5th Amendment is not applicable to cases of interception.

The privilege against self-incrimination is not expressly provided for in German legislation; however, the BVerfG has established *nemo tenetur se ipsum accusare* as a constitutional principle based on human dignity in Art. 1 GG as well as "Rechtsstaatlichkeit" in Art. 20 GG. The *nemo tenetur* principle has been said to apply only to official interrogations and "interrogation-like" situations. A passive interception therefore does not violate this principle. If an undercover agent is involved, the BGH excludes evidence only if the agents has entrapped a suspect into incriminating himself, if the suspect was under psychological pressure created by the undercover agent, or if the agent abused a special bond of trust between himself and the suspect. § 136a StPO leads to the exclusion of testimony obtained through certain prohibited interrogative methods. Unlike the 5th Amendment, which is limited to compulsion, § 136a StPO also prohibits obtaining incriminating statements from defendants through deceit. German courts, however, interpret "deceit" in a restrictive way. In their view, deceit must be equivalent to the other prohibited measures listed in § 136a StPO, such as torture. Measures under § 100a and § 100c StPO and the use of fake identification by undercover agents do not amount to this level of seriousness. Moreover, § 136a StPO applies only to interrogations not to measures that imply only passive listening.[1598]

In China, suspects were for a long time obliged to tell the truth during interrogations. The *CCPL* of 2012 was the first piece of Chinese legislation to incorporate the rule that "no one may be compelled to incriminate himself". Although this is only an evidentiary rule, not a general principle of criminal procedure law, it is still regarded as a huge progress in the protection of human rights in China. Torture, threats, inducement, deceit, and other illegal measures are prohibited in interrogations. This

[1597] See Section 6. a), Chapter I, Part I.

[1598] See Section 3. a) bb), Chapter IV, Part II.

provision, however, is mainly discussed in the context of confessions, not of TIMs because it applies only to formal interrogations.

b) Attorney-client Privilege

The attorney-client privilege is regarded as a corollary of the right to counsel because a lawyer is unable to offer his client a professional service without the privacy of communication.[1599] Governmental attempts to eavesdrop on privileged communications between lawyers and clients, either through electronic interception or through an undercover agent/informer, are regarded as a violation of this privilege. In the U.S., however, the two-pronged test of "reasonable expectation of privacy" decides on whether a lawyer and his client enjoy the privilege. Communications in the presence of third parties are generally not protected by the attorney-client privilege. The client and his lawyer thus take the risk that the information will be leaked when they allow a person who is not a member of the defense team to be present.

In Germany, the lawyer-client privilege is mainly protected by §§ 53, 148 I and 160a I StPO. Certain professionals, including lawyers, are free from interception when they communicate with their clients for professional purposes. When a conversation that should be free from interception begins, surveillance should be terminated or interrupted.[1600] Exceptions relate to terrorist-related crime and to situations in which lawyers are themselves suspected of crime.[1601]

In China, Article 38 of the *Law on Lawyers* obligates lawyers to maintain the privacy of their clients and to keep all their information confidential,[1602] unless this obligation has been waived. The *CCPL* does not grant defense lawyers the right to refuse to testify. It is not clear whether lawyers are obliged to actively inform public institutions of wrongdoing, or whether they have no obligation to keep their client's information private in situations provided for in the second paragraph of Art. 38 of the *Law on Lawyers.* Since Art. 38 is an obligation as opposed to a privilege or a right, it is unclear whether lawyers may refuse to disclose clients' information to the government. Rules referring to TIMs in the *CCPL* do not grant any special protection to communications between lawyers and clients. Therefore, such communications

[1599] *Friedman*, Washington University Journal of Urban and Contemporary Law 40 (1991), 109, 110.

[1600] *Werle*, JZ 1991, 482, 487.

[1601] See Section 2. c) cc), Chapter I, Part II.

[1602] Art. 38 of *Chinese Law on Lawyers:* "A lawyer shall keep the national secrets and trade secrets known in practicing law, and shall not divulge any privacy of a client."

"A lawyer shall keep confidential the relevant condition and information that is known by the lawyer in practicing law and the client and other persons are reluctant to disclose, however, except facts and information on a crime compromising the national security or public security or seriously endangering the safety of the body of a person, which a client or other person prepares to commit or is committing."

can be intercepted in the same way as other communications if the requirements for the TIM are met. In an online survey of three policemen, all three avoided answering the question of whether TIMs can be used to record the communication between lawyers and clients. This collective silence suggests that the police consider this to be a sensitive issue and do not wish to discuss this matter in public for fear of provoking protest from the legal profession.[1603] In an interview with another policeman, he said that there is no special treatment for lawyers.[1604] In practice, most suspects only get a lawyer after they have been taken into custody. In the past, police officers were present in meetings between lawyers and their clients when they were in custody. That practice has been abandoned. As a general practice nowadays, no recording can be made during a meeting between a lawyer and his/her client, but the police can observe the meeting from outside the visiting room; the police may film the conversation but must not record the words spoken.

Lawyers in China are in a weaker position than public institutions. There is a low rate of legal representation in criminal proceedings, the lawyer's right to visit his client in custody is often ignored by the police, and the attorney-client privilege is not officially recognized. A greater effort is needed to promote an effective defense in China.

III. Procedure

All three jurisdictions are in agreement that electronic surveillance infringes upon constitutional rights and should be used with restraint. In the U.S., courts emphasize that surveillance should be the "last resort", while provisions for surveillance in the StPO include subsidiarity clauses, requiring that surveillance measures can only take place if the investigation by other means "would be disproportionally difficult or futile". In China, although the phrase "last resort" is not expressly mentioned in legislation, the *CCPL* provides the most restrictive criteria for the adoption of TIMs compared to other investigative measures. In legal literature, it is also commonly recognized that such measures should only be used as a last resort. Given this consideration, various procedural guarantees are provided in legislation to restrict the use of such surveillance measures and to protect the right to privacy.

1. The Preeminence of the Police in Cases involving Surveillance

In practice, the police dominate investigative activities, especially in the implementation of surveillance, in all three jurisdictions. In the U.S. and Germany, judges issue warrants, however, they mainly rely upon the information filed by the

[1603] See Section 8, Chapter III, Part III.

[1604] Interview with Mr. Wu, a policeman in Guangdong Province, China.

police to make their decisions. Judges do not collect information by themselves, and even if they could check the reliability of the information presented by police, they might not be motivated to do so. The preeminent position of the police in cases involving surveillance is even more apparent in China because there is no judicial control and directors of police stations at city level or above are authorized to issue warrants. Moreover, the policemen who conduct surveillance play an important role in the termination and extension of surveillance warrants. In the U.S., police reports on the progress of the surveillance are checked by judges to determine whether the minimization requirement has been met. In China, the personnel in TIM departments do not normally hand over the original tapes to investigators, instead they only pass on what they deem to be useful information. This requires TIM personnel to know exactly what information is needed by the investigation staff and what information should be deleted due to concerns for privacy.

2. Warrants and Judicial Control

In the U.S. and Germany, if a surveillance warrant is needed, it can only be issued by a judge. In an emergency situation, the prosecutor may order surveillance, but it has to be confirmed afterwards by a judicial warrant. At the Federal level in the U.S., 18 U.S. Code § 2516(1) provides a centralized authorization system. The Office of the Attorney General is the only authority that can apply for a surveillance warrant by a competent federal judge. The judge reviews the application materials and decides whether a warrant should be issued in accordance with § 2518(3).

In Germany, the jurisdiction of the issuing court for a judicial order differs between telecommunication surveillance and acoustic surveillance of the home. Investigation judges are in principle in charge of issuing judicial orders for prosecutors whose offices are located in their jurisdiction. The same rule applies to surveillance outside of a "home" in accordance with § 100f IV StPO. § 100e II StPO provides that only a special criminal chamber of the District Court of the city in which the Regional Appellate Court is situated has jurisdiction to approve an order for the acoustic surveillance of a home.

In China, as mentioned above, there is no judicial control over surveillance warrants. Such warrants are issued by the director of police stations at city level or above, while warrants to investigate duty-related crimes are issued by supervision committees. The approval process takes the form of an administrative, not a judicial review.

3. The Legislative Requirements for a Warrant

18 U.S. Code § 2518 provides details on the findings that should be made before a surveillance warrant is issued. The corresponding provision in Germany is § 100e III StPO. In China, Art. 256 of the *Procedures for Criminal Cases* 2020 requires that "a report" should be submitted when applying for a warrant. What should be included in this report is not specified; no further information can be found in the *CCPL*. Only samples of previous surveillance warrants shed any light on this issue.

In application materials and warrants, the following information is required in all three jurisdictions: the name of persons to be intercepted, the crimes involved, the locations where communications take place, the type of the investigative measure, and the duration of the measure. Legislation in the U.S. and Germany requires probable cause or sufficient evidence to be included in the application to justify the necessity of surveillance. For instance, in the U.S., § 2518(3) requires judges to establish that there is probable cause that a crime has been committed or is taking place, that incriminating communications will be intercepted, that interception is the "last resort", and that the location of the interception is used by the suspect in question.

A minimization requirement applies to surveillance warrants in the U.S. In addition, § 2518(6) provides that a warrant may require reports on the progress of surveillance to be made to the issuing judge. These requirements have an impact on the admissibility at trial of evidence obtained from surveillance.[1605]

In Germany, issuing courts can require the prosecution office to submit more information at any time during the surveillance so that they can examine the necessity of further surveillance.

Both the U.S. and Germany grant issuing judges the authority to supervise and control the process of surveillance. Judges can require the police or prosecutors to submit reports and further information. This practice enhances the transparency of surveillance and makes the evidence from surveillance more compelling at trial.

4. Other Issues Influencing the Issuing of Warrants

In each jurisdiction, certain issues may be taken into consideration on the question of whether a warrant for surveillance should be issued.

In the U.S., due to the minimization requirement, surveillance is often conducted in real time. This means that a police officer listens to the intercepted communication while it is being recorded in order to "minimize the interception of communications not otherwise subject to interception" (18 U.S. Code § 2518(5)). This practice takes up a lot of judicial and financial resources. Given their limited budgets and human

[1605] See Section 2. c) cc), Chapter IV, Part I.

resources, officials must be highly selective in choosing cases for surveillance. Even if a warrant has been issued, surveillance is sometimes not conducted.[1606] Since a violation of the minimization requirement is grounds for excluding evidence, tape recordings cannot be edited afterwards. Defense lawyers may request to listen to the tapes to check whether the minimization requirement was violated.

By contrast, in Germany and China communications are recorded first and then the police listen to the tapes and decide which parts of the recordings are crime-related. Irrelevant material must be deleted within a reasonable period. This practice is much cheaper than real-time surveillance. Therefore, cost is not taken into consideration when warrants are implemented.

In China, although surveillance warrants are approved from within the police system, the process is not simpler than with judicial control. There are independent departments (TIM departments) within city level police stations, which are responsible for the implementation of TIMs. The technical feasibility of the measures must be examined by this department before a warrant is issued by the director of the police station. Investigators in charge of cases need to wait for feedback from the TIM department. This can take a long time and outcomes are not always satisfactory, since the personnel of TIM departments might not know exactly what information is needed or relevant. Given this situation, investigators are hesitant to apply for TIMs and instead prefer measures that they can take by themselves.

5. The Last Resort vs. Subsidiarity Principle

Judges in the U.S. first need to determine whether all other investigative measures are inadequate in accordance with 18 U.S. Code § 2518(1)(c). Surveillance measures cannot be undertaken if "traditional investigative techniques would suffice to expose the crime." The legislation regards such measures as the "last resort". However, given the strong position and experience of the police regarding investigative issues, judges are hesitant, without solid grounds, to challenge claims made by law enforcement officers that all other alternatives have been exhausted. Therefore, the judicial review of the "last resort" question does not always lead to a satisfactory outcome.

Instead of providing a "last resort" clause for surveillance measures, the German StPO uses a system called "Subsidiaritätsklauseln", consisting of different levels of subsidiarity for different investigative measures. While the term "last resort" is singular, the German word "Subsidiaritätsklauseln" refers to more than one clause or measure.[1607] This system is just as wearisome and frustrating as the "last resort" solution, due to its complexity and ambiguous distinctions between different subsidiary clauses.[1608] The "last resort" and subsidiary clauses emphasize that surveil-

[1606] See Section 2, Chapter VI, Part I.

[1607] See Section 2. f), Chapter I, Part II.

[1608] BGH 41, 34.

lance measures should be employed with great caution. In practice, however, neither system can effectively restrict the arbitrary use of surveillance measures.

In China, the CCPL emphasizes that TIMs are only allowed after being approved in a strict review process. This kind of review phase is not provided for other measures. It functions in a similar way as the "last resort" issue and demonstrates the seriousness of TIMs. In addition, due to the design of TIM departments, TIMs have the strictest procedural control among all measures that can be approved by the police.

6. Mechanisms to Enhance Transparency

Surveillance measures are, by their very nature, covert measures. This does not mean, however, that such measures are free from external control and remain covert forever. Their covertness mainly serves the effectiveness of the investigation. After the investigation has been concluded, the necessity for them to remain secret vanishes to a large degree. At trial, demands on transparency increase and the rights of defense should be prioritized. Although some considerations, such as the safety of undercover agents, can still prevent a full disclosure, information regarding surveillance measures should be disclosed as much as possible. Several mechanisms have been introduced to guarantee transparency.

The foremost procedural guarantee of transparency is the warrant requirement. It ensures that such measures cannot be imposed simply by any individual police officer. In addition, once a warrant has been issued, it must be entered into the case file. The comprehensive details included in warrants ensure the transparency of the investigative activities. In the U.S. and Germany, warrants along with the results of surveillance go into the case file and can later be reviewed by defense lawyers, who can glean a great deal of information from warrants.

In China, warrants must be kept within "investigative files", but they can be hidden from prosecutors, judges, and the defense if the information obtained from such measures is not deemed relevant or is not needed at trial. For instance, if other stronger evidence is found or other evidence is already sufficient, the police prefer not to reveal the fact that TIMs have been carried out. The warrant requirement in China nevertheless provides a possibility of further transparency. In the case of future reform, the legislature could require the police to hand over the investigative files to prosecutors and judges.

In the U.S. and Germany, notice of the implementation of surveillance must be given to the persons concerned after surveillance has finished. In the U.S., notice is also required if the application for surveillance was denied by the court (18 U.S. Code § 2518(8)(d)). This ensures that the affected persons are made aware of the measures and can seek a remedy. Only if defendants have been informed of the use of such

measures before trial can evidence obtained through surveillance be used against them at trial.

Both American and German legislation grants the issuing judge the authority to supervise and control the implementation of surveillance. Issuing courts in both jurisdictions can require the prosecution office to submit necessary information or reports at any time during surveillance for the purpose of examining the necessity of further surveillance. U.S. federal judges can make this stipulation a direct requirement. All such reports can be found in the case file, so the defense can be aware of what has occurred during the surveillance.

The *CCPL* 2012 has improved the transparency of TIMs. It allows information from such measures to be used as evidence at trial. The *Explanation of the Application of the CCPL* (2021) makes a further contribution to enhancing transparency, for example, it requires TIM evidence to be handed over to courts in order to be admitted. Although such rules still do not resolve the problem that police do not use TIM information directly as evidence and thus hide them from prosecutors, judges and defense lawyers, new evidentiary rules in the *CCPL* and the *Explanation of the Application of the CCPL* (2021) have opened the door for further reform to improve transparency. The compulsory handing-over of the warrant, the giving of notice to affected persons, and regular reports on the progress of surveillance are changes that could be considered by the Chinese legislature in the future.

IV. The Exclusionary Rule

The exclusionary rule reflects some of the fundamental values of modern criminal procedure, such as human dignity, truth-finding, and fairness.[1609] Although the provisions for the exclusionary rule in the three jurisdictions reflect these different values to different degrees, they share common solutions for extreme cases where basic human values have been seriously infringed upon. For example, confessions extracted through torture are excluded in all three jurisdictions,[1610] because torture violates human dignity and cannot be tolerated by modern criminal procedure under the rule of law.

In most regards, however, the scope and content of the exclusionary rule vary widely across the three jurisdictions,[1611] and solutions are not always as clear-cut as in the situation of torture. The values of human dignity, truth-finding and fairness often seem to come into conflict when the issue of excluding evidence is discussed. This creates challenges, not only for judges but also for legislatures. The exclusionary rule

[1609] *Lippke*, in: Brown et al. (ed.), The Oxford Handbook of Criminal Process, 26 ff.

[1610] *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 256.

[1611] *Ibid.*

is therefore one of the most controversial topics in criminal procedural law in all three jurisdictions.[1612]

1. The Role of the Courts

In each jurisdiction, the development of the exclusionary rule followed a different path. The exclusionary rule in the U.S. is a judge-made remedy to enforce the 4th Amendment, rather than a remedy guaranteed by the 4th Amendment itself.[1613] Consequently, the courts, especially the U.S. Supreme Court, play a dominant role in interpreting the exclusionary rule. Through a series of landmark cases, such as *Weeks*, *Mapp* and *Wolf v. Colorado*, the U.S. Supreme Court in the 1960s developed and firmly established the exclusionary rule as well as the "fruit of the poisonous tree" doctrine.[1614] This period is referred to as the "high-water mark" of the exclusionary rule.[1615] In the 1970s, however, the Burger Court began to limit the exclusion of illegally obtained evidence. The Court reduced the group of individuals who may move for the suppression of evidence[1616], noted the high social cost of the exclusionary rule, acknowledged the risk of letting criminals go free,[1617] and recognized the negative effect of exclusion of evidence on truth-finding.[1618] In addition, the Burger Court introduced the inevitable discovery exception[1619] and the good faith exception[1620] to the exclusionary rule. The Rehnquist Court further expanded the application of the good faith exception.[1621] In 2006, the Court declared that the "suppression of evidence, however, has always been our last resort, not our first impulse."[1622] Since the end of the 20th Century, the Supreme Court has become very hesitant to apply the exclusionary rule and restricted its application due to its high social cost and its negative impact on truth-finding.[1623]

[1612] *Hsieh*, The Exclusionary rule of Evidence, 2014, 49.

[1613] *United States v. Calandra*, 414 U.S. 338 (1974).

[1614] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, Chapter 6; *Cammack*, in: Thaman (ed.), Exclusionary Rules in Comparative Law, 2013, 8–13.

[1615] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 186.

[1616] *Id.* at 187.

[1617] *Illinois v. Gates*, 462 U.S. 213 (1983) ("We will never know how many guilty defendants go free as a result of the rule's operation.").

[1618] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 196.

[1619] *Nix v. Williams*, 467 U.S. 431 (1984).

[1620] *United States v. Leon*, 468 U.S. 897 (1984); *Massachusetts v. Sheppard*, 468 U.S. 981 (1984).

[1621] *Illinois v. Krull*, 480 U.S. 340 (1987); Maryland v. Garrison, 480 U.S. 79 (1987); *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 206–208.

[1622] *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)

[1623] *Cammack*, in: Thaman (ed.), Exclusionary Rules in Comparative Law, 2013, 32; *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 260.

The German courts have less discretion when there is a "written exclusionary rule" ("geschriebenes Beweisverbot"), but especially the BGH and the BVerfG play a crucial role in issues relating to "unwritten exclusionary rules" ("ungeschriebene Beweisverbote"). Moreover, the BVerfG can impose exclusion of evidence based directly on GG. The "core area of privacy" doctrine is a good example of the protection of constitutional rights by excluding evidence. In addition, German courts rely on the "Rechtskreis" theory, the "protective purpose" theory and the balance of interests theory to support their decisions on excluding evidence. Unlike the U.S. Supreme Court, who adopted an extensive exclusionary rule only to then limit its application, German courts initially refrained from establishing a general rule of excluding illegally obtained evidence, declaring that police misconduct does not automatically lead to the exclusion of evidence. The "fruit of the poisonous tree" principle was ultimately rejected by German courts.[1624] German courts maintain a cautious attitude toward the exclusion of evidence and emphasize the negative impact of exclusion on truth-finding and the effectiveness of the criminal process.

As mentioned above, the Chinese Supreme Court has made a great contribution to the development of the exclusionary rule, both in practice and in theory. Given their weak status in the judicial system, however, Chinese courts, especially the lower courts, still tend not to challenge the evidence presented by the police or prosecutors, except when there are strong indications that the evidence is unreliable. Chinese courts rarely exclude evidence merely on the grounds that the evidence was obtained through illegal measures.

From a procedural perspective, judges in Germany and China dominate the review of evidence at trial. Evidence at trial is not limited to that which is presented by the prosecution or the defense. Judges can present new evidence on their own initiative. By contrast, the scope of the evidence at trial in the U.S. is largely constrained by the materials submitted by the prosecution and defense. Judges respect the autonomy of both parties and do not pursue evidence that has not been presented.

2. The Function and Purpose of the Exclusionary Rule

Across the three legal jurisdictions, the exclusionary rule follows different rationales.[1625]

a) Deterring Police Misconduct

Excluding evidence with the aim of deterring police misconduct assumes that the police behave legally if they know that it is in their best interest to do so. The police

[1624] See Section 4, Chapter IV, Part II.

