5. ABSCHNITT
Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten, [verschlüsselter Nachrichten][1] und von Personen

Definitionen

§ 134. Im Sinne dieses Bundesgesetzes ist

1. „Beschlagnahme von Briefen" das Öffnen und Zurückbehalten von Telegrammen, Briefen oder anderen Sendungen, die der Beschuldigte abschickt oder die an ihn gerichtet werden,

2. „Auskunft über Daten einer Nachrichtenübermittlung" die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG), die nicht einer Anordnung gemäß § 76a Abs. 2 unterliegen, und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes),

2a. „Lokalisierung einer technischen Einrichtung" der Einsatz technischer Mittel zur Feststellung von geographischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer (IMSI) ohne Mitwirkung eines Anbieters (§ 92 Abs. 3 Z 1 TKG) oder sonstigen Dienstanbieters (§ 13, § 16 und § 18 Abs. 2 des E-Commerce-Gesetzes – ECG, BGBl. I Nr. 152/2001),

1 In Kraft vom 1. April 2020 bis 31. März 2025, BGBl. I 27/2018.

DIVISION 5
Seizure of letters, disclosure of data concerning transmission of messages, localizing a technical device, event-specific data storage, and surveillance of communication, [encrypted communication,][1] and persons

Definitions

§ 134. For the purpose of this Federal Code

1. 'seizure of letters' means opening and withholding telegrams, letters, or other mail sent by or addressed to the accused,

2. 'disclosure of data concerning transmission of messages' means the providing of information about usage data (§ 92 para. 3 subpara. 4 Telecommunications Act [Telekommunikationsgesetz (TKG)]), access data (§ 92 para. 3 subpara. 4a Telecommunications Act) that is not subject to a direction under § 76a para. 2, and geo-tracking data (§ 92 para. 3 subpara. 6 Telecommunications Act) of a telecommunication provider or an Information Society service (§ 1 para. 1 subpara. 2 Provision of Information Act [Notifikationsgesetz (NotifG)]),

2a. 'localizing a technical device' means the use of technical equipment to ascertain geographic locations and the international mobile subscriber identity (IMSI) numbers without involving a provider (§ 92 para. 3 subpara. 1 Telecommunications Act) or other service providers (§§ 13, 16, and 18 para. 2 E-Commerce Act [E-Commerce-Gesetz (ECG)], BGBl. No. 152/2001),

1 In force from 1 April 2020 until 31 March 2025, BGBl. I 27/2018.

2b. „Anlassdatenspeicherung“ das Absehen von der Löschung der in Z 2 genannten Daten (§ 99 Abs. 2 Z 4 TKG),

3. „Überwachung von Nachrichten“ das Überwachen von Nachrichten und Informationen, die von einer natürlichen Person über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) gesendet, übermittelt oder empfangen werden,

[3a. Überwachung verschlüsselter Nachrichten“ das Überwachen verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten und Informationen im Sinne von Z 3 sowie das Ermitteln damit im Zusammenhang stehender Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG durch Installation eines Programms in einem Computersystem (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden,][2]

4. „optische und akustische Überwachung von Personen“ die Überwachung des Verhaltens von Personen unter Durchbrechung ihrer Privatsphäre und der Äußerungen von Personen, die nicht zur unmittelbaren Kenntnisnahme Dritter bestimmt sind, unter Verwendung technischer Mittel zur Bild- oder Tonübertragung und zur Bild- oder Tonaufnahme ohne Kenntnis der Betroffenen,

5. „Ergebnis“ (der unter Z 1 bis 4 angeführten Beschlagnahme, Auskunft, Lokalisierung oder Überwachung) der Inhalt von Briefen (Z 1), die Daten einer

2 In Kraft vom 1. April 2020 bis 31. März 2025, BGBl. I 27/2018.

2b. ‘event-specific data storage’ means omitting to delete the data listed in subpara. 2 (§ 99 para. 2 subpara. 4 Telecommunications Act),

3. ‘surveillance of communication’ means monitoring communication and information sent, transmitted, or received by a natural person via a communication network (§ 3 subpara. 11 Telecommunications Act) or an Information Society service (§ 1 para. 1 subpara. 2 Provision of Information Act),

[3a. ‘surveillance of encrypted communication’ means monitoring messages that are sent, transmitted, or received with encryption and information within the meaning of subpara. 3 as well as the identification of related data within the meaning of § 76a [of this Code] and § 92 para. 3 subparas. 4 and 4a of the Telecommunications Act by installing software on a computer system (§ 74 para. 1 subpara. 8 Criminal Code [Strafgesetzbuch (StGB)], without the knowledge of the owner or other persons with power of disposition in order to break through encryptions when messages or information are sent, transmitted, or received,][2]

4. ‘video and audio surveillance of persons’ means the monitoring of a person’s conduct by breaking their privacy and of a person’s statements that are not meant for the direct attention of others by using technical equipment for video or audio transmission or video or audio recording without the knowledge of the person concerned,