[1625] *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 256.

must be discouraged from using illegal methods to obtain evidence by depriving them of any advantages that might be derived from such evidence.[1626] The U.S. Supreme Court refrained from proclaiming the exclusion of evidence to be a constitutional right[1627] and regards the deterrence rationale as the sole purpose and function of the exclusionary rule.[1628] However, the Court has become increasingly skeptical about the exclusionary rule and has suggested various alternative remedies which could also deter the police from gathering illegal evidence whilst still serving the interests of fighting crime.[1629] Pursuing the goal of restricting the application of the exclusionary rule, the Supreme Court has limited its use to cases in which it is likely to deter police from violating procedural rules.

Empirical studies have shown, however, that the deterrent effect of the exclusion of evidence on police behavior is low.[1630] This is obvious if the misconduct of the police was not motivated by the desire to collect incriminating evidence but, for example, by wishing to humiliate a suspect through torture.[1631] As early as in 1983, an empirical study of data from California found that non-prosecutions and/or non-convictions based on the exclusion of evidence were "in the range of 0.6 % to 2.35 %" for all felony arrests.[1632] Prosecutors rejected only 0.8 % of felony arrest cases because of illegal searches. The rate was even lower for violent crimes.[1633] These findings were confirmed by another empirical study which analyzed 7500 cases in three different counties.[1634] Both studies support the conclusion that the exclusionary rule has only a marginal impact on prosecutions and convictions.[1635]

[1626] *Hsieh*, The Exclusionary rule of Evidence, 2014, 42.

[1627] *United States v. Calandra*, 414 U.S. 338, 348 (1974) ("the rule (the exclusionary rule) is a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved.") (Powell, J.); *Maclin*, The Supreme Court and the Fourth Amendment's Exclusionary Rule, 2012, 149, 305.

[1628] *Bivens v. Six Unknown Federal Narcotics Agents*, 403 U.S. 388 (1971); *Lippman*, Criminal Procedure, 2020, 386; *Bradley*, Beweisverbote in den US und in Deutschland, GA 1985, 99, 101.

[1629] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 194; *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 260; *Hudson v. Michigan*, 547 U.S., 599.

[1630] *Alschuler*, University of Chicago L. Rev. 75 (2008), 1365, 1374.

[1631] *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 260.

[1632] Davies,American Bar Foundation Research Journal 8 (1983), 611, 621.

[1633] *Id.* at 611.

[1634] *Nardulli*, American Bar Foundation Research Journal 8 (1983), 585.

[1635] *Lippman*, Criminal Procedure, 2020, 413.

The deterrence doctrine plays only a marginal role in Germany[1636] and China. In both jurisdictions, legal professionals are concerned by its detrimental impact on truth-finding and crime-fighting.

b) Truth-finding

Due to the emphasis on truth-finding in Germany, the relationship between the exclusionary rule and truth-finding must be understood from two different perspectives. Unreliable evidence should be excluded to prevent such evidence from impeding truth-finding,[1637] but this does not explain why reliable evidence, such as illegally obtained wiretaps, should also be excluded in some cases.[1638] The second perspective emphasizes that finding the truth is not the only objective of the criminal process and that the truth must not be sought at any cost.[1639] The exclusionary rule thus establishes external limits on truth-finding.[1640] The BGH has declared that the exclusion of evidence is not dependent upon its reliability.[1641]

The rationale behind § 136a StPO can be regarded as a combination of these two perspectives. Some methods prohibited by § 136a StPO can easily lead to unreliable evidence, such as confessions obtained through torture.[1642] Some methods prohibited by § 136a StPO, such as obtaining statements by deceit, however, can produce relatively reliable evidence which still must be excluded.[1643] This shows that § 136a StPO mainly serves to protect human rights.[1644] In the context of technological surveillance, evidence is normally reliable. Therefore, exclusion here is based on this second perspective.

The emphasis on truth-finding, as opposed to procedural values, can also be traced back to the imperial period of Chinese law. Even today, truth-finding is the main priority of Chinese courts, particularly when deciding whether to exclude evidence. This can be seen in Arts. 1 and 2 of the *CCPL*. Reliable evidence is rarely excluded, especially if the evidence is necessary to convict defendants. Secret tape recordings and videos are normally deemed to be more reliable than confessions. Even if judges

---

[1636] *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 260; *Brandis*, Beweisverbote als Beweislastungsverbote, 2001, S. 44 ff.

[1637] *Correa Robles*, Die Fernwirkung, 2018, S. 29; *Schröder*, Beweisverwertungsverbote, 1992, S. 26.

[1638] *Schröder*, Beweisverwertungsverbote, 1992, S. 27.

[1639] *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 329.

[1640] *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 329; *Schilling*, Illegal Beweise, 2004, S. 150 ff.

[1641] BGH 5, 332, 333.

[1642] *Brandis*, Beweisverbote als Beweislastungsverbote, 2001, S. 38.

[1643] *Brandis*, Beweisverbote als Beweislastungsverbote, 2001, S. 39.

[1644] *Schröder*, Beweisverwertungsverbote, 1992, S. 31.

find that TIM evidence has been obtained illegally, they normally just ask for a correction and then admit the tape.

c) Human Rights

The second perspective mentioned above shows that other values should also be considered in the process of truth-finding.[1645] The most frequently discussed value in legal literature is human rights. The exclusionary rule is an effective remedy for defendants if their rights have been violated. The U.S. Supreme Court regards the exclusionary rule as a tool for enforcing the 4th Amendment and protecting constitutional rights.

After World War II, human rights were promoted by international courts and international conventions such as the ICCPR. The international requirements for a fair trial, the right to privacy, and the right not to be compelled to incriminate oneself provide guidelines for domestic legal systems to adopt procedural guarantees.[1646] The exclusionary rule is one option to enforce these guarantees.

In Germany, the goal of protecting individual rights as a function of the exclusionary rule was first articulated by Rogall.[1647] According to Rogall, the exclusionary rule aims at protecting fundamental rights and enables the individual to defend against improper state interference.[1648] This view has gained support, especially with regard to exclusion under § 136a of StPO and the "core area of privacy" doctrine.[1649]

The exclusionary rule's impact on the protection of human rights, however, is somewhat indirect, in the same way as deterrence. Supporters of both the human rights and deterrence doctrines focus on the effect of the exclusionary rule for the future, because the violation of human rights cannot be erased *ex post facto* through the exclusion of evidence.[1650] The protection of human rights through the exclusionary rule can only be brought about through changing police behavior, in a similar way as under the deterrence doctrine.[1651]

The human rights doctrine does not resolve the potential conflict between truth-finding and the protection of human rights. Given that the exclusionary rule has only an indirect effect on human rights, it is difficult to establish the degree to which

[1645] BGH 14, 365; 31, 308.

[1646] *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 261.

[1647] *Rogall*, ZStW 91, 1979, 1.

[1648] *Rogall*, ZStW 91, 1979, 1, 17 ff.

[1649] *Correa Robles*, Die Fernwirkung, 2018, S. 41; *Schröder*, Beweisverwertungsverbote, 1992, 33; *Eisenberg*, Beweisrecht der StPO, 2017, Rn. 330 ff.

[1650] *Dencker*, Verwertungsverbote im Strafprozess, 1977, S. 88; *Amelung*, Informationsbeherrschungsrechte, 1990, S. 24.

[1651] *Turner/Weigend*, in: Gless/Richter (ed.), Do Exclusionary Rules Ensure a Fair Trial?, 2019, 262.

human rights should be allowed to compromise the purpose of truth-finding. This dispute is of utmost importance when courts need to decide whether illegally obtained but reliable evidence should be excluded.

3. Theories relating to the Exclusionary Rule

a) Balancing Theory

In Germany, the balancing theory plays an important role when courts decide whether to exclude evidence, especially since the violation of a "Beweiserhebungsverbot" does not automatically lead to a "Beweisverwertungsverbot". German courts are called upon to balance the interests of the public against the rights of the individual in each case. Even if evidence is excluded it can often still be employed as a lead for further investigation. Since the 1970s, the U.S. Supreme Court also has often employed a balancing theory. In *Calandra*, the Court used a cost-benefit analysis to decide on the exclusion of evidence. In terms of "cost", the U.S. Supreme Court considers various social costs, such as the risk of allowing criminals go to free,[1652] of wasting judicial resources, of imposing obstacles to truth-finding, and of promoting disrespect for the law.[1653] In terms of benefits, the court considers the deterrent effect on illegal police activities, which is more abstract and hence more difficult to evaluate. Therefore, the Court has often found that the application of the exclusionary rule is inappropriate because the potential cost of excluding evidence is deemed to be high, while the deterrent effect is seen to be limited.[1654]

b) "Protective Purpose" Theory

Instead of recognizing the "protective purpose" approach as an independent theory in Germany, the U.S. Supreme Court reasoned that this argument was based on the balancing theory.[1655] When the use of illegally obtained evidence has no further detrimental cost, there is no good reason to exclude it.

[1652] *United States v. Leon*, 468 U.S. 897, 907 (1984).

[1653] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 196; *United States v. Calandra*, 414 U.S. 338, 352 (1974).

[1654] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 195; *Stone v. Powell*, 428 U.S. 465 (1976). The application of the balancing theory to the exclusion of evidence has gained support in the legal literature. For an analysis from an economic perspective see *Simmons*, Smart Surveillance: How to Interpret the Fourth Amendment in the Twenty-First Century, 2019, 14.

[1655] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 195.

c) Inevitable Discovery Rule

The inevitable discovery rule as applied by U.S. courts is an exception to the exclusion of evidence from illegal searches or seizures. The rule allows the court to admit evidence from illegal searches or seizures if law enforcement officers can prove that the evidence would have been inevitably discovered legally.[1656] This rule was first discussed by the U.S. Supreme Court in *Nix v. Williams*, where the defendant Williams was interrogated in violation of his right to counsel and as a consequence of his interrogation the body of the victim was discovered. Since the search team looking for the body were not far from its location,[1657] the Supreme Court assumed that the body would have been inevitably found within three to five hours even if Williams had not cooperated with the police.[1658]

German courts and scholars have developed the "hypothetische Ermittlungsverläufe" theory, which is similar to the inevitable discovery rule.[1659] In the German legal context, "hypothetische Ermittlungsverläufe" means that if a piece of evidence could have been obtained legally it can be admitted even though it was obtained illegally.[1660]

Both theories justify the admission of evidence resulting from police misconduct through a hypothetical thought process. However, the theories are applied with a different level of vigor in the two jurisdictions. The "hypothetische Ermittlungsverläufe" theory in Germany is applied in most cases as one factor to be balanced against other factors and is rarely used independently as grounds for admitting illegally obtained evidence.[1661] The inevitable discovery rule in the U.S. is applied as an independent exception to the exclusionary rule, in a similar way as the good faith or independent source exceptions. Its application can also be regarded as a consequence of the intent to restrict the use of the deterrence doctrine.[1662] In addition, U.S. courts apply the inevitable discovery rule whenever its conditions are met,[1663] whereas German courts only apply the "hypothetische Ermittlungsverläufe" theory with great restraint.[1664] One problem with "hypothetische Ermittlungsverläufe" is that discussions of this issue remain very abstract in Germany.[1665] Some courts have introduced the notion of "hypothetische Ermittlungsverläufe" even where the police did not make any effort to collect evidence legally, based on a mere possibility that

[1656] *Lippman*, Criminal Procedure, 2020, 409.
[1657] *Nix v. Williams*, 467 U.S. 431 (1984).
[1658] *Nix v. Williams*, 467 U.S., 448.
[1659] *Ossenberg*, Die Fernwirkung, 2011, S. 186 ff.
[1660] See Section 2. c), Chapter IV, Part II.
[1661] *Jahn/Dallmeyer*, NStZ 2005, 297, 301.
[1662] *Cammack*, in: Thaman (ed.), Exclusionary Rules in Comparative Law, 2013, 16.
[1663] *Ossenberg*, Die Fernwirkung, 2011, S. 189.
[1664] *Jahn/Dallmeyer*, NStZ 2005, 297, 301.
[1665] *Schröder*, Beweisverwertungsverbote, 1992, S. 112 ff.

the evidence could have been obtained legally.[1666] For example, in a case decided by the BGH[1667] police offers searched the suspect's house upon an emergency order issued by the prosecutor, who had not made any effort to reach the judge but immediately had issued the emergency order. The BGH declared the evidence found in the suspect's home to be admissible because a judicial warrant could have been issued in advance and the search was not conducted arbitrarily.

U.S. courts have established more concrete standards for the inevitable discovery rule. The prosecution must prove that an independent, lawful investigative measure was on its way and that the legal measure would have inevitably led to the same evidence as found through the illegal search.[1668] U.S. courts are divided over whether the inevitable discovery rule requires that a legal investigative measure must have taken place or at least have been attempted before the illegal measure was adopted. In *U.S. v. Griffin*[1669] and *Murray v. U.S.*,[1670] the U.S. Supreme Court discussed whether the effort of the police to obtain a warrant at the time of the illegal search or after the search should be considered when applying the inevitable discovery rule.[1671]

In both jurisdictions, these theories have been criticized because of their possible undermining of "Richtervorbehalt". They also ignore factual violations and may lead to uncertain outcomes.[1672] In addition, they might encourage the police to use illegal methods to fast-track the investigation even when legal methods are available to them.[1673]

No clear theories have yet developed in China in regard of the exclusionary rule. Art. 123 of the *Explanation of the Application of the CCPL* (2021) provides an absolute exclusion of confessions brought by torture or threats, while a relative exclusion of documents and physical evidence is prescribed in Art. 126. In practice, courts usually apply a balancing theory. They mainly consider the reliability of the evidence and the effect of excluding evidence on the chances of conviction. They exclude evidence obtained through illegal measures only in extreme cases, such as the situation described in Art. 123 of the *Explanation of the Application of the CCPL* (2021).

[1666] *Fezer*, NStZ 2003, 625, 629 f.; *Jahn/Dallmeyer*, NStZ 2005, 297, 301.

[1667] BGH NStZ 2004, 449, 450.

[1668] *LaFave* et al., Criminal Procedure, 2020, § 9.3(e).

[1669] *U.S. v. Griffin*, 502 F.2d 959 (6th Cir. 1974). In this case, one agent went to judge to get a warrant and meanwhile his other colleagues went to search without a warrant.

[1670] *Murray v. United States*, 487 U.S. 533 (1988).

[1671] *LaFave* et al., Criminal Procedure, 2020, § 9.3(e).

[1672] *Jahn/Dallmeyer*, NStZ 2005, 297, 303; *Ambos*, Beweisverwertungsverbote, 2010, S. 135 ff.; *Lippman*, Criminal Procedure, 2020, 409.

[1673] *Alschuler*, Iowa L. Rev. 93 (2008), 1741; *Schröder*, Beweisverwertungsverbote, 1992, S. 113 ff.

4. Grounds for Excluding Surveillance Evidence

In the U.S. and Germany, the grounds for excluding evidence need to be understood at the constitutional and the statutory level. The constitutional level has been discussed in some detail in Section 1, Chapter I of this Part. The U.S. Supreme Court excludes evidence obtained without a warrant if the act of the police constitutes a search or seizure under the "reasonable expectation of privacy" doctrine. Since the surveillance of wire and some oral communications is deemed to constitute a search, a warrant is required except in specified situations. German Courts have developed the "core area of privacy" and the *nemo-tenetur* principle from the protection of human dignity and the general personality right guaranteed by the GG. If evidence falls within the "core area of privacy" or investigative activities violate the *nemo tenetur* principle, the evidence is to be excluded. In other cases, the exclusion of evidence is subject to the balancing of interests.

At the statutory level, German and U.S. laws have similar "central provisions", such as the requirement for a judicial warrant, a catalogue of crimes, a requirement of probable cause or sufficient facts to justify a warrant, and a duration requirement. *Title III* in the U.S. provides detailed procedural requirements for a surveillance warrant. Regarding the exclusion of evidence, the U.S. Supreme Court has held that if investigative activities violated a rule which "is intended to play a central role in the statutory scheme", the evidence must be excluded. This practice is similar to the case law of the BGH, which differentiates between material and formal preconditions of a warrant. American courts, however, interpret most provisions in *Title III* as "central provisions" and therefore frequently and proactively exclude evidence, whereas German courts hesitate to do so. From this perspective, the American exclusionary rule is more "powerful" and "stricter" than the German one.[1674] Under the "reasonable expectation of privacy" doctrine, however, the American police have more discretion and do not even need a warrant to enact surveillance in many situations, while judicial orders are generally required in Germany. This contrast in approach is clearly reflected in two examples: in the situation of "plain hearing" and in the recordings made by undercover agents. The fact that judicial control in the U.S. often functions only *ex post facto* might explain that American courts have developed a strong and extensive rule for the exclusion of evidence, concentrating on deterring police from violating the rules.[1675] By contrast, judicial control *ex ante* is more prevalent in Germany.

The practice of excluding illegal evidence is not as effective in China. Exclusion can occur in any phase of a criminal process, from the beginning of an investigation to the trial. In most situations, exclusion decisions are made in a soft way and frequently no explanation is given for abandoning certain evidence. It might simply be that such evidence or information is not useful and would not help the police or prosecutors to

[1674] *Ossenberg*, Die Fernwirkung, 2011, S. 10 ff.

[1675] *Bradley*, GA 1985, 99, 101 ff.

obtain a conviction. Some judgements also mention the unreliability of the evidence as grounds for exclusion. In addition, if the police consider that the evidence has been collected illegally and that it would cause problems at the trial, they tend to refrain from using the evidence. As an alternative, the police employ various strategies to transform "problematic" evidence into more "acceptable" material.

Regarding TIMs, Art. 109 of the *Explanation on the Application of the CCPL* (2021) provides two "compulsory" reasons for the exclusion of audio-visual materials: first, if their reliability cannot be verified, and second if there are doubts regarding the time, location and methods of producing or collecting the evidence.[1676] It is rare that evidence from TIMs is excluded on the grounds of illegality. Due to the limited information regarding the implementation of TIMs included in police files, it is difficult for defense lawyers to challenge and for judges to review the legality of TIMs. The police should be required to submit more information about their applications and the implementation of TIMs.

5. Exceptions

All three jurisdictions provide for exceptional situations where judicial warrants are not required, can be applied for *ex post facto*, or police misconduct can be tolerated.

a) Plain Hearing

U.S. courts make an exemption from the warrant requirement if the police officers are "in a place where they had a right to be and they rely upon their naked ears".[1677] If the police can hear the communication with naked ears, they can record it with an unenhanced sensory device. U.S. courts argue that the process of making a recording in this situation is only a means to preserve the evidence.

In Germany, judicial orders are, in principle, required for the recording of conversations, including non-public conversations in a public area, regardless of whether the police have a right to be there or whether they can hear the conversation with naked ears. Only public conversations can be recorded without an order. A plain hearing exception for recordings is thus not recognized in Germany.

In China, there is no case law or legislation which regulates whether the police can record what they hear without a warrant. In some places, especially in affluent cities, police are required to wear body-cameras when on duty. The original purpose of these cameras was to deter the abuse of police power and to encourage police officers to act in accordance with the law. Yet, if one of these cameras were to record a member of

[1676] See Section 11, Chapter V, Part III.

[1677] *United States v. Fisch*, 474 F.2d 1071, 1076 (9th Cir. 1973).

the public behaving illegally, or record a conversation pertaining to criminal activities, these recordings could be used as evidence in a criminal proceeding.

b) Consent Surveillance

Another important exception from the warrant requirement in the U.S. is consent to surveillance. It refers to a situation that a person either is a party to a conversation or has obtained the consent to record the conversation from one of the parties involved. In either case, that person may record the communication without acquiring the agreement of all parties. This rule was first established by the U.S. Supreme Court, based on its interpretation of the "reasonable expectation of privacy": Once a person shares information with others in a communication, he accepts the risk that the information will be recorded.

Based on the logic discussed in Section 5. a) of this Chapter, German police must obtain a judicial order for recording communications even if they are participating in those communications, unless they have the consent of all parties. The American understanding of consent surveillance does not exist in Germany.

c) Emergency Situations

U.S. and German laws agree that in emergency situations a warrant can be applied *ex post facto*, but both jurisdictions have a cautious attitude towards that option. In the U.S., courts require that the situation must be sufficiently urgent to justify an emergency warrant. In an emergency, an application for a judicial warrant can be made within 48 hours after the interception took place. Warrant exceptions for emergency situations have, nevertheless, been criticized in the U.S. because of possible abuses of power. Yet in practice, this has not become a systematic problem because law enforcement officers use this exception sparingly.[1678]

§ 100e I and II StPO provide that "bei Gefahr im Verzug", i. e., if it is important to start surveillance immediately, the prosecutor can issue an "emergency order". Such an order becomes ineffective unless it is confirmed by the court within three working days. The BVerfG has emphasized that the term "emergency" must be interpreted very strictly since it should not undermine judicial control. In search cases, certain elements must be taken into consideration, for example, the amount of time needed to obtain a warrant, whether the exigency was unnecessarily provoked by law enforcement officers, and whether the law enforcement officers attempted to obtain a warrant at the earliest opportunity. In addition, the reasons for the emergency and the

[1678] NWC Report, 1976, 111 – 112.

concrete facts of the case should be put on file.[1679] According to an empirical study, only 12 % of orders on telecommunication surveillance were "emergency orders".[1680]

In China, there is no specific legislation or regulation on the issuance of warrants in emergency situations. This might be because surveillance warrants are issued from within police system, so it is not necessary to provide for shortcuts. If the situation is an emergency, the director of the police station can simply issue the warrant immediately.

d) Good Faith

In the U.S., the good faith exception is not an exception to the requirement of a judicial warrant but to the application of the exclusionary rule. In 1984, "good faith" was recognized as an exception in order to further restrict the application of that rule.[1681] Later, the U.S. Supreme Court expanded the application of this exception[1682] and applied it, e. g., when the police executed a warrant issued by a judge without probable cause,[1683] when police relied on an unconstitutional statute or a precedent which was later overruled,[1684] or when they relied on consent given by a third person who actually did not have authority to give consent.[1685] The good faith exception was also applied when the issuing judge had failed to sign the warrant.[1686]

The good faith exception also plays a role when courts decide on the exclusion of tapes from a surveillance which violated the minimization requirement. As discussed in *Scott v. U.S.*,[1687] if law enforcement officers violate the minimization requirement in good faith, suppression is granted only for conversations that should have been minimized.[1688] The good faith argument is not accepted, however, if a substantial violation of the minimization requirement can be proved, for example, if "a pattern of

[1679] *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung?, 2003, S. 53, 54, 79, 110; *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung, 2003, S. 451.

[1680] See Section 1. c), Chapter III, Part II.

[1681] *United States v. Leon*, 468 U.S. 897 (1984); *Massachusetts v. Sheppard*, 468 U.S. 981 (1984). Compared with Fn. 1620 and the companying texts. Section 5, Chapter V, Part I.

[1682] *Mcinnis*, The Evolution of the Fourth Amendment, 2009, 206.

[1683] For example, *U.S. v. Bourassa*, 2019 WL 5288137.

[1684] For example, *Illinois v. Krull*, 480 U.S. 340 (1987).

[1685] For example, *Illinois v. Rodriguez*, 497 U.S. 177 (1990).

[1686] *U.S. v. Scala*, 388 F. Supp. 2d 396, 403 (S.D. N.Y. 2005). More on the good faith exception can be found in *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.44; *Lippman*, Criminal Procedure, 2020, 402 – 405.

[1687] *Scott v. U.S.*, 436 U.S. 128(1978).

[1688] For example, *U.S. v. Charles*, 213 F.3d 10, 21 – 22 (1st Cir. 2000). See also Section 4. c) aa) (1), Chapter V, Part I.

unlawful interception is established"[1689] or no effort has been made to minimize the interception of pertinent communications.[1690]

In Germany, the issue of police acting in "good faith" ("in gutem Glauben") is one of many issues considered by courts in balancing, but good faith is not regarded as an independent exception to the exclusion of evidence. If the police or the prosecutors operated in good faith but made a mistake,[1691] that fact supports a decision not to exclude evidence. However, the BGH rejected the good faith argument where an undercover agent had intentionally avoided judicial control or had abused the trust of a suspect by recording their conversation without a judicial order.[1692]

The good faith of the police is not mentioned in Chinese legislation or in regulations regarding TIMs, thus Chinese courts have no legal basis for excluding tainted evidence on the ground that the police acted in bad faith. If a police officer acted in "bad faith" to obtain evidence and his behavior is prohibited by law, the evidence can nevertheless be admitted. Chinese courts are unlikely to discuss the "bad faith" of police officers. If the evidence is believed to be reliable, courts tend to admit it. If it is discovered that a police officer obviously acted in "bad faith", he will probably be sanctioned in accordance with police disciplinary rules, which could lead to him being fired. If his act is serious enough to be deemed criminal, the police officer will be investigated and may be charged with a crime.

6. The "Fruit of the Poisonous Tree" vs. the Distance Effect of Exclusion

Motivated by the deterrence doctrine, the U.S. Supreme Court adopted the "fruit of the poisonous tree" doctrine. Under this doctrine, the inadmissibility of direct or primary evidence from illegal searches or seizures also leads to the exclusion of "secondary" or "derivative" evidence. There are exceptions to this rule, some of which overlap with the exceptions for the exclusion of direct evidence, such as the independent source, the inevitable discovery and the attenuated connection rules.[1693] These exceptions were developed by the Supreme Court in order to restrict the scope of the "fruit of the poisonous tree" doctrine. The Supreme Court justifies these exceptions either by denying the existence of a causal link between the direct evidence and the indirect evidence or by arguing that the causal link is too weak.

[1689] *U.S. v. Dorfman*, 542 F. Supp. 345, 394–395 (N.D. Ill. 1982). See also Section 4. c) aa) (1), Chapter V, Part I.

[1690] *State v. Thompson*, 191 Conn. 360, 464 A.2d 799, 812–813 (1983). See also Section 4. c) aa) (1), Chapter V, Part I.

[1691] BGHSt 24, 125, 130. See also *Ossenberg*, Die Fernwirkung, 2011, S. 183 ff.; Section 2. c), Chapter IV, Part II.

[1692] BGHSt 31, 304, 308.

[1693] *Ambos*, Beweisverwertungsverbote, 2010, S. 131 ff.

Whereas the American model is "excluding the fruits of the poisonous tree, with exceptions", the German model is "admitting the fruits of the poisonous tree, with exceptions". German courts generally do not recognize the distant effect of exclusionary rules.[1694] This means that the inadmissibility of direct evidence does not automatically lead to the exclusion of indirect evidence, but the admissibility of derivative evidence is subject to a balancing test in each individual case.[1695]

The different models reflect the different aims and functions of the exclusionary rule in each jurisdiction. As stated above, the U.S. builds its exclusionary rule solely on the deterrence doctrine, whereas German criminal procedure prioritizes truth-finding. The reach of exclusionary rules corresponds with these general priorities. The U.S. Supreme Court has, however, become skeptical as to the deterrent effect of the exclusionary rule and has adopted a balancing theory, restricting the exclusion of evidence. The American application of the exclusionary rule thus approaches the German model.[1696]

7. When to Exclude Evidence

a) United States

The decision to exclude evidence is initiated by a motion to suppress, in most cases filed by defendants.[1697] The administration of the exclusionary rule in the U.S., however, is different from state to state. Motions to suppress evidence can only be filed at the pre-trial hearing or during trial. Although the suspect can also file a pre-charge motion to quash a search warrant before a criminal charge is filed, granting this motion does not obligate courts to exclude the evidence at trial.[1698] In some states, motions to suppress evidence are submitted and decided on at the trial, whereas in other states such motions need to be filed before trial.[1699] The decision whether to exclude evidence is made by the judge after a suppression hearing. It would then be rare for it to be reconsidered at trial unless new or additional evidence is produced which affects the credibility of the evidence.[1700]

In the context of wire and oral communication surveillance, in accordance with § 2518(10)(a), an aggrieved person as defined in § 2510(11), may, in any trial, hearing, or proceeding in or before any court, move to suppress the contents of any

[1694] For example, BGHSt 34, 362.For further discussions of the "fruit of the poisonous tree" doctrine in German literature, see *Gleß*, in: Löwe/Rosenberg, StPO, Band 4/1, 27. Aufl., 2019, § 136a, Rn. 75.

[1695] See BGHSt 32, 68.

[1696] *Ossenberg*, Die Fernwirkung, 2011, S. 186.

[1697] The prosecution can also file a motion to suppress evidence produced by defendant.

[1698] *Carr* et al., The Law of Electronic Surveillance, 2002, § 10.1(c).

[1699] *Id.* § 10.1(a).

[1700] *Id.* § 10.6(c).

wire or oral communication or any evidence derived therefrom. § 2518(10)(a) further requires that the motion to suppress should be made before the trial, hearing, or proceeding, unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. The pre-trial motion requirement aims to avoid interruptions of the trial and to prevent the evidence from being exposed to the jury. In addition, the prosecution and the defense can better prepare if they are already aware from the pre-trial hearing whether certain evidence will be admitted at the trial.[1701] This arrangement also enables the government to appeal the exclusion of evidence in accordance with § 2518(10)(b).[1702]

b) Germany

In their charging document (*Anklageschrift*), German prosecutors can limit themselves to listing admissible evidence and omit legally problematic evidence. This is not an official exclusion decision, but it has the effect of reducing the possibility of such evidence being heard at trial. This list, however, has no binding effect on the court. German judges decide in their discretion what evidence to hear, including evidence not listed in the charging document. This means that even evidence that prosecutors deem "problematic" can be heard by the judges. If the court finds that certain evidence listed by the prosecutor has been obtained illegally and should be excluded, they can decide not to introduce it at the trial. The exclusion of certain evidence is thus not necessarily proclaimed by a judicial ruling. At trial, the defense can also file a motion to suppress certain evidence. The court will then decide on that motion.

c) China

Art. 56 II of the *CCPL* and Art. 33 of the *Supervision Law* provide that the police, prosecutors, judges, and supervision committees may exclude illegal evidence if a case falls within their jurisdiction. Police station, prosecution office and supervision committee must review the legality of the evidence collected by their colleagues before the files are passed on to the next stage. Each institution must ensure that inadmissible evidence does not go to the next stage. The exclusion of evidence can occur at any time, from the beginning of the investigation until the final judgment. Judges can officially rule on excluding evidence, however, it is more common for judges to simply not use the evidence if they think that it should be excluded. The police, prosecutors as well as inspectors in supervision committees can also exclude evidence by not putting it into the file.

[1701] *Id.* § 10.1(a).

[1702] *Carr* et al., The Law of Electronic Surveillance, 2020, § 6.23.

8. Evidence Obtained by Private Parties

In the U.S., *Title III* regulates interceptions conducted by both private persons and law enforcement officers. Thus, the exclusion clause provided for in 18 U.S. Code § 2515 also applies to private interceptions. The exclusionary rule under the 4th Amendment, however, only applies to governmental activities.[1703] To resolve the conflict, the United States Court of Appeals for the Sixth Circuit in *United States v. Murdock*[1704] introduced the "clean hands" exception to § 2515, allowing the prosecutor to introduce communications illegally obtained by a private party as long as "the government played no part in the unlawful interception" and thus had "clean hands".[1705] The "clean hands" exception is, however, highly controversial and was later overruled by *United States v. Crabtree*.[1706] Given the statutory exclusion clause in § 2515, most courts tend to reject "clean hands" exceptions to § 2515 and suppress evidence derived from communications illegally obtained by private persons.

German courts employ the balancing theory when deciding on the admissibility of tapes illegally recorded by private persons.[1707] The automatic exclusion of such tapes is not required, but strict standards for its admission are applied.[1708] It should be noted that it is more difficult for private persons to record material legally in Germany than in the U.S. In Germany, private persons need to get the consent of all parties to a non-public conversation in order to record it legally, whereas in the U.S. any party to a conversation can record it, even without the consent of the other parties. Therefore, the U.S. police might have more opportunities to benefit from private persons' recordings than their German colleagues, although material illegally recorded by a private person will not be admitted by U.S. courts.

Chinese legislation does not address the issue of the admissibility of evidence obtained illegally by private persons in criminal cases. Although Art. 106 of the *Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law* excludes evidence "formed or acquired by serious infringement upon the lawful rights and interests of others, violation of the law", criminal evidence may follow different standards from those of civil evidence law. Therefore, the admissibility of private evidence in criminal proceedings has not been clarified.[1709]

The exclusionary rule provided in the *CCPL* does not apply to private evidence because it only regulates the conduct of judges, prosecutors, and the police. Due to

---

[1703] *Burdeau v. McDowell*, 256 U.S. 465 (1921).

[1704] *United States v. Murdock*, 63 F.3d 1391 (6th Cir. 1995).

[1705] *United States v. Murdock*, 63 F.3d 1391, at 1403–04 (6th Cir. 1995). See Section 4. c) ee), Chapter V, Part I.

[1706] *U.S. v. Crabtree*, 565 F.3d 887 (4th Cir. 2009).

[1707] OLG Frankfurt NJW 1967, 1047, 1408.

[1708] *Stoffer*, Wie viel Privatisierung, 2016, S. 429; *Bockemühl*, Private Ermittlungen im Strafprozeß, 1996, S. 122.

[1709] See Section 13. a), Chapter V, Part III.

the emphasis on truth-finding, however, the police can legitimize the evidence to make it admissible, even if a private person had originally acted illegally in obtaining the evidence. Or private persons may offer the police evidence that they collected, then the police collect their own version of the same evidence. This practice, which resembles the "clean hands" practice in the U.S., has been criticized as a waste of police resources because the evidence has to be collected "repeatedly".[1710]

V. Empirical Studies

Empirical studies expand our understanding of criminal justice from "law on the books" to "law in action".[1711] This is especially important when it comes to the study of surveillance measures because such measures are intensely practice-based. The actual efficiency of such measures in producing information and evidence is important when evaluating whether current rules are justified. A quantitative approach contributes to understanding the benefits and costs of such measures. The official statistics on the use of surveillance of wire and oral communications are published in the U.S. and Germany, which makes such a quantitative analysis possible. For instance, the annual reports of the U.S. Courts give details on the number of people arrested and convicted as a result of telecommunication interceptions, the average number of people intercepted per order, and the average number of incriminating communications intercepted on the basis of a surveillance order.

Such statistics remain undisclosed in China, hence interviews with well-informed judges, experienced police officers and prosecutors were the only empirical method available for this study. This took the form of an online survey. The results of this survey are presented in the Appendix. In addition, a few interviews were conducted. Due to the limited size of the samples, the results are not representative. They can, nevertheless, cast some light on the current practice of surveillance measures and the opinions of legal practitioners in China.

1. Number of Surveillance Warrants

Empirical analysis demonstrates that each jurisdiction has a different method for implementing surveillance measures. In the three jurisdictions, the police and prosecutors also use different methods for calculating the number of surveillance measures. In the U.S., one surveillance warrant can include more than one person, facility or offense, and the number of warrants is normally dependent upon the

[1710] See Section 13, Chapter V, Part III.

[1711] *Hodgson/Mou*, in: Brown et al. (eds.), The Oxford Handbook of Criminal Process, 2019, 44; *Cane/Kritzer*, in: Cane/Kritzer (eds.), The Oxford Handbook of Empirical Legal Research, 2012, 1; *Leeuw*, Empirical Legal Research, 2017, 2–3.

number of cases or investigative activities. For instance, if the police investigate a narcotics case, only one warrant will be needed, regardless of the number of suspects and facilities involved in the crime. If other less serious crimes are also suspected, they can be listed in the same warrant. This means that applicants have a great deal of leeway to decide what information is included in the application. By contrast, judicial orders for surveillance of telecommunications in Germany tend to be issued for specific telephone numbers. If one suspect uses more than one telephone, which is quite common, more than one order needs to be issued against this person. According to German statistics, between 2008 and 2018 more than three judicial orders were issued, on average, per procedure under § 100a StPO. Moreover, the number of warrants issued in the U.S. includes warrants for wire, oral and electronical surveillance, while in Germany only the number of judicial orders for surveillance of telecommunications and in the home are included.

It is not quite clear how the Chinese police calculate the number of warrants issued per case. Based on the warrant template for a telecommunication surveillance, the identity of the person to be intercepted seems to play a central role. No specific phone numbers are mentioned in the warrant. Establishing the phone numbers used by the suspect is probably the responsibility of the TIM departments, so the investigator completing the warrant application would be unaware of this information. If the identity of the suspect has yet to be established, however, it can be assumed that the phone numbers will be central to the application for a warrant.

Since 2009, the rate of the implementation of surveillance warrants has dramatically decreased in the U.S. Only 24 Federal warrants were implemented in 2014.[1712] German statistics on telecommunication surveillance never mention such rates. It can be assumed that the number of non-implementations is negligible.

From this perspective, it seems that Germany adopts telecommunication surveillance far more often than the U.S., which has a far larger population than Germany. Given the different data collection methods adopted in the two jurisdictions, however, the number of surveillance warrants issued in the past few years in the U.S. and in Germany cannot be compared in a meaningful way.

2. Types of Surveillance Measures

Surveillance measures in the U.S. are classified into three categories, namely, surveillance of wire, oral and electronic communications. Reports on surveillance released by the German Ministry of Justice include reports on surveillance of telecommunications under § 100a StPO and acoustic surveillance of the home under § 100c StPO. The reports on measures under § 100a StPO divide intercepted telecommunications into four further categories: telecommunications intercepted through fixed phones, mobile phones, the internet and via radio cells.

[1712] Table 2 in Part I.

The type of surveillance measures adopted in the U.S. and Germany are similar; wiretapping and telecommunication surveillance are the prevailing practice, while the surveillance of oral communications and the acoustic surveillance of the home are less frequent.

3. Major Offenses in Surveillance Orders

The statistics in the U.S. show that the most frequently cited offense in surveillance orders is drug crime. Warrants citing narcotics or other offenses related to drugs accounted for 77 % of all warrants issued in 2018. Drug offenses are also most often cited in German surveillance procedures, with a portion of 40 % between 2015 and 2018. In the Chinese questionnaire, all interviewees stated that organized gang crime was the most common grounds for the use of TIMs, while two thirds of the interviewees also cited drug-related crimes. Of course, it is not unusual for organized crime gangs to commit drug-related crimes. Hence, organized gang crime and drug-related crime are often concurrent.

4. Cost

Statistics in the U.S. record the cost for each implementation of a surveillance warrant. The cost depends on the length of the interception and the days in operation. According to the Wiretap Report of 2018, the most expensive state wiretap was for a 365-day wiretap, which cost $3,331,169. Between 2008 and 2018, the average cost per warrant ranged from $39,485 to $83,356. In Germany, only the costs of the acoustic surveillance of homes under § 100c StPO are recorded. Between 2008 and 2018, surveillance cost around €23,400 on average. The main reason for the high cost of surveillance in the U.S. is that it must be conducted in real time, while in Germany this is not necessary. Law enforcement officers in the U.S. must take the high cost of surveillance into account, whereas in Germany the police are less concerned with cost in cases of telecommunication surveillance. In China, no information regarding the cost of TIMs is available. But since China does not require real-time surveillance recording, it seems likely that cost does not play an important role when deciding whether to implement a TIM.

5. Efficiency

Efficiency can be interpreted from different perspectives. In the U.S. statistics, the average number of incriminating intercepts per installed warrant provides a sense of the efficiency of surveillance measures for producing useful information and evidence. 20 % of all intercepted communications were incriminating. Another index to

be considered is the number of arrests and convictions arising from interceptions. According to the statistics from 2000 to 2009, 19 % of intercepted persons were arrested and 46 % of arrested persons were convicted as a result of the interception. On average, one authorized warrant led to 3.91 persons being arrested and 1.81 persons being convicted.

In Germany, no such statistics are available for measures under § 100a StPO. Reports for measures under § 100c StPO include information on whether the findings of the measures were pertinent to the original investigation or led to further investigations of other criminal activities. The term "Relevanz" is not defined in the reports, however, incriminating intercepts are definitely regarded as "relevant". The reports also detail the number of intercepted suspects and the number of third persons who were also intercepted. This data demonstrates the concern of the legislature about the infringement of the rights of third persons and suggests that the effectiveness of such measures does not always justify their use. The degree of infringement on the rights of innocent third persons should be taken into consideration and be closely supervised. Between 2008 and 2018, only 50 % of persons under home acoustic surveillance were suspects and 60.5 % of all such procedures obtained relevant information.

VI. Final Comments and Suggestions for Reforms in China

The rules governing TIMs in the *CCPL* have a very short history. The development of these regulations has only attracted limited interest from scholars. There are various reasons for this. First, the right to privacy is more of a priority for the civil law system, and the Chinese legal system and constitution lack a clear concept of this right. The discussion of TIMs thus lacks a solid constitutional basis. In addition, the right to privacy does not have priority among other personal rights. Therefore, the infringement of these rights by TIMs has not attracted much attention. Second, the rules are too vague and are therefore quite difficult to discuss. Third, there are many other restrictions on research on this topic. Principally, it is difficult to get access to first-hand material. The practice of TIMs is to a large degree kept confidential. Statistics for TIMs have not been released. Moreover, even if the legal research were of a high quality, it is still difficult to say whether the Chinese police would take it seriously for improving their practice. Although the discussion of TIMs is not a topic of great interest in China, it cannot be denied that Chinese regulations regarding this issue are far from satisfactory and need further development.

1. Constitutional Level

The current text of the *Chinese Constitution* dates from 1982, when TIMs were regarded as being closely related to national security and, as such, should be kept entirely confidential. Therefore, the *Constitution* did not even mention TIMs. Art. 39, however, provides for the inviolability of the residence and prohibits illegal searches. This has mostly been interpreted as only prohibiting physical searches or invasions. The surveillance of conversations taking place in a residence is not regarded as a search of the residence. Such investigative activities are only regulated by the *CCPL*. Citizens enjoy no constitutional protection from TIMs if no physical trespass of the residence occurs. To afford broader protection for the inviolability of residence, it would be advantageous to expressly provide for TIMs as a form of a search by adding a second paragraph to Art. 39 of the *Constitution*. Although the *Constitution* cannot be directly applied in court, the granting of constitutional protection against the use of TIMs in residences could still have a strong political impact and demonstrate the serious attitude taken by the legislature regarding TIMs. This enactment might make the police more cautious when using TIMs.

As demonstrated by the *Berger* case,[1713] U.S. courts have authority to interpret the Constitution and may even push for legislative reform by outlining the standards that new legislation would have to fulfil in order to be deemed constitutional, and the same is true for German Courts. Chinese courts, by contrast, currently have no authority to review the constitutionality of new regulations. This means that courts cannot challenge legislation from the perspective of the Constitution. The courts, therefore, lack authority to improve legislation, even if they find it to be improper or unconstitutional. This might lead to a long delay before any amendments can be made to the Chinese regulations on TIMs, as opposed to other jurisdictions where the examination of the constitutionality of laws is possible.

Although Chinese courts presently cannot apply the *Constitution*, a possible influence of the Constitution on jurisprudence is one of the most popular but also controversial topics of discussion. Referring to the *Constitution* would enable courts to interpret the *Constitution* in deciding cases, including in situations where the constitutionality of legislation is in question. The examination of the constitutionality of laws is a sensitive subject in China and is unlikely to be introduced in the near future. Therefore, appealing for a direct amendment to legislation is a more realistic strategy for offering better protection against TIMs in China.

[1713] *Berger v. New York*, 388 U.S. 41 (1967).

2. Legislation Level

a) Greater Clarification of TIMs in Legislation and in Practice

Section 8 of the *CCPL* does not contain a definition of TIMs. The legislature had originally proposed a definition of TIMs in the first draft of the *CCPL* in 2012, but there was a strong concern that a fixed definition might not keep pace with the continuous development of technology. It was quite controversial as to whether some new technological measures, such as locating an IP address, should be covered by Section 8 of the *CCPL*. Therefore, the legislature abandoned the attempt to define this core term in the *CCPL*.[1714]

The lack of a definition of TIMs in the *CCPL* causes fundamental problems. Unlike in the U.S. and Germany, where surveillance measures are further divided into different forms, such as wire and oral surveillance, there are no sub-categories defined under the term "technological investigative measures" in the *CCPL*. The term can only be interpreted literally as any measure involving technology. This definition is detached from current practice; the police are not pleased to see such a broad interpretation since they must follow stricter procedural controls for TIMs. Art. 264 of the *Procedures for Criminal Cases* provides that TIMs refer to the surveillance of records, the tracing of a person, and the surveillance of telecommunications and locations. It only lists a few categories of TIMs and does not give a precise definition. Therefore, it is still not clear which measures fall within the term "technological investigative measures".

Regardless of this problem, it seems that the police have formulated their own working definition of what measures are classified as TIMs. Their understanding is strongly influenced by past practice; therefore, many investigative measures using new technology, such as face recognition systems, are not covered. Face recognition and surveillance camera systems are powerful tools to track suspects and maintain social security in China. Camera systems work for twenty-four hours a day as a form of "strategic intelligence surveillance", as defined by U.S. law. If the police want to track somebody, they can simply install a camera system to use face recognition technology. This does not require a special warrant. If the use of this more advanced technology is not covered by the term "technological investigative measures", the procedural guarantees for TIMs only have a limited effect. Therefore, some scholars support calls for a broader interpretation of the term "technological investigative measures" and argue that all measures that are conducted covertly with the assistance of technology should be regarded as TIMs.[1715]

"Technological investigative measures" is such a vague term that it might even violate the principle of certainty. This term should be further explained and clarified

[1714] See Section 4, Chapter III, Part III.

[1715] For example, *Liao/Zhang*, 技术侦查规范化研究 (Research on the Normalization of Technological Investigation), 2015, 3. See also Section 4, Chapter III, Part III.

by adopting a list of measures as well as the procedural requirements for each measure. In this regard, German legislation could provide a good model. The main advantage of § 100a ff. StPO is that the legislation provides different conditions for different measures in accordance with the level of their intrusiveness.

b) Greater Detail in Application Materials and Warrants

Neither the *CCPL* nor any other regulation provides for what should be included in application materials and warrants for TIMs. The police have a template to fill out when applying for a warrant for TIMs, but the template does not provide much guidance. It is not clear whether investigators need to submit a comprehensive report to their directors for obtaining a warrant. Comprehensive reports are in any event not included in the files handed over to prosecutors and judges. Prosecutors and judges therefore have only limited information on which to determine the legality of evidence based on a TIM-warrant.

To improve the application of the exclusionary rule regarding TIM evidence at trial, it is necessary for the police to provide reasons for probable cause in their applications. Warrants should also describe the scope of the intercepted communications in as much detail as possible. For example, it might be advantageous to provide in a warrant the exact hours during which the surveillance can be conducted, certain conditions under which the surveillance can begin, such as only when the suspect talks to a specific person, or to restrict surveillance to certain places. The authorized period for surveillance should be calculated by hours instead of days.

Under the current rules, relevant materials need to be handed over only when TIM evidence is to be used at trial. The *Explanation of the Application of the CCPL* (2021) requires TIM evidence, while Art. 268 of the *Procedures for Criminal Cases* regulating police behaviors and Art. 229 of the *Rules of Criminal Procedure* regulating prosecutors require only issued warrants to be handed over to judges if such evidence is to be considered at trial. For better transparency, whenever TIMs were adopted, the application materials and issued warrants, including probable cause and detailed information of the surveillance, should all be put on file and handed over to judges even if TIM evidence will not be used. These files should also be accessible to defense lawyers. This requirement would work against an arbitrary use of TIMs by the police. If the police were compelled to provide justifications for each use of TIMs, their activities could be reviewed by prosecutors and judges and ultimately challenged by defense lawyers. This would encourage police to use TIMs only when necessary.

Moreover, police officers responsible for implementing warrants should be required to write surveillance blogs to record the surveillance process. These blogs should also be put on file for a judicial review.

Generally speaking, police should hand over as much information as possible regarding surveillance, to guarantee prosecutors, judges and defense lawyers free

access to related evidence, including application materials, warrants, regular blogs, evidence obtained from TIMs, except where the law provides otherwise, such as in the case of an undercover agent's safety being endangered. Such a change of practice can only be achieved if the Ministry of Public Security and the Supreme Prosecution Office confirm it and instruct their staff to do so. A judicial explanation would not be sufficient. Nevertheless, more transparency is essential not only for judges to ensure the quality of convictions involving TIM evidence, but also for defense lawyers to conduct an effective defense.

c) Warrants to be Approved by Prosecutors

No outside supervision is provided for TIM warrants in China. Such warrants are, in principle, approved within the police system or by a supervision committee. The police rely upon internal controls to examine the necessity and feasibility of TIMs. There are TIM departments in police stations at the city level and above. An application for a warrant for a TIM must be approved by the TIM department before it goes to the director of the police station. The involvement of the TIM department is not ideal; there is a risk that TIM applications are unsuccessful due to miscommunications between the TIM department and the investigators. Although TIM departments only analyze the feasibility of the technology and implement the surveillance according to the warrant, this cumbersome procedure only serves to increase the cost of a TIM. This could also deter investigators from applying for TIMs.

The disadvantages of a mere internal control are obvious. First, without outside control, the legality and necessity of TIMs cannot be substantially reviewed. Although the rejection rate is also extremely low in jurisdictions with judicial review, as in the U.S. and Germany, judicial review can prevent extreme infringements upon the right to privacy. At the present time in China, police are only required to disclose the use of TIMs in cases where the evidence is used at trial. Judicial review can prevent the police from concealing their practices regarding TIMs. Compared to TIMs that actually produce incriminating evidence, unsuccessful TIMs are more likely to be legally problematic or even arbitrary. The persons involved should have an opportunity to seek a remedy even if the information gathered through surveillance is never used.

Introducing judicial review of surveillance warrants into the Chinese criminal justice system, however, is not possible at the current time because any "interference" from the courts is excluded during the investigative phase. The police are authorized to issue warrants for most investigative measures, including search and seizure warrants. One exception is arrest warrants, which involve the highest level of infringement upon personal rights and which must therefore be issued by prosecutors. Given this context, it is even hard to justify a requirement of approval by prosecutors for TIM warrants, because TIM warrants are regarded as less intrusive than search and seizure warrants. Short of calling for a judicial review of TIMs, it would be

expedient for all warrants for investigative measures, including TIMs and search warrants, to be issued by prosecutors. Introducing judicial review would be the next step in the path towards reform.

d) Limiting the Use of Chance Findings and Tracking Technology

In China, there exist few limits on the use of information obtained from surveillance. It can be used to trigger further investigation and as evidence of crimes not named in the crime catalogue. It is difficult for the Chinese police to accept the idea that they cannot pursue crimes when they have incriminating evidence at hand. The legislature should consider expressly regulating the issue of using information obtained from surveillance in other criminal processes. They also need to provide a mechanism to guarantee that the police follow these regulations.

Art. 150 III of the *CCPL* allows for the use of necessary technology to trace a wanted person without being limited to certain crimes. It is applicable in principle even in minor crimes, such as theft. This is, of course, disproportional. TIMs cannot be justified in all situations. Therefore, TIMs for the purpose of arrest should only be allowed in the investigation of crimes listed in the catalogue of Art. 150 I of the *CPPL.*

e) Reporting System and Statistics

18 U.S. Code § 2519 and § 101b StPO in Germany require judges and prosecutors to report statistical data regarding surveillance on an annual basis. These reports can be found on websites accessible to the public. Having access to large volumes of first-hand data is of great value to researchers. In addition, summaries of these statistics permit law enforcement officers and the courts a degree of self-regulation. Yearly reports provide them with an overview of their practices over the previous year; if they find systematic failings, they can adjust accordingly. Making these reports accessible to the public would also allow for greater transparency. Public scrutiny would provide an indirect supervision of the practice of surveillance.

In China, it is not clear whether the police are required to submit regular reports, and in any event, nothing is made public. Therefore, it is of great importance for the Chinese legislature to establish a mechanism for collecting statistics relating to TIMs and to make them public on an annual basis. This might encourage the police to refrain from using TIMs too frequently, since the extensive use of TIMs might incite public protest. Given China's advanced use of information technology, the development of a nation-wide database or online platform for providing the statistics relating to TIMs would not be an impossible task. If the police were required to store information on each TIM warrant (the procedure, the outcome as well as other related information) on this online platform, the Public Security Ministry could summarize

the statistics and then publish reports. In that case, there would be no extra work for investigators.

f) Reform of the Application of the Exclusionary Rule

In China, the police, prosecutors, and supervision committees exclude illegal evidence if a case falls within their jurisdiction. In many cases, they prefer a "soft" exclusion of evidence by simply setting the evidence aside making a ruling on exclusion. As this is rarely recorded, it is difficult to calculate how often evidence is quietly excluded. The same situation is observed by judges. It is unusual to see a clear ruling on the exclusion of evidence in a judgment. The basic reason for this is the lack of independence of judges as individuals and of the judicial system as a whole. The courts are vulnerable to external pressure and too weak to supervise or challenge the police and prosecutors. Therefore, judges are likely to exclude evidence only if they are strongly convinced that the evidence is not reliable.

In China, the application of the exclusionary rule is fraught with systematic problems, which are not limited to evidence from TIMs. Therefore, a systematic reform is needed to redefine the exclusionary rule. First, it should be clarified that the criminal process does not only serve to find the truth and that procedural rules have their own independent value. Review of the evidence should not be limited to its reliability, and procedural guarantees should be taken more seriously. Just as the BGH has declared, truth must not be pursued at any cost. Second, to make exclusion at trial (or in pre-trial hearings) possible, more information regarding investigative activities should be recorded on the file and be made available to judges. Third, judges should be accorded broad authority to review the evidence at trial. From a general perspective, strengthening the position of judges and courts and allowing them to act with autonomy would enable them to challenge the police and prosecutors more effectively.

Finally, the role of defense lawyers in the exclusion process should not be underestimated. Defense lawyers have the most to gain from a procedure which makes possible a review of the legality of the evidence against their client. Currently, the involvement of defense lawyers in regard of the exclusionary rule is far from satisfactory. One reason for this is the rare participation of lawyers in criminal cases; another reason is that the rights of defense lawyers are not guaranteed. It is usual for the police not to cooperate with defense lawyers. Since criminal cases are generally less profitable than civil cases for lawyers, the government should offer more financial aid for criminal cases, especially in more remote areas, so as to attract more lawyers to take up legal aid case work. Moreover, the legislature, the Ministry of Public Security and other competent institutions should provide more detailed guidelines to guarantee the rights of defense lawyers, such as the right to access files and the right to meet their clients in custody. Lawyer associations should also assist defense lawyers in fulfilling their role effectively. For instance, if police try to prevent

defense lawyers from accessing files, lawyers should be able to complain to lawyers' associations, which could then apply pressure on the director of the responsible police station.

3. Prospects for Better Criminal Justice

China has a long history of an advanced legal system based on Confucian theory during the era of monarchy. However, since the mid-19th century China has fallen behind. China lost wars to Japan and western colonists and was half-colonized. China suffered continuous civil wars, two World Wars and social unrest for more than one century. Given this background, law was no longer taken seriously although efforts were made to modernize the Chinese legal system. In the 1950s, the first Constitution and other legislation were enacted by the P.R. of China based on the model of the Soviet Union. During the Cultural Revolution of the 1960s and 1970s, the rule of law was abolished. Only since the 1980s did law start to play an important role in social life again.

This brief overview shows that China is a country with a long history but that its experience with a modern legal system has been limited to little more than 40 years. It is not surprising, then, that many flaws and defects can be found in the Chinese legal system. Many Chinese have realized that it is important to learn from Western countries for further developing China's legal system.

This study also seeks to serve the purpose of helping to build a better criminal justice in China. At present, the rules on TIMs in the *CCPL* are too vague, and many issues regarding TIMs remain hidden from the public, even from judges and defense lawyers. A systematic improvement on TIMs law is required. The core of this reform is to reduce the potential for abuse of police power, which is a chronic and stubborn disease in Chinese criminal justice. Enhancing transparency can be its cure.

The reform of a criminal justice system is never easy and cannot be accomplished in a short time. I hope that this study may draw attention to the topic of TIMs and presents a few ideas for a reform to be considered in the future.

Appendix

Reports on the questionnaires

Originally, I have designed two questionnaire models for face-to-face interviews, Model A for police with the focus on TIMs, while Model B for the prosecutors and judges concerning TIMs during the prosecution and the trial.

However, after I showed these two questionnaires to a prosecutor, Song, to review and asked for the feedbacks. He said the police, the prosecutors and judges can be very hesitated to talk to people on this issue face-to-face, or do not tell the truth. He suggested to work out an online survey and he would help me to spread the links among his "friend circle", including the police, the prosecutors and judges, via Wechat (Whatsapp- und twitter-alike App). He also said, in this way, I can reach more interviewees in different cities, and review the results immediately on the back-station of the survey-design App,[1] once one questionnaire is submitted. Moreover, when the survey would be conducted anonymously, the answers would be more reliable. Therefore, I translated most of the questions into multi-choices forms and only few in blank-filling forms. This is because interviewees normally have less patience to type much their own words.

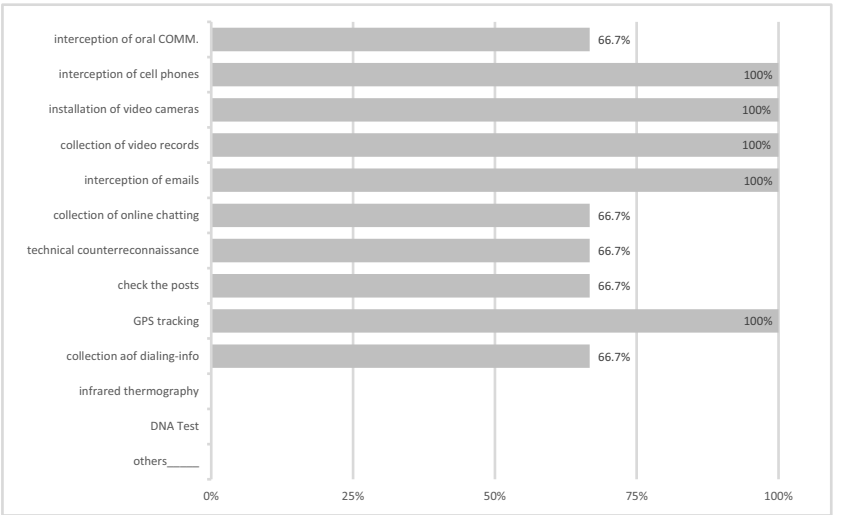
Model A consists of 37 questions, while Model B has 29 questions. Both questionnaires were released on 19. March 2019. After three hours, Mr. Song told me that one of his police friends told him that they police are not allowed to answer questions on TIMs online. I had to invalidate the links. Within the first three hours, Model A has been visited 5 times with 3 effective submissions. Model B kept valid all the time, thus 9 effective feedbacks have been collected finally, 7 prosecutors and 2 judges. In general, the prosecutors and judges showed a more cooperative attitude than the police when they worked on the interview questions. For instance, the former skipped fewer questions and offered more information willingly. The interviewees all have plenty working experience, thus I suppose they know their work quite well and their answers are reliable.

[1] The website for the survey design: https://wj.qq.com/mine.html.

Report on Model A (for Police)

Q 1

What TIMs and high-tech devices have you ever used?

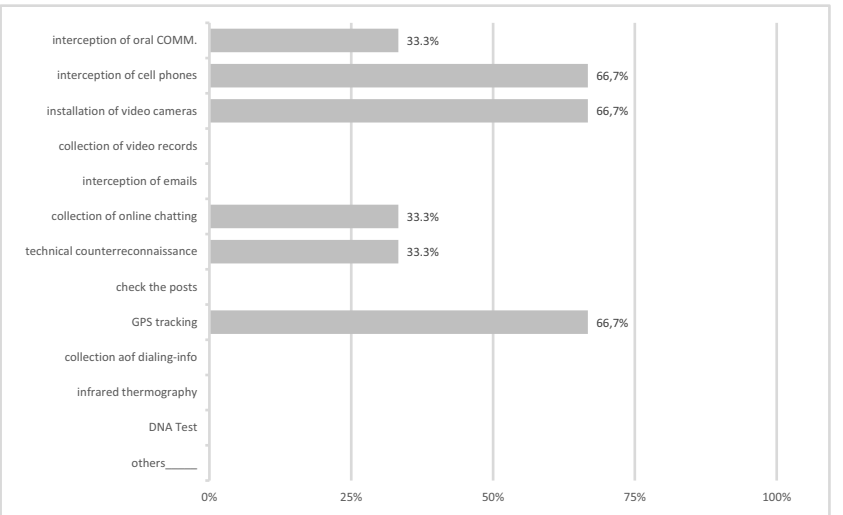


From the above chart, it shows what measures are regarded as TIMs, i. e. infrared thermography and DNA Test are not regarded as TIMs, although they involve high technics. The measures can be divided into two categories: one is the measures that police need to install the device themselves in order to collect evidence, such as interception of cell phone; the other is that the police purely collect the information that is already obtained or stored by others, such as telecommunication companies. For the latter, the police does not need to operate any technical devices. They only need to get a warrant and require, for example, telecommunication company, to offer related information.

DOI https://doi.org/10.3790/978-3-428-58566-3 | Generated on 2025-08-14 01:51:00

Q 2

Which measures from Q 1 have you used most frequently?



The first three measures used most frequently are interception of cell phones, installation of cameras and GPS tracking. The first one results from the widely spread of cell phones which even replace the fixed phone to a large degree in China, especially in private life. The video cameras installed by the police cover most of the public space, such as train stations, subway stations, streets. This can result in that the police does not need to collect video records from other cameras that often. Their own cameras can solve most of the problems. Moreover, the police needs TIM warrant only when the camera is firstly installed, afterwards, they can get access to the records without need of any further permission. As to the GPS tracking, its adoption is not limited by the crime-catalogue,[2] therefore, it is not surprising that this measure is used quite often.

Q 3

In how many cases are TIMs averagely used among every 10 cases?

A. 0–2 (1) B. 2–4 (1) C. 4–6 (1) D. 6–8 (0) E. 8–10 (0)

The frequency can vary according to the positions of the interviewees and their working places.

[2] Art. 150 CCPL.

Q 4

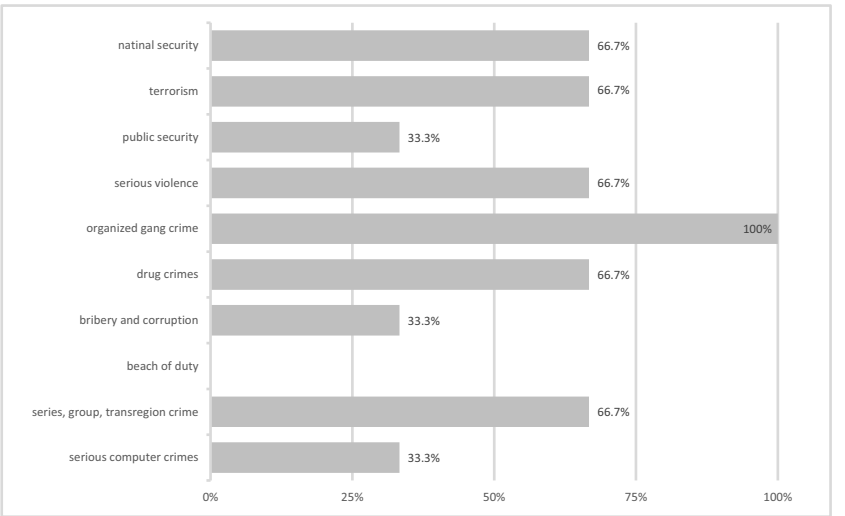
Whether the defense lawyer can be the target of TIMs?

A. yes (0) B. no (0)

All three interviewees skipped this question. It shows that this is a sensible question. From one hand, it can be speculated from such silence that the situation described is not totally excluded. Otherwise the interviewees would not hesitate and directly chosen "no". From the other hand, the interviewees realized that it can be quite problematic and confronted with strong resistance from the lawyer professionals when they know they are overheard.

Q 5

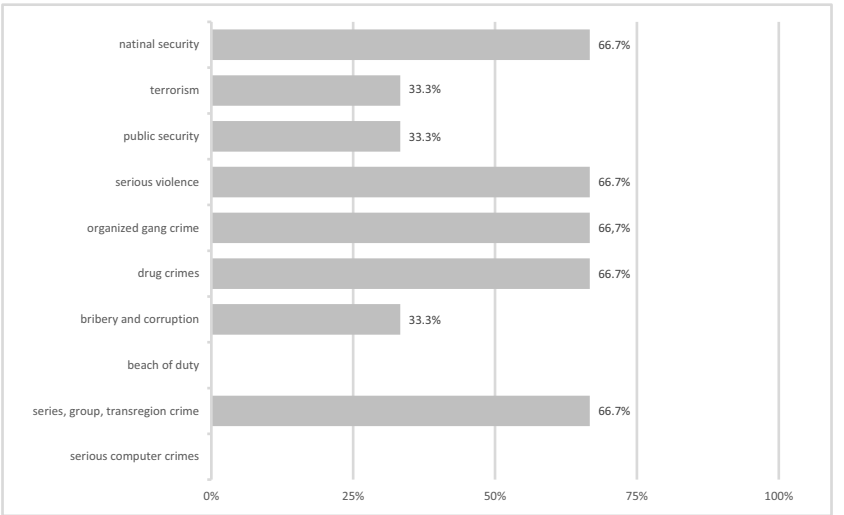
In which type of cases are TIMs used?



I designed the options according to Art. 150 *CCPL*, Art. 227 of the *Rules of Criminal Procedure* and Art. 263 of the *Procedures for Criminal Cases.* Only "breach of duty" is not mentioned in any above documents. It shows that all three used to adopt TIMs in organized gang crimes. That no one selected "breach of duty" is a good sign to show that TIMs are not abused to this non-catalogue-crime.

Q 6

In which type of cases are TIMs used more often?



It is interesting that TIMs are not used quite often in computer crimes. The national security, the organized crime and the drug crimes are often committed in a more secret way, which might be a reason for the preference for such measures. As to the violent crime and the trans-region crimes, the seriousness and the complication of the crimes might be taken into the consideration.

Q 7

Who is responsible to apply for TIMs?

A. *The investigator who is directly responsible for the case will apply for TIMs to the president of the police station at the city level or above. (1)*

B. *The direct charger of the department which investigates the case will apply for TIMs to the charger of the police station at the city level or above. (3)*

It shows that both are possible.

Q 8

What are the legal foundations for the procedural rules on the application mentioned in Q 7?

A. *CCPL (2)*

B. *Provisions on the Procedures for Handling Criminal Cases (3)*

C. *internal rules (1)*

Q 9

Whether is it possible that the procedural rules on the approvals vary from places to places?

A. yes (3) B. no (0)

Given Q 7 and Q 9, different processes are followed in different places. The legal rules are too vague, and the local organs thus need to fulfil those gaps and work out an applicable process by themselves. The problems here are that the rules worked out by the individual organs are normally not public. Therefore, it is difficult for the defense lawyers to find out whether rules are followed or not. It can be concluded that more applicable procedural rules are required at national level, either in the *CCPL* directly or worked out by Public Security Ministry.

Q 10

What elements are considered normally for the application/approval of TIMs?

A. money costs (2)

B. B personal costs (2)

C. time costs (2)

D. Whether the application/approval meet the requirements provided in law. (2)

E. Whether the desirable goals can be achieved. (1)

F. others (0)

The results show that all these elements can be considered but do not have to be considered in every case. However, according to the legislation, the last two elements (D. and E.) should be met in any case before the application/approval are decided. However, in the practice, these two are sometimes ignored, and the last option is even less interesting than A., B. and C. for the decision-maker. It cannot exclude the possibility that no other elements also play a role. The interviewees can be just too lazy to fill a blank or to think out some other elements.

Q 11

Has an application for a TIM ever been rejected?

A. yes (3) B. no (0)

It shows that the internal approval process has sometimes a controlling function.

Q 12

How many rejections against the application for a TIM in every 10 cases?

A. 0–2 (1) B. 2–4 (1) C. 4–6 (1) D. 6–8 (0) E. 8–10 (0)

The answers vary. This can be influenced by many elements. For example, the place or the department where the interviewees work; the personal experience of the decision-maker; the types of the cases which the interviewees often deal with, etc.

Q 13

Are the materials collected through TIMs (such as the recordings) handed over to the prosecution office along with the case files?

A. yes (1) B. no (1) C. depending on the individual cases (1)

It might reflect the different practice in different places. At least it shows that the materials from TIMs can be "hidden" from the prosecutors. The answer B. can be interpreted that it is still a common practice in some places or for some investigators that such materials are not included in the charging files at all.

Q 14

Who will decide whether the materials collected through TIMs (such as the recordings) handed over to the prosecution office along with the case files? (only for the interviewee who chose C. in Q 13)

A. the investigator who is directly in charge of the case (0)

B. the direct chef of A (for instance, the chef of the department) (0)

C. the president of the police station at the city level or above (1)

In the local government, the president of the police station at the city level or above is an officer with high hierarchy in that level of the government, and always a member of standing Committee of it which is the decision-making organ for the government. From the administrative power, the president of the police station has more political influence than the president of the court and the prosecution office with the same level. If the decision described in Q 14 is made by the president of the police station at the city level or above, the prosecutors and the judges can be hesitated to challenge this decision when the materials from TIMs are not included in the files.

Q 15

What elements are considered when the materials from TIMs are decided to be handed over to the prosecutors? (only for the interviewee who chose C. in Q 13)

A. the security of the related persons (1)

B. other serious results (in the meaning of Art. 154 CCPL) (1)

C. the tediousness of the process (0)

D. The concerns that the legality of such materials can be challenged in a latter stage (1)

A. and B. are both expressively required by Art. 154 *CCPL*. D. is a rather practical concern by the police. Once the materials are challenged and approved by the court, it will cause a lot of trouble to the police. The police might need to submit extra explanation or even have to testify during the trial. Therefore, when the police have a concern on the legality of the materials by himself, he will avoid to include them in

the files. The tediousness of the process is more relevant for the application of TIMs. When TIMs have been executed, the process is no longer a problem.

Q 16

In how many cases are the materials collected through TIMs (such as the recordings) handed over to the prosecution office along with the case files in every 10 cases where TIMs have been taken? (only for the interviewee who chose C. in Q 13)

A. 0–2 (1) B. 2–4 (0) C. 4–6 (0) D. 6–8 (0) E. 8–10 (0)

It seems that it is rare to include such materials in the files. In most of the cases, such materials are not seen in the files for charging. Since the defense lawyer can only read the charging file from the prosecutors, so they have no access to the information about TIMs.

Q 17

In how many cases are TIMs prolonged in every 10 cases where TIMs have been taken?

A. 0–2 (1) B. 2–4 (1) C. 4–6 (1) D. 6–8 (0) E. 8–10 (0)

Q 18

Does the prolongation have to be approved by the same person who approved the original warrant?

A. yes (3) B. no (0)

Q 19

Have the executions of TIMs ever exceeded the duration approved by the warrant?

A. yes (2) B. no (1)

Q 20

Art. 152 CCPL provides: "The investigators…shall promptly destroy the irrelevant materials to the cases which are obtained from technical investigation measures." When are the irrelevant materials exactly destroyed?

A. The investigators destroy such materials immediately when the materials are collected. (1)

B. The investigators decide when to destroy the materials. (2)

C. The materials are destroyed after the cases have been decided. (3)

D. The materials are destroyed after certain period of time. (1)

E. The chef of the investigators decides when to destroy the materials. (2)

The divided answers show that there are no unified rules on this question. The practices vary from places to places and cases to cases. The same conclusion can be drawn as in Q 9 A., that more detailed rules are required at national level.

Q 21

Who has right to get access to the materials collected through TIMs?

A. *The executor of TIM Department can get access to materials from TIM that he or she has executed. (3)*

B. *The chef of TIM department and the president of that police station can get access to all the materials ever collected from TIM. (3)*

C. *The direct investigator can get access to materials in the case that he or she is responsible to. (2)*

One interviewee did not choose C because sometimes the direct investigator only gets transcripts from TIM department instead of the original materials.

Q 22

After how long are the materials from TIMs destroyed?

No one answered this question. It may be because the interviewees do not know or because there are no fixed rules on this issue.

Q 23

When TIMs violates the law during the approval process or execution (such as the lack of the required documents for approval or the execution out of the validity), can the materials collected from TIMs still be used as a clue or evidence?

A. yes (2) B. no (1) C. depending on the seriousness of the violation in individual cases (0)

It shows that the seriousness of the violation is normally not considered in the practice. Combined with Q 15 A., it seems that the police concerns more about whether the violation can be figured out by the prosecutors or defense lawyers.

Q 24

Have you ever dealt any cases where the materials from TIMs as evidence have been excluded by the court?

A. yes (2) B. no (1)

It shows at least that such materials can be excluded by the court in practice.

Q 25

In order to investigate category-crime A, the police officer executes TIMs, but occasionally found clues or evidence for crime B, however, crime B per se does not meet the criteria for taking TIMs, can such clues or evidence still be used for crime B?

A. yes (3) B. no (0)

It shows that the materials from TIMs can be used for the crimes which themselves do not qualify for TIMs. In this way TIMs can be, in principle, applied to any crime.

For the slight crimes, the police might not consider TIMs, since it is not "worthy". However, the police can use the materials against any crimes involved.

Q 26

After the rules on TIMs have been introduced into CCPL in 2012, do you notice any changes in practice where the materials from TIMs are used as evidence in the trial?

A. More materials from TIMs are used as evidence in the trial. (3)

B. no changes (1)

C. other changes (0)

It is hard to explain why one interviewee chose A. and B. at the same time. It might mean that the changes are too small to notice in his opinion. Since all three interviewees chosen A., it reflects that the modification of the *CCPL* in 2012 does have a positive effect in order to promote the materials from TIMs to be present at the trial. This is the precondition of the cross-exam.

Q 27

After the rules on TIMs have been introduced into CCPL in 2012, do you notice any changes in the process regarding TIMs generally?

A. The process is stricter (3)

B. The process is looser (0)

C. no changes (0)

D. other changes (0)

Combined with Q 26 A., *CCPL* 2012 promotes a better process-control on the TIMs.

Q 28

Is there big data about TIMs at the national level (such as in how many cases are TIMs adopted in a year)?

A. yes (2) B. no (1) C. no big data at the national level, but at the local level (0)

The answers are confusing. It is still not sure whether data about TIMs is collected national-wide and analyzed by certain ministry (such as the Public Security Ministry or Justice Ministry). At least, I did not find any statistics on TIMs released by any ministry to the public. I am not sure whether such statistics, when they exist, fall also within "national secrecy".

Q 29

Is there a regular report system regarding TIMs?

A. yes (3) B. no (0)

It shows that there is an internal report system to collect data or information on the adoption of TIMs. It is not clear in which extend and what type of data or information is included in the reports. This means the situation of TIMs are evaluated or supervised by the government regularly. It is a pity that no such reports are ever public.

Q 30

In your opinion, what problems does the current rules on TIMs have? What difficulties are there in the practice? (open question)

Two interviewees did not answer, one answered no.

Q 31

Do you have any suggestions on the improvement of the rules on TIMs? (open question)

Two interviewees did not answer, one answered no.

Q 32

Are there any comments on TIM system? (open question)

Two interviewees did not answer, one answered no

The interviewees might be too lazy to answer the open questions.

Q 33

The age of the interviewee.

No one answered.

Q 34

How long have the interviewee worked as police?

No one answered.

Q 35

The position of the interviewee.

One answered that he worked at the department which is responsible for the economic crimes; another one answered that he is an investigator. The third one skipped the question.

Q 36

The level of the police station where the interviewees work.

All three work at the provincial police station.

Q 37

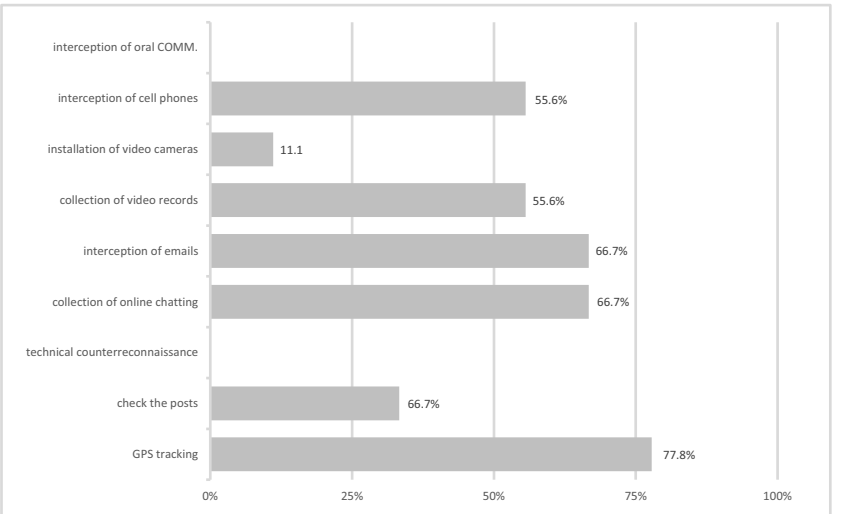
The place where the interviewees work

One works at the Sinkiang; the other works at Nantong, Jiangsu Province; and the third one did not answer.

Report on Model B (for Prosecutors and Judges)

Q 1

The evidence from what kinds of TIMs have you ever dealt with during the charging/trial?

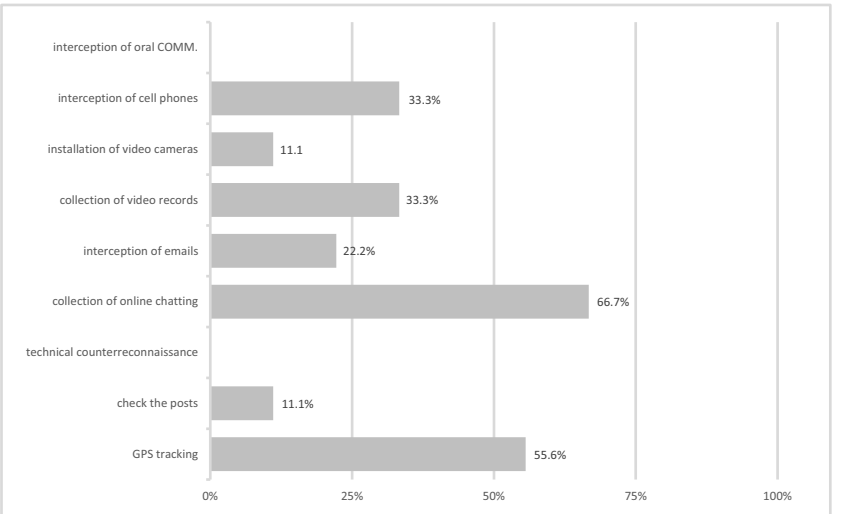


Compared with Q 1 A., it shows what kinds of TIMs are often included in the charging files and are seen by the prosecutors and judges. The evidence from the interception of the oral communication is rarely seen in the charging files, while the interception of the cell phone is included in the charging files more often. One explanation might be that the evidence from the former measure has more risk to disclose the identities of the persons who intercept the communication and how the communication is intercepted. Then the police tends to hide this part of investigation and shows the prosecutors and judges only (for instance, physical or documental) evidence collected from the further investigation.

The video records, emails or the online chatting can be obtained from the third parties, such as the internet offers or other organs, without the risk to disclose the identities of the related persons. Moreover, they have almost equal proving weight as physical or documental evidence, which means are more reliable. This makes these types of evidence easier to be accepted. GPS-tracking is also the most used measure according to Q 1 A., since it can be applied in any crime whenever the police wants to locate the suspects.

Q 2

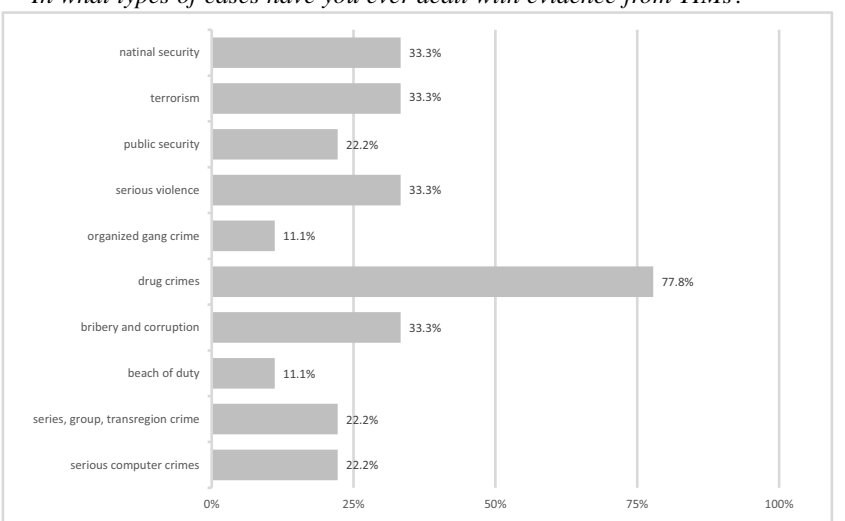
Which type of TIMs have you seen most often in the files?



The percentages here are not correspondent with the one in Q 2 A. The measures often used by the police are not always the ones often seen in the charging files. This reflects that the police have great discretion space to decide what the prosecutors/ judges can see in the files that they receive from the police.

Q 3

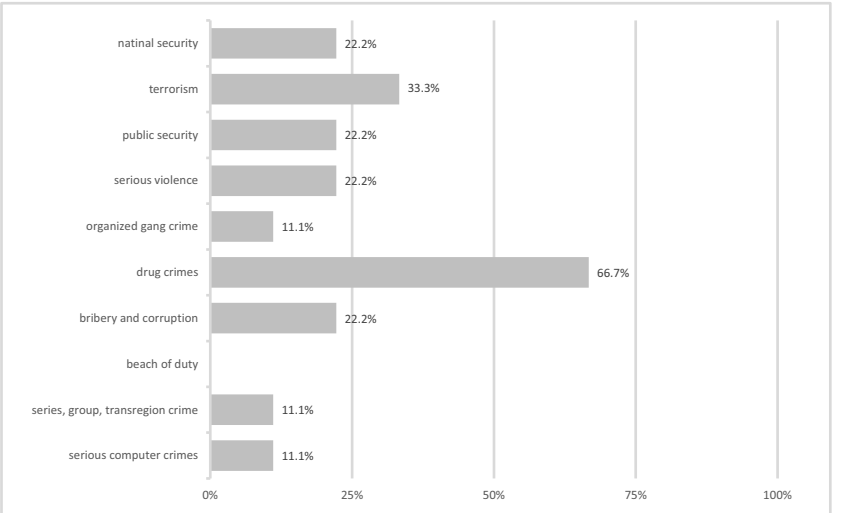
In what types of cases have you ever dealt with evidence from TIMs?



The tendency here is quite comparable with the one in Q 5 Model A. This means once the police take TIMs in certain type of cases, the prosecutors/judges might have a chance to see them in the files.

Q 4

In what types of cases have you ever dealt with the evidence from TIMs most often?



Compared to Q 6 Model A, TIMs used most often by the police are not always the ones that are seen most often in the files by the prosecutors/judges. It shows that the types of the cases play a role when the police decides whether TIM should be included in the files. Moreover, with the same conclusion in Q 2 Model B, the police have great discretion power on deciding whether to include the materials from TIMs in the charging files.

Q 5

Have you ever seen any file that includes the procedural details of TIMs (such as the warrants)?

A. yes (4) B. no (5)

The answers are quite divided. It shows that sometimes the procedural details are offered to the prosecutors/judge, but in more situations they are not. The percentage showed here is not optimistic, when 5 of interviewees said that they have never seen one case where the procedural details were reported.

Q 6

Are the materials from TIMs included in the charging files? If yes, in what forms?

A. The original materials are submitted, such as the recording tapes. (1)

B. Only the transcripts of the recordings or the final reports are submitted. (3)

C. No materials are submitted, any the final evidence can be seen. (5)

It is still a common practice that no materials from TIMs are submitted to the prosecutors/judges. This situation should be improved. For instance, the legislation can impose the police an obligation that they have to include the materials from TIMs in the charging files with very limited exceptions. This will give the police more pressure and in turn, the police will be more cautious when they are taking TIMs.

Q 7

In how many cases are materials from TIMs included in the charging files and handed over to the prosecutors/judges in every 10 cases?

A. 0 B. 1–2 (7) B. 2–4 (0) C. 4–6 (1) D. 6–8 (0) E. 8–10 (1)

I was surprised to see that one interviewee has chosen E. I checked his questionnaire, and found that he chose C. in Q 6 Model B. I supposed that he misunderstood this question and mixed "the materials from TIM" with "the final evidence". The interviewee who chose C. in this question, has chosen A. both in Q 5 Model B and Q 6 Model B. To the contrary, most of the interviewees chosen B. It shows that the materials of TIMs are included in the charging files with a low percentage, but it is not excluded that there is a higher percentage in some places.

Q 8

If the procedural details and materials from TIMs have been included in the charging files, would you review the legality of TIMs?

A. yes (7) B. no (2) C. depending on the individual cases (0)

It shows that the prosecutors/judges do have a relatively high motivation to review the legality of TIMs once they get information on TIMs. Therefore, it is expectable that there will be a better control once the materials from TIMs are required to be submitted more often.

Q 9

Have you ever found out and ruled that a TIM is illegal? (only for the interviewees who have chosen A. and C. in Q 8 Model B)

A. yes (1) B. no (6)

Although the prosecutors/judges do review the legality of TIMs quite often, it is rare that they rule that TIMs have been taken illegally. One explanation can be that the police submits only the materials when they think TIMs have no legal problems.

Q 10

What elements do you consider when you rule on the legality/illegality of TIMs? *(only for the interviewees who have chosen A. and C. in Q 8 Model B)*

A. The approval-process for TIMs is illegal. (5)

B. TIMs have released the national secret, trade secret or privacy. (2)

C. TIMs have exceeded the duration approved in the warrant. (3)

D. TIMs have been applied improperly to slight crimes. (2)

E. TIMs have been applied to the third persons who are not included in the warrant. (5)

F. other reasons (0)

It seems that the prosecutors/judges take the approval-process and the involvement of the third persons in TIMs more seriously. The violation of the duration is easy to figure out and define, while B. and D. follow a softer standard. It is not clear whether the prosecutors/judges have considered the situation described in Q 25 Model A as "*applied improperly to slight crimes*".

Q 11

What do you do when you found out that TIMs had been taken illegally? (only for the interviewees who have chosen A. and C. in Q 8 Model B)

A. to send the files back to the police/prosecutors for further investigations (2)

B. to exclude the evidence which is illegally obtained (3)

C. to admit the materials as evidence (1)

D. to communicate with the investigators (6)

E. others (0)

It shows that most of the prosecutors/judges prefer a soft solution described in D. Meanwhile, some of them will also exclude the evidence in certain situations.

Q 12

What is the percentages that evidence obtained from a TIM is excluded in every 10 TIM? (only for the interviewees who chosen B. in Q 11 Model B)

A. 0 (1) B. 0–2 (2) C. 2–4 (0) D. 4–6 (0) E. 6–8 (0) F. 8–10 (0)

The percentage is relatively low. Compared with Q 11 Model B where only 3 out of 7 exclude the illegal evidence directly, it means that even after the prosecutors/judges have found out that evidence had been obtained illegally, it is still extremely rare that such evidence is excluded.

Q 13

In order to investigate category-crime A, the police execute TIMs, but occasionally found clues or evidence for crime B, however, crime B per se does not meet the criteria for taking TIMs, can such clues or evidence still be used in order to charge or to convict crime B?

A. yes (1) B. no (0)

B. depending on the individual cases (7)

C. *It cannot be known that the evidence for crime B came originally from TIMs for crime A. (2)*

D. *others (0)*

One interviewee chose C. and D. at the same time, thus there are 10 answers. Compared to Q 25 Model A, the prosecutors/judges do not take the admissibility of such accidental results for granted, while most of the police does. The prosecutors/judges prefer to evaluate the admissibility of such accidental results in individual cases. D. reflects the same problem as C. in Q 6 Model B. More information about TIMs should be released to the prosecutors/judges for their review.

Q 14

When the defense lawyer challenges the legality of TIMs during the trial, will the judges subpoena the police who executed TIMs to testify?

A. *Once the lawyer proposes the challenges, the judges will subpoena the police who executed TIMs to testify. (0)*

B. *The judges will not subpoena the police who executed TIMs to testify. (4)*

C. *The judges decide on whether to subpoena the police who executed TIMs to testify in individual cases. (6)*

Q 15

In how many cases where the defense lawyer challenges the legality of TIMs during the trial, will the judges subpoena the police who executed TIMs to testify in every 10 cases? (only for the interviewees who chosen C. in Q 14 Model B)

A. 0–2 (6) B. 2–4 (0) C. 4–6 (0) D. 6–8 (0) E. 8–10 (0)

Compared Q 14 and 15 Model B, it can be concluded that the police might be subpoenaed to testify about the legality of TIMs that has been taken, however, it is not a popular practice.

Q 16

Art. 154 CCPL provides: "Where the use of such evidence (evidence from TIMs) may threaten the personal safety of relevant personnel or result in other serious consequences, protective measures shall be adopted to avoid the exposure of the applied technical measures and the true identity of such personnel, and when necessary, judges may verify the evidence outside courtrooms." How are "other serious consequences" understood in practice? (an open question)

Eight answers have been collected:

1. *many circumstances*
2. *For instance, the investigation work has not been finished, or the police needs to take the same measure to investigate other suspects.*
3. *I have never met such a situation.*

4. *There can be a revenge when the information is released.*
5. *The disclosure of the identities of the persons will endanger the personal safety.*
6. *The personal safety of the family members.*
7. *The national secret will be leaked.*
8. *During the undercover agency, the identity of the investigator will be disclosed. For instance, the identity of the undercover agent in drug cases will be disclosed.*

It shows there is not an identical understanding towards "other serious consequences" in the practice. The most considered elements referred here are the personal safety, including the investigators themselves and the family members. This actually explains the understanding of "the personal safety of relevant personnel", instead of "other serious consequences". The possible imperilment to the investigations and the leak of the national secret can be considered as "serious consequences".

Q 17

After the rules on TIMs have been introduced into CCPL in 2012, do you think that the TIM follow the legal rules better than before?

A. *yes (8)*
B. *no changes (1)*
C. *others (0)*

Together with Q 27 Model A, the answers here confirm the positive effect of the modification of CCPL 2012 on TIMs.

Q 18

After the rules on TIMs have been introduced into CCPL in 2012, do you notice any changes in practice where the materials from TIMs are used as evidence in the trial?

A. *More materials from TIMs are used as evidence in the trial. (6)*
B. *no changes (3)*
C. *other changes (0)*

Together with Q 26, 27 Model A and Q 17 Model B, the answers here confirm the positive effect of the modification of CCPL 2012 on TIMs and more materials from TIMs are open to the public and accepted as evidence.

Q 19

After the rules on TIMs have been introduced into CCPL in 2012, do you think that it is easier to apply the exclusionary rules to TIM evidence?

A. *The modifications in CCPL 2012 provide the legal basis for the application of the exclusionary rules to TIM evidence. (6)*

B. It is not possible to exclude the evidence according to the new rules on TIMs in CCPL. (3)

C. others (0)

Art. 154 *CCPL* legitimate the materials from TIMs to be legal evidence. It is regarded as a big development. However, the wording is quite vague and it does not include anything about the exclusionary rule. This means, on the one hand, the new rules of *CCPL* grant the prosecutors/judges the chance to review the TIM evidence. On the other hand, the prosecutors/judges can only apply the general exclusionary rule to TIM evidence based on their own understanding. The special section on TIMs in *CCPL* 2012 plays only a marginal role in the exclusion of evidence.

Q 20

Is there big data about TIMs at the national level (such as in how many cases are TIM adopted in a year)?

A. yes (0) B. no (8) C. no big data at the national level, but at the local level (1)

Compared with Q 28 Model A, it is quite interesting that the police and the prosecutors/judges gave quite different answers. All 9 prosecutors/judges-interviewees denied that there is a big data on TIMs at the national level, while two police-interviewees confirmed such a big data bank. Therefore, it is confusing whether such a big data bank exists or not. One possible explanation can be that such a big data bank would exist inside of the police system, but is kept confidential. Even the prosecutors/judges do not know about it.

Q 21

Is there a regular report system regarding TIMs?

A. yes (1) B. no (8)

Compared with Q 29 Model A, inside of the police system, there is a regular report system where the police needs to report about their application of TIMs, while it is not popular that the prosecutors/judges are required to do so. The interviewee who chose A here is a prosecutor. It can be a local practice that the prosecutors need to submit regular reports.

Q 22

What problems are there in the current rules on TIMs in your opinion? What difficulties are there in the practice? (open questions)

Five answers have been collected:

1. *The rules do not comply with the practice.*
2. *not found*
3. *no*
4. *The process for the approval is too strict.*

5. *The process for the approval is too troublesome and the timing for the investigation can be passed.*

There are only 3 effective answers. The one for No. 1 is a judge and prosecutors wrote No. 4 and No. 5 and complained about the design of the process. It seems that the two prosecutors referred to the investigation work that they undertook for the duty-related crimes before *the Supervision Law.* At that time, when the prosecutors wanted to adopt TIMs against certain suspect, they needed to get approval from their own chef first and handed over to the police for another review.

Q 23

Do you have any suggestions on the improvement?

One answer has been collected:

To reduce the administrative levels which the approval-process needs to go through.

This answer was given by the prosecutor who gave answer No. 5 in Q 22 B.

Q 24

Are there any comments on TIM system? (open question)

Two answered no, and other seven did not answer.

Q 25 – Q 29

These five questions are about the personal information of the interviewees:

Q 25: the age of the interviewee

Q 26: the profession

Q 27: the time period in that the interviewee undertakes this profession

Q 28: the level of the organ where the interviewee works

Q 29: the exact position or work

(The following number sequence does not comply with the numbers in the above open questions, such as Q 22 Model B)

37-year-old; a judge; 11 years; district court; a judge

40-year-old; a judge; 15 years; city court; middle ranking (with middle level the interviewee referred to the administrative ranking. For instance, a chef of a criminal chamber belongs to a "middle ranking".)

50-year-old; a prosecutor; 16 years; city prosecution office; dealing with the cases (not sure what it means)

40-year-old; a prosecutor; 15 years; city prosecution office; to approve the arrest warrants.

44-year-old; a prosecutor; 18 years; city prosecution office; to charge a case

45-year-old; a prosecutor; 20 years; city prosecution office; to approve the arrest warrants.

48-year-old; a prosecutor; 23 years; provincial prosecution office; to charge a case.

35-year-old; a prosecutor; 9 years; city prosecution office; the former anti-corruption department.

37-year-old; a prosecutor; 11 years; provincial prosecution office; to supervise the investigative activities.

References

Albrecht, Hans-Jörg/*Dorsch*, Claudia/*Krüpe*, Christiane: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den § 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Max-Planck-Institut f. ausländ. u. inter. Strafrecht, 2003 (cited: Rechtswirklichkeit und Effizienz der Überwachung).

Alexy, Robert: Grundrechte und Verhältnismäßigkeit, in: Schliesky, Utz/Ernst, Christian/Schulz, Sönke E. (Hrsg.), Die Freiheit des Menschen in Kommune, Staat und Europa. Festschrift für Edzard Schmidt-Jortzig. C.F. Müller, 2011, S. 3.

Alschuler, Albert W.: Fourth Amendment Remedies: The Current Understanding, in: Hickok, Eugene W. (ed.), The Bill of Rights. University Press of Virginia, 1991.

– The Exclusionary Rule and Causation: Hudson v. Michigan and Its Ancestors, Iowa L. Rev. 93 (2008), 1741.

– Studying the Exclusionary Rule: An Empirical Classic, University of Chicago Law Review 75 (2008), 1365.

Ambos, Kai: Beweisverwertungsverbote. Duncker & Humblot, 2010.

Amelung, Knut: Informationsbeherrschungsrechte im Strafprozeß. Dogmatische Grundlagen individualrechtlicher Beweisverbote. Duncker & Humblot, 1990.

Amsterdam, Anthony: Perspectives on the Fourth Amendment, Minnesota Law Review 58 (1974), 349.

Aynes, Richard L.: Katz and the Fourth Amendment: A Reasonable Expectation of Privacy or, A Man's Home Is His Fort, Cleveland State Law Review 23 (1974), 63.

Backes, Otto/*Gusy*, Christoph: Wer kontrolliert die Telefonüberwachung? Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung. Peter Lang, 2003.

Bao, Ji (鲍霁) (ed.): 张友渔学术精华录 (Memo of Scholarship of Zhang Youyu). Beijing Normal University Press, 1988.

Bär, Wolfgang: Die Neuregelung zur Erhebung von Verkehrsdaten (§ 100g StPO), NZWiSt 2017, 81.

Beatty, David M.: The Ultimate Rule of Law. Oxford University Press, 2004.

Beling, Ernst von: die Beweisverbote als Grenzen der Wahrheitserforschung im Strafprozess. Schletter, 1903.

Belknap, Michal R.: The Supreme Court and Criminal Procedure. CQ Press, 2011.

Bender, Eric Dean: The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?, New York University Law Review 60 (1985), 725.

Bernsmann, Klaus/*Jansen*, Kirsten: Heimliche Ermittlungsmethoden und ihre Kontrolle. Ein systematischer Überblick, StV 1998, 217.

Bernsmann, Klaus: Beweisgewinnung unter Verwendung des satellitengestützten Navigationssystems »GPS«, StV 2001, 382.

– „Der wohnungslose Gefangene". Anmerkungen zu einem fast vergessenen Problem, in: Feltes, Thomas/Pfeiffer, Christian/Steinhilper, Gernot (Hrsg.), Kriminalpolitik und ihre wissenschaftlichen Grundlagen. Festschrift für Hans-Dieter Schwind zum 70. Geburtstag. C. F. Müller, 2006, S. 515.

Beulke, Werner: Hypothetische Kausalverläufe im Strafverfahren bei rechtswidrigem Vorgehen von Ermittlungsorganen, ZStW 103 (1991), 657.

Bienert, Anja: Private Ermittlungen und ihre Bedeutung auf dem Gebiet der Beweisverwertungsverbote. Shaker, 1997.

Blozik, Michael: Subsidiaritätsklauseln im Strafverfahren. Universitätsverlag Göttingen, 2012.

Bludovsky, Oliver: Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100c Abs.1 Nr. 3 StPO. Peter Lang, 2002.

Blumenthal, Jeremy A./*Adya*, Meera/*Mogle*, Jacqueline: The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy", University of Pennsylvania Journal of Constitutional Law 11 (2009), 331.

Bockemühl, Jan: Private Ermittlungen im Strafprozeß. Nomos, 1996.

Bockemühl, Jan: Private Ermittlungen im Strafprozeß. Ein Beitrag zu der Lehre von den Beweisverboten. Nomos, 1996.

Bomser, Alan H.: Report: A Lawyer's Ramble Down the Information Superhighway, Fordham Law Review 6 (1995), 697.

Bourdeau, John/*Gebauer*, John A./*Harnad*, Glenda K./*Melley*, Anne E.: Searches and Seizures, American Jurisprudence 2d, Vol. 68, 2nd Edition. Thomson West, updated in 2021.

Bradley, Craig M.: Beweisverbote in den USA und in Deutschland, GA 1985, 99.

Brandis, Tobias: Beweisverbote als Belastungsverbote aus Sicht des Beschuldigten? Peter Lang, 2001.

Brenncke, Martin: Judicial Law-making in English and German Courts. intersentia, 2018 (cited: Judicial Law-making).

Brenner, Susan W.: The Privacy Privilege: Law Enforcement, Technology, and the Constitution, Journal of Technology Law & Policy 7 (2002), 128.

Burger, Warren E.: Who Will Watch the Watchman?, American University Law Review 14 (1964), 1.

Burkell, Jacquelyn: Deciding for Ourselves: Some Thoughts on the Psychology of Assessing Reasonable Expectations of Privacy, Canadian Journal of Criminology and Criminal Justice 50 (2008), 307.

Cammack, Mark: The United States: The Rise and Fall of the Constitutional Exclusionary Rule, in: Thaman, Stephen (ed.), Exclusionary Rules in Comparative Law. Springer, 2013, p. 3.

Cane, Peter/*Kritzer*, Herbert M. (eds.), The Oxford Handbook of Empirical Legal Research. Oxford University Press, 2012.

Cao, Jianming (曹建明): 关于人民检察院规范司法行为工作情况报告 (Work Report on the Standardization of Judicial Behaviors of Prosecutors), 29.10.2014. https://www.spp.gov.cn/spp/zdgz/201410/t20141029_82786.shtml, visited at 01.02.2021.

Carr, James G./*Bellia*, Patricia L./*Creutz*, Evan A.: The Law of Electronic Surveillance. Thomson Reuters, 2020.

Chauveau, Adolphe/*Hélie*, Faustin-Adolphe: Théorie du Code Pénal, Band 2, 1837.

Chen, Guangzhong (陈光中): 刑事诉讼法 (Criminal Procedure Law), 5th ed. Beijing University Press, 2013.

Chen, Ruihua (陈瑞华): 论瑕疵证据补正规则 (Rules on Repair of Defective Evidence), 法学家 (Legal Scholar) 2 (2012), 66.

– 论监察委员会的调查权 (Inspection Power of the Supervision Committees), 中国人民大学学报 (Review of Renmin University) 4 (2018), 10.

Chen, Weidong (陈卫东): 2012刑事诉讼法修改条文理解与适用 (The Interpretation and the Application of the Modified Provisions in the Criminal Procedure Law 2012). China Legal Publishing House, 2012.

– 丰富庭前会议功能助力法庭集中审理 (To Promot the Concentration of Trials by Enriching the Function of Pre-trial Meeting), 人民法院报 (People's Court Daily) 24.02.2017.

– 理性审视技术侦查立法 (A Rational Review of the Legislation of Technological Investigations), 法治日报 (Legal Daily) 21.09.2011.

Chen, Weidong (陈卫东)/*Nie*, Youlun (聂友伦): 职务犯罪监察证据若干问题研究 (Problems on Evidence from Supervision Activities in Duty Offenses), 中国人民大学学报 (Review of Chinese Renmin University) 4 (2018), 2.

Cheng, Lei (程雷): "侦查"的定义的修改与监察调查权" (The Modification of the Definition of "Investigation" and the Inspection Power of the Supervision Committees), 国家检察官学院学报 (Review of the National College of Prosecutors) 26 (2018), 125.

– 技术侦查证据使用问题研究 (Problems on the Evidence from the Technological Investigative Measures), 法学研究 (Legal Research) 5 (2018), 153.

Clancy, Thomas K.: What Does the Fourth Amendment Protect: Property, Privacy, or Security, Wake Forest Law Review 33 (1998), 307.

Cloud, Morgan: Pragmatism, Positivism, and Principles in Fourth Amendment Theory, UCLA Law Review 41 (1993), 199.

Cohen-Eliya, Moshe/*Porat*, Iddo: Proportionality and the Culture of Justification, American Journal of Comparative Law 59 (2011), 463.

– Proportionality and Constitutional Culture. Cambridge University Press, 2013.

Colb, Sherry F.: The Qualitative Dimension of Fourth Amendment "Reasonableness", Columbia Law Review 98 (1998), 1642.

Correa Robles, Carlos: Die Fernwirkung der Beweisverbote. Peter Lang, 2018 (cited: Die Fernwirkung).

*Criminal Law Division of the Standing Committee of Chinese National Parliament (*全国人大常委会法制工作委员会刑法室*)* (ed.): 中华人民共和国刑事诉讼法:条文说明、

立法理由及相关规定 (Criminal Procedure Law of People's Republic of China: Interpretation of Texts, Reasons of Law-making and Related Rules). Beijing University Press, 2008.

– 中华人民共和国刑法:条文说明、立法理由及相关规定 (Criminal Law of People's Republic of China: Interpretation of Texts, Reasons of Law-making and Related Rules). Beijing University Press, 2009.

Daiber, Birgit: Verhältnismäßigkeit im engeren Sinne, JA 2020, 37.

Davies, Thomas Y.: A Hard Look at What We Know (And Still Need to Learn) about the "Costs" of the Exclusionary Rule. The NIJ Study and Other Studies of "Lost" Arrests, American Bar Foundation Research Journal 8 (1983), 611.

Deckers, Rüdiger: Geheime Aufklärung durch Einsatz technischer Mittel, StraFo 2002, 109.

Deckers, Rüdiger/*Gercke*, Björn: Strafverteidigung und Überwachung der Telekommunikation, StraFo 2004, 84.

Dencker, Friedrich: Verwertungsverbote im Strafprozess. Ein Beitrag zur Lehre von den Beweisverboten. Heymanns, 1977.

Dezza, Ettore: Geschichte des Strafprozessrechts in der Frühen Neuzeit. Springer, 2017.

Dickerson, Oliver Morton: Writs of Assistance as a Cause of the American Revolution, in: *Morris*, R. (ed.), The Era of the American Revolution: Studies Inscribed to Evarts Boutell Greene. Columbia University Press, 1939, p. 40.

Doenges, William S.: Search and Seizure: The Physical Trespass Doctrine and the Adaptation of the Fourth Amendment to Modern Technology, Tulsa Law Journal 2 (1965), 180.

Dong, Kun (董坤): 论技术侦查证据的使用 (The Use of Evidence from Technological Investigation), 四川大学学报 (哲学社会科学版) (Review of Sichuan University·Philosophy and Social Science) 3 (2012), 151.

Dorsch, Claudia: Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO. Duncker & Humblot, 2005.

Douse, Steven C.: The Concept of Privacy and the Fourth Amendment, University of Michigan Journal of Law Reform 6 (1972), 154.

Doyle, Charles: Privacy: An Overview of the Electronic Communications Privacy Act (CRS Report R41733), 2012 (cited: Privacy).

Du, Meng (杜萌): "河南非法证据排除第一大案"庭审纪实 (Trial Record of "Very First Case on the Exclusion of Illegal Evidence in Henan Province"), 法制日报 (Legal Daily) 14/10/2013.

Du, Qiangqiang (杜强强): 论宪法规范与刑法规范之诠释循环 –以入户抢劫与住宅自由概念为例 (The Interpretation of Constitutional and Criminal Norms-Robbery with Housebreaking and Freedom of Residence as Example), 法学家 (Legal Scholar) 2 (2015), 15.

Dubber Markus D./*Hörnle*, Tatjana: Criminal Law: A Comparative Approach. Oxford University Press, 2014.

Dumbs, Mathias: Die Entwicklung des Grundsatzes der Verhältnismäßigkeit in der Rechtsprechung des Bundesverfassungsgerichts. Verlag Wissenschaft & Öffentlichkeit, 2015.

Duttge, Gunnar: Abhören von Gesprächen mit Angehörigen im Besucherraum der Untersuchungshaftanstalt, JZ 1999, 261.

Eder, Florian: Beweisverbote und Beweislast im Strafprozess. utz, 2015.

Edlin, Douglas E.: Judges and Unjust Laws. The University of Michigan Press, 2011.

Eisenberg, Ulrich: Beweisrecht der StPO, 10. Auflage. C.H. Beck, 2017.

Epping, Volker/*Hillgruber*, Christian (Hrsg.): BeckOK Grundgesetz, 46. Ed. C.H. Beck, 2021.

Fabri, Marco: Four Criminal Procedure Case Studies in Comparative Perspectives: China-Italy-Russia-U.S.A. Nomos, 2016.

Fezer, Gerhard: Grundfragen der Beweisverwertungsverbote, C.F. Müller, 1995. Überwachung der Telekommunikation und Verwertung eines „Raumgesprächs", NStZ 2003, 625.

Fishman, Clifford S./*McKenna*, Anne: Wiretapping and Eavesdropping, Westlaw Database, 2015.

– Wiretapping and Eavesdropping. Thomson Reuters, 2019.

Fishman, Clifford S.: The Minimization Requirement in Electronic Surveillance: Title III, the Fourth Amendment, and the Dread Scott Decision, American University Law Review 28 (1979), 315.

– Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice, Georgia Law Review 22 (1987), 1.

Fradella, Henry F./*Morrow*, Weston J./*Fischer*, Ryan G./*Ireland*, Connie: Quantifying Katz: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context, American Journal of Criminal Justice 38 (2011), 289.

Franck, Thomas M.: Proportionality in International Law, Law and Ethics of Human Rights 4 (2010), 46.

Friedman, Joshua T.: The Sixth Amendment, Attorney-Client Relationship and Government Intrusions: Who Bears the Unbearable Burden of Proving Prejudice?, Washington University Journal of Urban and Contemporary Law 40 (1991), 109.

Gao, Wenying (高文英)/*Xing*, Jie (邢捷): 警察法学 (Law of Police). China University of Political Science and Law Press, 2017.

Gardner, Thomas J./*Anderson*, Terry M.: Criminal Evidence: Principles and Cases,. 3rd ed. West Publishing Company, 1995.

Garner, Bryan A. (ed.): Black's Law Dictionary, 10th ed. Thomson West, 2014.

Gless, Sabine: Germany: Balancing Truth Against Protected Constitutional Interests, in: Thaman, Stephen (ed.), Exclusionary Rules in Comparative Law. Springer, 2013, p. 113.

Goldsworthy, Jeffrey: Constitutional Interpretation, in: Rosenfeld, Michel/Sajó, András (eds.), The Oxford Handbook of Comparative Constitutional Law, Oxford University Press, 2013, p. 689 (cited: Handbook).

Göres, Ulrich L./*Kleinert*, Jens: Die Liechtensteinische Finanzaffäre – Steuer- und steuerstrafrechtliche Konsequenzen, NJW 2008, 1353.

Graf, Jürgen (Hrsg.): BeckOK StPO mit RiStBV und MiStra, 39. Edition. C.H. Beck, 2021.

Greenawalt, Kent: Statutory and Common Law Interpretation. Oxford University Press, 2013.

Greenleaf, Simon: A Treatise on the Law of Evidence, 12th ed., carefully rev., with large additions, by Isaac F. Redfield, Little, Brown, 1866.

Grünwald, Gerald: Beweisverbote und Verwertungsverbote im Strafverfahren, JZ 1966, 489.

Guo, Hua (郭华): 我国检察机关侦查权调整及其互涉案件程序的探讨 (Restructure of the Investigative Power of the Prosecution Offices and the Procedure), 法治研究 (Research on Rule of Law) 1 (2019), 26.

Gusy, Christoph: Anmerkung zu BVerfG, 20. 2. 2001 – 2 BvR 1444/00, JZ 2001, 1033.

Han, Dayuan (韩大元): 1954年宪法与中国宪政 (The 1954 Constitution and Chinese constitutionalism), 2nd ed. Wuhan University Press, 2008.

Hannich, Rolf (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung, 8. Auflage. C.H. Beck, 2019.

Herrmann, Joachim: Aufgaben und Grenzen der Beweisverwertungsverbote, in: Vogler, Theo (Hrsg.), Festschrift für Hans-Heinrich Jescheck zum 70. Geburtstag. Duncker & Humblot, 1985, 1291.

Hilger, Hans: Neues Strafverfahrensrecht durch das OrgKG, NStZ 1992, 457.

Hirschberg, Lothar: Der Grundsatz der Verhältnismäßigkeit. Schwartz, 1981.

Hodgson, Jacqueline S./*Mou*, Yu: Empirical Approaches to Criminal Procedure, in: Brown, Darryl K./Turner, Jenia I./Weisser, Bettina (Hrsg.), The Oxford Handbook of Criminal Process. Oxford University Press, 2019, p. 43.

Howard, George Elliott: Preliminaries of the Revolution, 1763–1775. Harper, 1905.

Hsieh, Kuo-hsing: The Exclusionary rule of Evidence. Comparative Analysis and Proposals for Reform. Routledge, 2014.

Hu, Jinguang (胡锦光)/*Han*, Dayuan (韩大元): 中国宪法 (Chinese Constitutional Law), 4th ed. Law Press, 2018.

Hu, Zhonghui (胡忠惠): 基于实证观察的我国非法证据排除规则研 (Empirical Research on Chinese Exclusionary Rule of Illegal Evidence). China University of Political Science and Law Press, 2018.

Huang, Lihong (黄利红): 住宅不受侵犯权研究 (Inviolability of Residence). Intellectual Property Publishing House, 2014.

Huang, Xiangqing (黄祥清): 抢劫罪情节加重犯的认定思路与方法 (Approach to Determination of Aggravated Circumstances for Robbery), 政治与法律 (Political Science and Law) 6 (2005), 138.

Huber, Ernst Rudolf: Dokumente zur deutschen Verfassungsgeschichte, Band III. W. Kohlhammer, 1990.

Hubmann, Heinrich: Wertung und Abwägung im Recht. Heymanns, 1997.

Hutchinson, Thomas: The History of the Colony of Massachusetts Bay, 3 vols. 1764–1828.

Hyatt, Seth M.: Text Offenders: Privacy, Text Messages, and the Failure of the Title in Minimization Requirement, Vanderbilt Law Review 64 (2011), 1347.

Jäger, Christian: Beweisverwertung und Beweisverbote im Strafprozess. C.H. Beck, 2003.

– Du sollst nicht von Dritten profitieren!, JA 2017, 74.

Jahn, Matthias/*Dallmeyer*, Jens: Zum heutigen Stand der beweisrechtlichen Berücksichtigung hypothetischer Ermittlungsverläufe im deutschen Strafverfahrensrecht, NStZ 2005, 297.

Jahn, Matthias: Verhandlungen des 67. Deutschen Juristentages Erfurt 2008, Band I: Gutachten/Teil C: Beweiserhebung und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus. C.H. Beck, 2008 (cited: Gutachten 67. DJT 2008, CI).

Janker, Helmut: Zur Reichweite der Eingriffsermächtigung des § 100 c I Nr. 2 StPO bei Abhörmaßnahmen in Kraftfahrzeugen, NJW 1998, 269.

Ji, Weidong (季卫东): 中国宪法改革的途径与财产权问题 (The Reform Approach to Chinese Constitution and the Problem of Property Right), 当代中国研究 (Modern China Studies) 3 (1999), 48.

– 宪法的理念与中国实践 (The Constitutional Idea and Chinese Practice). Shanghai People's Publishing House, 2017.

Jiang, Ming'an (姜明安): 国家监察法立法的若干问题探讨 (Discussions on Legislating Problems of the Supervision Law), 法学杂志 (Law Science Magazine) 3 (2017), 1.

Jirard, Stephanie A.: Criminal Law & Procedure. Sage, 2019.

Joecks, Wolfgang: Die strafprozessuale Telefonüberwachung, JA 1983, 59.

Jones, Robert E./*Rosen*, Gerald E./*Wegner*, William E./*Jones*, Jeffrey S.: Federal Civil Trials and Evidence. Rutter Group, 2020.

Jugl, Benedikt: Fair trial als Grundlage der Beweiserhebung und Beweisverwertung im Strafverfahren. Nomos, 2016 (cited: Fair trial).

Julie, Richard S.: High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age, American Criminal Law Review 37 (2000), 127.

Junker, John M.: The Structure of the Fourth Amendment: The Scope of the Protection, Journal of Criminal Law & Criminology 79 (1989), 1105.

Kamin, Sam/*Marceau*, Justin: Double Reasonableness and the Fourth Amendment, University of Miami Law Review 68 (2014), 589.

Kaplan, Howard J./*Matteo*, Joseph A./*Sillet*, Richard: The History and Law of Wiretapping, (Paper delivered at the ABA Section of Litigation 2012 Annual Conference, April 18–20, 2012).

Karaaslanoglu, Ugur: Beweisverbote im deutschen und im türkischen Strafverfahrensrecht. Logos, 2015.

Kaspar, Johannes: Strafprozessuale Verwertbarkeit nach rechtswidriger privater Beweisbeschaffung – Zugleich ein Beitrag zur Systematisierung der Beweisverbotslehre, GA 2013, 206.

Keiler, Johannes/*Roef*, David (ed.): Comparative Concepts of Criminal Law, 3rd ed. intersentia, 2019.

Kelnhofer, Evelyn: Hypothetische Ermittlungsverläufe im System der Beweisverbote. Duncker & Humblot, 1994.

Kerr, Orin S.: The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, Michigan Law Review 102 (2004), 801.

King, Karen E./*Kilby*, Matthew B.: Fifth Amendment at Trial, Georgetown Law Journal 90 (2002), 1690.

Kitch, Edmund W.: Katz v. United States: The Limits of the Fourth Amendment, Supreme Court Review 1968, 133.

Klatt, Matthias/*Meister*, Moritz: Der Grundsatz der Verhältnismäßigkeit, JuS 2014, 193.

Knauer, Christoph (Hrsg.): Münchener Kommentar zur StPO, Band III, 1. Auflage. C.H. Beck, 2019.

Kölbel, Ralf: Zur Verwertbarkeit privat-deliktisch beschaffter Bankdaten– Ein Kommentar zur causa „Kieber", NStZ 2008, 241.

Koutnatzis, Stylianos-Ioannis G.: Verfassungsvergleichende Überlegungen zur Rezeption des Grundsatzes der Verhältnismäßigkeit in Übersee, VRÜ 44 (2011), 32.

Kudlich, Hans (Hrsg.): Münchener Kommentar zur StPO, Band I, 1. Auflage. C.H. Beck, 2014.

LaFave, Wayne R./*Israel*, Jerold H.: Handbook Criminal Procedure. West Publishing, 1992.

LaFave, Wayne R./*Israel*, Jerold H./*Kerr*, Orin S./*King*, Nancy J.: Criminal Procedure. Thomson Reuters, 2020.

LaFave, Wayne R.: Search and Seizure: A Treatise on the Fourth Amendment. Thomson West, 2020.

Landau, Herbert: Die Pflicht des Staates zum Erhalt einer funktionstüchtigen Strafrechtspflege, NStZ 2007, 121.

Lang, Sheng (郎胜) (ed.): 〈中华人民共和国刑事诉讼法〉修改与适用 (Modification and Application of Chinese Criminal Procedure Law). Xinhua Press, 2012.

Leeuw, Frans L.: Empirical Legal Research. A Guidance Book for Lawyers, Legislators and Regulators. Edward Elgar, 2017.

Lerner, Craig S.: The Reasonableness of Probable Cause, Texas Law Review 81 (2003), 951.

Lesch, Heiko: Funktionale Rekonstruktion der Lehre von den Beweisverboten, in: Hassemer, Winfried/Kempf, Eberhard/Moccia, Sergio (Hrsg.), In Dubio Pro Libertate. Festschrift für Klaus Volk zum 65. Geburtstag. C.H. Beck, 2009, S. 311.

Li, Jian (李剑)/*Yang*, Wei (杨威): 律师请王海代理索讨通信秘密权案 (Lawyer Hai WANG Represented Lawyers to Sue for the Right to Confidence of the Correspondence), 法治日报 (Legal Daily) 23. 12. 2002.

Li, Kun (李锟): 技术侦查证据质证的实践困境及其出路 (The Dilemma of the Cross Examination of the Evidence from the Technological Investigative Measures and the Resolutions), 法治论坛 (Forum of Rule of Law) 50 (2018), 105.

Li, Ming (李明): 刑事诉讼中私人监听问题研究 (Private Interceptions in Criminal Procedure), 河北法学 (Hebei Law) 11 (2005), 7 .秘密侦查法律问题研究(Research on

Legal Problems of Covert Investigations). China University of Political Science and Law Press, 2016.

Li, Yang (李洋): 通信自由的保护与限制 (Protection and Restriction on the Freedom of Correspondence), 中国电信业 (Chinese Telecommunication) 118 (2010), 46.

Liao, Bin (廖斌)/*Zhang*, Zhong (张中): 技术侦查规范化研究 (Research on the Normalisation of Technological Investigation). Law Press, 2015.

Lin, Laifan (林来梵): 宪法学讲义 (Textbook on the Constitutional Law), 2nd ed. Law Press, 2015. –从宪法规范到规范宪法 –规范宪法学的一种前言 (From Constitutional Norm to Normativ Constitution – Foreword to Normative Constitution). The Commercial Press, 2017.

Lippke, Richard L.: Fundamental Values of Criminal Procedure, in: Brown, Darryl K./Turner, Jenia I./Weisser, Bettina (Hrsg.), The Oxford Handbook of Criminal Process. Oxford University Press, 2019, p. 26.

Lippman, Matthew: Criminal Procedure, 4th ed. Sage, 2020.

Liu, Ang (刘昂): <监察法>实施中的证据合法性问题研究 (Research on the Legality of Evidence during the Enforcement of the Supervision Law), 证据科学 (Evidence Science) 26 (2018), 410.

Liu, Juan (刘娟): 人格尊严及其实现 –道德与法的双重考量 (Human Dignity and Ist Realisation – Double Consideration from Morality and Law). China University of Political Science and Law Press, 2014.

Liu, Yanhong (刘艳红): 监察委员会调查权运作的双重困境及其法治路径 (The Dilemma and the Legal Approach of the Inspection Power of the Supervision Committees), 法学论坛 (Legal Forum) 6 (2017), 5.

Lockard, Kathleen: Qualified Immunity as a Defense to Federal Wiretap Act Claims, University of Chicago Law Review 68 (2001), 1369.

Lockhart, James: What Constitutes Compliance by Government Agents with Requirement of 18 U.S.C.A. § 2518(5) that Wire Tapping and Electronic Surveillance Be Conducted in such Manner as to Minimize Interception of Communications Not Otherwise Subject to Interception, American Law Reports, Federal 181 (2002), 419.

Löffelmann, Markus: Die normativen Grenzen der Wahrheitserforschung im Strafverfahren. de Gruyter, 2008.

Lohberger, Ingram: Mittelbare Verwertung sog. Zufallserkenntnisse bei rechtmäßiger Telefonüberwachung nach §§ 100a, b StPO?, in: Ebert, Udo/Roxin, Claus/Rieß, Peter/Wahle, Eberhard (Hrsg.): Festschrift für Ernst-Walter Hanack zum 70. Geburtstag. de Gruyter, 1999, 253.

Long, Edward V.: The intruders. Praeger, 1967.

Löwe/Rosenberg (Hrsg.): Die Strafprozessordnung und das Gerichtsverfassungsgesetz. de Gruyter.

– Band IX, 26. Auflage, 2010.

– Band III/1, 27. Auflage, 2018.

– Band. IV/1, 27. Auflage, 2019.

– Band IV/2, 27. Auflage, 2020.

Luo, Yilong (罗一龙): 公安执法适用非法证据排除规则的实证研究 (Empirical Studies on the Application of Exclusionary Rules on Illegal Evidence by Police during Enforcing the Law), 政法学刊 (Journal of Political Science and Law) 28 (2011), 71.

Ma, Mingliang (马明亮)/*Zhang*, Penghao (张彭皓): 探讨"审判之前的审判"模式 (Discussion on the Model of "Trial before Trial"), 甘肃政法学院学报 (Review of Gansu College of Political Science and Law) 4 (2018), 59.

Mack, Renata Lawson: Comparative Criminal Procedure: History, Processes and Case Studies. William s Hein & Co, 2008.

Maclin, Tracey: The Supreme Court and the Fourth Amendment's Exclusionary Rule. Oxford University Press, 2012.

Mahlstedt, Tobias: Die verdeckte Befragung des Beschuldigten im Auftrag der Polizei. Duncker & Humblot, 2011.

Mangano, Basil W.: The Communications Assistance for Law Enforcement Act and Protection of Cordless Telephone Communications: The Use of Technology as a Guide to Privacy, Cleveland State Law Review 44 (1996), 99.

Mangoldt von/Klein/Starck, Kommentar zum Grundgesetz, Band I, 7. Auflage. C.H. Beck, 2018.

Maunz, Theodor/*Dürig*, Günter (Hrsg.), Kommentar zum Grundgesetz, Band I. C.H. Beck, August 2020.

McCabe, Neil Colman: Legislative Facts as Evidence in State Constitutional Search Analysis, Temple Law Review 65 (1992), 1229.

McEwan, J.: Ritual, Fairness and Truth: The Adversarial and Inquisitorial Models of Criminal Trial, in: Duff, R. A./Farmer, Lindsay/Marshall, Sandra/Tadros, Victor (ed.), The Trial on Trial – Volume 1: Truth and Due Process. Hart Publishing, 2004, p. 51.

Mcinnis, Thomas N.: The Evolution of the Fourth Amendment. Lexington, 2009.

Meyer-Goßner/Schmitt, Strafprozessordnung, 63. Auflage. C.H. Beck, 2020.

Michael, Lothar: Grundfälle zur Verhältnismäßigkeit, JuS 2001, 654.

Möller, Hauke: Verfassungsrechtliche Überlegungen zum »nemo-tenetur«-Grundsatz und zur strafmildernden Berücksichtigung von Geständnissen, JR 2005, 314.

Müller, Kai/*Trurnit*, Christoph: Eilzuständigkeiten der Staatsanwaltschaft und des Polizeivollzugsdienstes in der StPO, StraFo 2008, 144.

Nardulli, Peter F.: The Societal Cost of the Exclusionary Rule: An Empirical Assessment, American Bar Foundation Research Journal 8 (1983), 585.

Nardulli, Peter F.: The Societal Cost of the Exclusionary Rule: An Empirical Assessment, American Bar Foundation Research Journal 8 (1983), 585.

Ni, Bo (倪波): 从住宅不受侵犯权看高校对学生宿舍的检查 (Study on the Checking of Students' Dormitories by the University from the Perspective of the Inviolability of Residence), Master Thesis of Nanjing Normal University, 2016.

Note, A Reconsideration of the Katz Expectation of Privacy Test, Michigan Law Review 76 (1977), 154.

Note, From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection, New York University Law Review 43 (1968), 968.

Note, The Right to Privacy in Nineteenth Century America, Harvard Law Review 94 (1981), 1892.

Oreschnik, Bernhard: Verhältnismäßigkeit und Kontrolldichte. Springer, 2019.

Ossenberg, Sarah: Die Fernwirkung im deutsch-U.S.-amerikanischen Vergleich. Kovač, 2011 (cited: Die Fernwirkung).

Paeffgen, Hans-Ullrich, Überlegungen zu einer Reform des Rechts der Überwachung der Telekommunikation, in: Schünemann, Bernd u. a. (Hrsg.), Festschrift für Claus Roxin zum 70. Geburtstag. de Gruyter, 2001, S. 1299.

Paul, Tobias: Unselbständige Beweisverwertungsverbote in der Rechtsprechung, NStZ 2013, 489.

Pesciotta, Daniel T.: I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century, Case Western Reserve Law Review 63 (2012), 187.

Peters, Anne: Verhältnismäßigkeit als globales Verfassungsprinzip, in: Baade, v. Björnstjern/Ehricht, Sebastian/Fink, Matthäus/Frau, Robert u. a. (Hrsg.), Verhältnismäßigkeit im Völkerrecht. Mohr, 2016, S.1.

Petersen, Julie K.: Introduction to Surveillance Studies. CRC Press, 2013.

Pikowsky, Robert A.: The Need for Revisions to the Law of Wiretapping and Interception of Email, Michigan Telecommunications and Technology Law Review 10 (2003), 1.

Pitsch, Christoph: Strafprozessuale Beweisverbote. Kovac, 2009.

*Politics Sub-division of the Research Division of the Standing Committee of Chinese National Parliament (*全国人大常委会办公厅研究室政治组*)*:中国宪法精释(Interpretation of the Chinese Constitution). China Democracy Legal System Publishing House, 1996.

U.S. President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society, 1967.

Price, Robert: The Admissibility of Wiretap Evidence in the Federal Courts, University of Miami Law Review 14 (1959), 57.

Rieß, Peter: Über Subsidiaritätsverhältnisse und Subsidiaritätsklauseln im Strafverfahren, in: Dehnicke, Diether/Geppert, Klaus (Hrsg.), Gedächtnisschrift für Karlheinz Meyer. de Gruyter, 1990, S. 367 (cited: Meyer-GedSchr).

Roberson, Cliff: Constitutional Law and Criminal Justice, 2nd Edition. CRC Press, 2016.

Rogall, Klaus: Gegenwärtiger Stand und Entwicklungstendenzen der Lehre von den strafprozessualen Beweisverboten, ZStW 91 (1979), 1.

Rogall, Klaus: "Abwägungen" im Recht der Beweisverbote, in: Ebert, Udo u. a. (Hrsg.), Festschrift für Ernst-Walter Hanack zum 70. Geburtstag. de Gruyter, 1999, S. 293.

Roggan, Fredrik: Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung. Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, 821.

Rosenzweig, Margaret Lybolt: The Law of Wire Tapping, Cornell Law Quarterly 32 (1946–1947), 514.

Roxin, Claus/*Schünemann*, Bernd: Strafverfahrensrecht, 29. Auflage. C.H. Beck, 2017.

Rudolphi, Hans-Joachim: Die Revisibilität von Verfahrensmängeln im Strafprozeß, MDR 1970, 93.

Rudolphi, Hans-Joachim: Grenzen der Überwachung des Fernmeldeverkehrs nach den §§ 100a, b StPO, in: Grünwald, Gerald (Hrsg.), Festschrift für Friedrich Schaffstein zum 70. Geburtstag. Schwartz, 1975, S. 433.

Sachs, Micheal (Hrsg.): Grundgesetz Kommentar, 9. Auflage. C.H. Beck, 2021.

Schenke, Ralf P.: Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, Archiv des Öffentlichen Rechts 125 (2000), 1.

Schilling, Hellen: Illegal Beweise. Eine Untersuchung zum Beweisverfahren im Strafprozess. Nomos, 2004.

Schlink, Bernhard: Proportionality, in: Rosenfeld, Michel/Sajó, András (eds.), The Oxford Handbook of Comparative Constitutional Law. Oxford University Press, 2013, p. 719.

Schmidt, Eberhard: Die Verletzung der Belehrungspflicht gemäß § 55 II StPO als Revisionsgrund, JZ 1958, 596.

Schneider, Hartmut: Zur Zulässigkeit strafprozessualer Begleitmaßnahmen im Zusammenhang mit dem Abhören des nicht öffentlich gesprochenen Wortes in Kraftfahrzeugen, NStZ 1999, 388.

Schönke/Schröder, Strafgesetzbuch, 30. Auflage. C.H. Beck, 2019.

Schröder, Svenja: Beweisverwertungsverbote und die Hypothese rechtmäßiger Beweiserlangung im Strafprozeß. Duncker & Humblot, 1992 (cited: Beweisverwertungsverbote).

Shaff, Colin: Is the Court Allergic to Katz? Problems Posed by New Methods of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test, Southern California Interdisciplinary Law Journal 23 (2014), 409.

Shields, Marjorie A.: Who May Apply or Authorize Application for Order to Intercept Wire or Oral Communications Under Title III of Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. §§ 2510 et seq.), American Law Reports, Federal 169, 169.

Sievers, Malte: Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes. Nomos, 2003.

Simmons, Ric: Smart Surveillance. How to Interpret the Fourth Amendment in the Twenty-First Century. Cambridge University Press, 2019, p. 14.

Simons, Michael A.: Prosecutorial Discretion and Prosecution Guidelines: A Case Study in Controlling Federalization, New York University Law Review 75 (2000), 893.

Singelnstein, Tobias: Rechtsschutz gegen heimliche Ermittlungsmaßnahmen nach Einführung des § 101 VII 2–4 StPO, NStZ 2009, 481.

– Strafprozessuale Verwendungsregelungen zwischen Zweckbindungsgrundsatz und Verwertungsverboten, ZStW 120 (2008), 854.

Slobogin, Christopher: Privacy at Risk: New Government Surveillance and the Fourth Amendment. University of Chicago Press, 2007.

Smith, Maurice Henry: The Writs of Assistance Case. University of California Press, 1978.

Sobel, Richard/*Horwitz*, Barry/*Jenkins*, Gerald: The Fourth Amendment Beyond Katz, Kyllo and Jones: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy, Boston University Public Interest Law Journal 22 (2013), 1.

Sowada, Christoph: Beweisverwertungsverbote im Spannungsfeld zwischen nemo-tenetur-Grundsatz und fair-trial-Prinzip, in: Geisler, Claudius (Hrsg.), Festschrift für Klaus Geppert zum 70. Geburtstag. de Gruyter, 2011, S. 689.

Spencer, J. R.: *Evidence*, in: Spencer, J. R./Delmas-Marty, Mireille (eds.), European Criminal Procedures. Cambridge University Press, 2005, p. 594.

*Standing Committee of the National Parliament (*全国人大常委会*)*: 2004 年 4 月 9日关于"宪法"第 40 条的法律询问答复 (Response to the Question on Art. 40 of the Chinese Constitution on 9th April, 2004), 中国人大 (Chinese Parliament) 13 (2004).

Stephens, Otis H./*Glenn*, Richard A.: Unreasonable Searches and Seizures: Rights and Liberties under the Law. ABC-CLIO, 2006.

Stoffer, Hannah: Wie viel Privatisierung "verträgt" das strafprozessuale Ermittlungsverfahren?, Mohr Siebeck, 2016 (cited: Wie viel Privatisierung).

Sun, Maoli (孙茂利): 公安机关刑事法律文书制作指南与范例 (Instructions and Examples of Legal Documents in Criminal Issues used by Public Security). China Chang'an Press, 2015.

Sun, Yuhua (孙煜华): 何为"严格的批准手续" (What is the "Strict Approval Procedure"), 环球法律评论 (Global Law Review) 4 (2013), 33.

Sweet, Alec Stone/*Mathews*, Jud: Proportionality, Judicial Review, and Global Constitutionalism, in: Bongiovanni, Giorgio/Sartor, Giovanni/Valentini, Chiara (eds.), Reasonableness and Law. Springer, 2009, p. 171.

Tang, Zhongmin (唐忠民): 公民通信自由和通信秘密保护的两个问题 (Two Problems on the Protection of the Freedom and the Confidence of Correspondence), 法学 (Law) 12 (2017), 13.

Tants, Malte: Beweisverwertungsverbote im Rahmen einer „Gesamtschau in der Rechtsprechung". Kovač, 2020.

Taylor, Telford: Two Studies in Constitutional Interpretation: Search, Seizure, and Surveillance and Fair Trial and Free Press. Ohio State University Press, 1969.

– Wiretapping and Eavesdropping. Westlaw Database, updated December 2015.

Trüg, Gerson/*Habetha*, Jörg: Beweisverwertung trotz rechtswidriger Beweisgewinnung – insbesondere mit Blick auf die "Liechtensteiner Steueraffäre", NStZ 2008, 481.

Turner, Jenia Iontcheva/*Weigend*, Thomas: The Purpose and Functions of Exclusionary Rules: A Comparative Overview, in: Gless, Sabine/Richter, Thomas (Hrsg.), Do Exclusionary Rules Ensure a Fair Trial?. Springer, 2019, p. 255.

United States National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, Commission Hearings:

– May 20, 1975, William V. Cleveland, Assistant Director in Charge of Special Investigations, Organized Crime Division, Federal Bureau of Investigation (cited: *Cleveland*, NWC Commission Hearings, May 20, 1975).

– May 21, 1975, Thomas E. Kotoske, Attorney-in-Charge, San Francisco Organized Crime Strike Force, U.S. Department of Justice (cited: *Kotoske*, NWC Commission Hearings, May 21, 1975).

– June 10, 1975, Richard Uviller, Professor, Columbia University School of Law (cited: *Uviller*, NWC Commission Hearings, June 10, 1975).

– June 11, 1975, Edith Lapidus, Professor, Queens College, N. Y. (cited: *Lapidus*, NWC Commission Hearings, June 11, 1975).

United States National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance: Electronic surveillance: Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, Washington: The Commission, 1976 (cited: NWC report).

– Strategy and Tactics in the Prosecution and Defense of Complex Wire-Interception Cases, Washington: The Commission, 1976.

Vassilaki, Irini E.: Die Überwachung des Fernmeldeverkehrs nach der Neufassung der §§ 100a, 100b StPO. Erweiterung von staatlichen Grundrechtseingriffen?, JR 2000, 446.

Verrel, Torsten: Selbstbelastungsfreiheit und Täuschungsverbot bei verdeckten Ermittlungen, in: Paeffgen, Hans-Ullrich/Böse, Martin/Kindhäuser, Urs/Stübinger, Stephan et al. (Hrsg.), Strafrechtswissenschaft als Analyse und Konstruktion. Festschrift für Ingeborg Puppe zum 70. Geburtstag. Duncker & Humblot, 2011, S. 1629.

Voßkuhle, Andreas: Grundwissen – Öffentliches Recht: Der Grundsatz der Verhältnismäßigkeit, JuS 2007, 429.

Wahl, Rainer: Der Grundsatz der Verhältnismäßigkeit: Ausgangslage und Gegenwartsproblematik, in: Heckmann, Dirk/Schenke, Ralf P./Sydow, Gernot (Hrsg.), Verfassungsstaatlichkeit im Wandel. Duncker & Humblot, 2013, S. 823.

Wang, Chao (王超): 非法证据排除调查程序难以激活的原因与对策 (Reasons for the Difficulties of Initiating Process on Excluding Illegal Evidence and its Resolutions), 政治与法律 (Political Science and Law) 6 (2013), 142.

Wang, Fuchun (王复春): 论非法侵入住宅罪客观构成要件符合性的判断 (The Compliance to the Objective Constructive Elements of Illegal Invasion to Residence), 河南财经政法大学学报 (Law Review of Henan University of Business and Political Science) 2 (2016), 97.

Wang, Haiyan (汪海燕)/*Ma*, Kang (马康): 监听中的非法证据排除规则的适用 (The Application of the Exclusionary Rule to the Illegal Evidence from Interception), 中国法学教育研究 (Research on Chinese Legal Education) 3 (2013), 148.

Wang, Konglin (王孔林): 巴南女教师性骚扰案宪法性分析 (Constitutional Analysis on Sexual Harassment on Female Teacher in Banan), Mater Thesis in Chinese Southwest University of Political Science and Law, 2008.

Wang, Lizhi (王立志): 技术侦查措施中应对隐私权予以保护 (The Right to Privacy Should be Protected during the Technological Investigative Measures), 知与行 (Knowledge and Practice) 19 (2017), 67.

Wang, Xiuzhe (王秀哲): 隐私权的宪法保护 (Constitutional Protection on the Right to Privacy). Social Sciences Academic Press, 2007.

Warntjen, Maximilian: Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung. Nomos, 2007 (cited: Zwangsmaßnahmen).

Wei, Xiaona (魏晓娜): 定位与实效:庭前会议功能再审视 (Reconsideration of the Function of Pretrial Meetings), 北大法律评论 (Beijing University Law Review) 17 (2016), 2.

Weigend, Thomas: Using the Results of Audio-surveillance as Penal Evidence in the Federal Republic of Germany, Stanford Journal of International Law 24 (1988), 21.

– Entscheidungsanmerkung zu LG Frankfurt a. M. v. 9. 4. 2003, StV 2003, 436.

– Mobile Phones as a Source of Evidence in German Criminal Procedure, in: Essays in Honor of Masahito Innouye, Tokyo, 2019, p. 877.

Werle, Gerhard: Schutz von Vertrauensverhältnissen bei der strafprozessualen Fernmeldeüberwachung?, JZ 1991, 482.

Weßlau, Edda: Das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung. Auswirkungen auf den Strafprozess, in: Roggan, Fredrik (Hrsg.), Lauschen im Rechtsstaat. Zu den Konsequenzen des Urteils des Bundesverfassungsgerichts zum grossen Lauschangriff. Gedächtnisschrift für Hans Lisken. Berliner Wissenschafts, 2004, S. 47.

Wohlers, Wolfgang: Die Hypothese rechtmäßiger Beweiserlangung – ein Instrument zur Relativierung unselbständiger Verwertungsverbote?, in: Weßlau, Edda/Wohlers, Wolfgang (Hrsg.), Festschrift für Gerhard Fezer zum 70. Geburtstag. de Gruyter, 2008, S. 311.

– Die Nichtbeachtung des Richtervorbehalts, StV 2008, 434.

Wolter, Jürgen (Hrsg.): SK-StPO-Systematischer Kommentar zur Strafprozessordnung, Band II, 5. Auflage. Heymanns, 2016.

Wu, Hongyao (吴宏耀): 非法证据排除的规则与实效 (Rules and Practical Effects of the Exclusion of Illegal Evidence), 现代法学 (Modern Law Science) 36 (2014), 121.

– 论刑事诉讼法与监察法的制度衔接 (The Connection between the Criminal Procedure Law and the Supervision Law), 中国检察官 (Chinese Prosecutors) 23 (2018), 23.

Xue, Zhen (薛振)/*Xiong*, Lisi (熊理思): 技术侦查的规范适用 (Proper Application of Technological Investigation), 人民法院报 (People's Court Daily) 19. 09. 2018.

Yan, Zhaohua (闫召华): "名禁实允"与"虽令而不行":非法证据排除难研究 ("Applying despite Prohibition" and "Not Applying despite the Order": The Difficulties of Exclusion of Illegal Evidence), 法制与社会发展 (Law and Social Development) 2 (2014), 182.

Yang, Kaixiang (杨开湘): 宪法隐私权导论 (Introduction to the Right to Privacy in the Constitutional Law). China Legal Publishing House, 2010.

Yao, Jianlong (姚建龙)/*Yi*, Nana (尹娜娜): 监察法视野下职务违法与职务犯罪的界分 (The Distinction between Duty Defect and Duty Offense under the Supervision Law), 上海政法学院学报 (Review of Shanghai College of Political Science and Law) 6 (2018), 23.

Yi, Yanyou (易延友): 非法证据排除规则的立法表述与意义空间 –"刑事诉讼法》第 54 条第 1 款的法教义学分析" (Legislating Express and the Meaning of Exclusionary Rules on Illegal Evidence: Dogmatical Analysis on § 54 I Chinese Criminal Procedure Law), 当代法学 (Contemporary Law Review) 1 (2017), 38.

– 瑕疵证据的补正与合理解释 (Repair of Defective Evidence and its Rational Interpretation), 环球法律评论 (Global Law Review) 3 (2019), 19.

Yuan, Ming (元明): 侦查监督部门防止冤错案件浅议 (Discussion on the Supervision Departments on Investigations' Work on the Prevention of Wrong Convictions), 人民检察 (People's Procuratorial Semimonthly) 6 (2015), 26.

Zhang, Jinfan (张晋藩): 中国宪法史 (History of Chinese Constitutional Law). Jilin People's Publishing House, 2004.

Zhang, Jun (张军)/*Jiang*, Wei (姜伟)/*Tian*, Wenchang (田文昌): 新控辩审三人谈 (New Discussions among Three-the Prosecutor, Defense Lawyer and the Judge). Beijing University Press, 2014.

Zhang, Qianfan (张千帆): 宪法学导论 – 原理与应用 (Introduction of Constitution Theories – Principles and Application), 3rd ed. Law Press, 2014.

Zhang, Xinbao (张新宝): 延安 "黄碟案" 引发的法学思考 (Legal Consideration raised by Sexual Videos in Yan'an), 法学家 (Legal Scholar) 3 (2003), 15.

Zhang, Yuan (张媛): 北京开审非法证据排除第一案 (First Case on the Exclusion of Illegal Evidence in Beijing), 新京报 (New Beijing Daily) 14.09.2012.

Zhang, Yuyou (张友渔): 关于修改宪法的几个问题 (Several Issues on the Modification of the Constitution), 法学研究 (Research on Law)3 (1982), 1.

Zheng, Xi (郑曦): 论非法证据排除规则对监察委办理案件的适用 (The Application of Exclusionary Rules on Illegal Evidence on the Cases Dealt by Supervision Committees), 证据科学 (Evidence Science) 26 (2018), 420.

Zhou, Lingmin (周羚敏)/*Zhou*, Weimin (周卫民): 证据排除规则视野下的私人非法取证 (Exclusionary Rules on Illegal Collection of Evidence by Private Persons), 广西警官高等专科学校学报 (Journal of Guangxi Police Academy) 5 (2011), 14.

Zhou, Qiang (周强): 最高人民法院工作报 2017 (Work Report of the Supreme Court 2017). Law Press, 2017.

Zhou, Wei (周伟): 通信自由与通信秘密的保护问题 (Problems on the Protection of Freedom and Confidence of Correspondence), 法学 (Law) 6 (2006), 57.

– 宪法基本权利:原理·规范·应用 (Fundamental Rights in Constitutional Law: Principles·Norm·Application). Law Press, 2006.

Zhu, Fuhui (朱福惠)/*Wang*, Jianxue (王建学): 苏联1936年宪法与我国1954年宪法之比较研究 (The Comparative Study of the 1936 Constitution of Soviet Union and the 1954 Constitution in the People's Republic of China), in: Zhang, Qingfu (张庆福)/Han, Dayuan(韩大元) (eds.), 1954年宪法研究 (Research on 1954 Constitution). Chinese People's Public Security University Press, 2015, p. 59.

Zhu, Xiaoqing (朱孝清): 试论技术侦查在职务犯罪侦查中的适用 (On Application of Technical Investigation to Official Crimes Investigation), 国家检察官学院学报 (Review of the National College of Prosecutors) 12 (2004), 111.

Zöller, Mark A.: Heimlichkeit als System, StraFo 2008, 15.

Zuo, Weimin (左卫民): 热与冷:非法证据排除规则适用的实证研究 (Cold Welcome and Hot Discussion: Empirical Study of the Application of the Exclusion of Illegal Evidence), 法商研究 (Studies in Law and Business) 3 (2015), 151.

– 未完成的变革 (Unfinished Reform), 中外法学(Beijing University Law Journal) 27 (2015), 469.

Zuo, Weimin (左卫民)/*An*, Qi (安琪): 监察委员会调查权:性质、行使与规制的审思 (Inspection Power of the Supervision Committees: Consideration on the Nature, Practice and Rules), 武汉大学学报 (哲学社会科学版) (Review of Wuhan University) (Philosophy and Social Science Edition) 1 (2018), 100.

Zuo, Weimin (左卫民)/*Tang*, Qingyu (唐清宇): 制约模式:监察机关与检察机关的关系模式思考 (Mode of Control: The Relationship between Supervision Committees and Prosecution Offices), 现代法学 (Modern Law) 4 (2018), 18.

专家谈刑诉法修改:应避免技术侦查滥用侵犯人权 (Experts Discuss the Modification of Criminal Procedure Law: to Avoid Technological Investigative Measures from Infringing upon Human Rights), 人民日报 (China Daily) 12/10/2011.

"性骚扰"案女主角:法院取证违宪 (The Plaintiff of the Sexual Harassment Case: the Collection of Evidence by the Court is Unconstitutional), 成都商报 (Chengdu Business Post) 21.02.2006.

Index