5. ‘result’ (of the seizure, information, localizing or monitoring under subparas. 1 to 4) means the content of letters

2 In force from 1 April 2020 until 31 March 2025, BGBl. I 27/2018.

Nachrichtenübermittlung (Z 2), die festgestellten geographischen Standorte und zur internationalen Kennung des Benutzers dienenden Nummern (IMSI) (Z 2a), die gesendeten, übermittelten oder empfangenen Nachrichten und Informationen (Z 3), [die verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen im Sinne von Z 3 sowie damit in Zusammenhang stehende Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG (Z 3a)][3] und die Bild- oder Tonaufnahme einer Überwachung (Z 4).

(subpara. 1), data concerning transmission of messages (subpara. 2), the geographic locations and international mobile subscriber identity (IMSI) numbers ascertained (subpara. 2a), sent, transmitted or received messages or information (subpara. 3), [sent, transmitted, or received with encryption and information under subpara. 3 and related data within the meaning of § 76a [of this Code] and § 92 para. 3 subparas. 4 and 4a of the Telecommunications Act (subpara. 3a)],[3] and video and audio recordings of a surveillance (subpara. 4).

3 In Kraft vom 1. April 2020 bis 31. März 2025, BGBl. I No. 27/2018.

3 In force from 1 April 2020 until 31 March 2025, BGBl. I 27/2018.

Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten

§ 135. (1) Beschlagnahme von Briefen ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist.

(2) Auskunft über Daten einer Nachrichtenübermittlung ist zulässig,

1. wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird,

2. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann und der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt, oder

3. wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und auf Grund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können.

4. wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der

Seizure of letters, disclosure of data concerning transmission of messages, localizing a technical device, event-specific data storage, and surveillance of communication

§ 135. (1) It is permissible to seize letters if this is necessary to make inquiries about a criminal offence committed intentionally and punishable by imprisonment for more than one year.

(2) Disclosure of data concerning transmission of messages is permissible,

1. if and so long there is strong suspicion that the person affected by the disclosure has kidnapped or otherwise taken control of another person and if the disclosure of data is limited to messages believed to be transmitted, received, or sent by the accused during the deprivation of liberty,

2. if it is to be expected that the disclosure can contribute to inquiries about a criminal offence committed intentionally and punishable by imprisonment for more than six months and if the owner of the technical device that is or will be the source or destination of the transmission of messages expressly consents to the disclosure, or

3. if it is to be expected that the disclosure can contribute to inquiries about a criminal offence committed intentionally and punishable by imprisonment for more than one year and if because of particular material facts it is believed that through the disclosure data of the accused can be investigated.

4. if because of particular material facts it is expected that through the disclosure the whereabouts of an accused who has absconded or is absent and who is under

Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

(2a) Lokalisierung einer technischen Einrichtung ist in den Fällen des Abs. 2 Z 1, 3 und 4 ausschließlich zur Feststellung der in § 134 Z 2a genannten Daten zulässig.

(2b) Anlassdatenspeicherung ist zulässig, wenn dies aufgrund eines Anfangsverdachts (§ 1 Abs. 3) zur Sicherung einer Anordnung nach Abs. 2 Z 2 bis 4 oder einer Anordnung nach § 76a Abs. 2 erforderlich erscheint.

(3) Überwachung von Nachrichten ist zulässig,

1. in den Fällen des Abs. 2 Z 1,
2. in den Fällen des Abs. 2 Z 2, sofern der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Überwachung zustimmt,
3. wenn dies zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten Straftaten ansonsten wesentlich erschwert wäre und

a. der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder einer Straftat gemäß §§ 278 bis 278b StGB dringend verdächtig ist, oder

strong suspicion of having intentionally committed a criminal offence punishable by imprisonment for more than one year can be established.

(2a) In cases under para. 2 subparas. 1, 3 and 4, localizing a technical device is only permissible to ascertain the data listed in § 134 subpara. 2a.

(2b) Event-specific data storage is permissible based on a reasonable suspicion (§ 1 para. 3) if this appears necessary to ensure a direction under para. 2 subparas. 2 to 4 or a direction under § 76a para. 2.

(3) Surveillance of communication is permissible,

1. in cases under para. 2 subpara. 1,
2. in cases under para. 2 subpara. 2 if the owner of the technical device that is or will be the source or destination of the transmission of messages consents,
3. if this appears necessary for the inquiry about a criminal offence committed intentionally and punishable by imprisonment for more than one year or if the inquiry or prevention of a criminal offence committed or planned as part of a criminal association, terrorist association, or criminal organization (§§ 278 to 278b Criminal Code) would otherwise be significantly obstructed and

a. if the owner of the technical device that is or will be the source or destination of the transmission of messages is under strong suspicion for a criminal offence committed intentionally and punishable by imprisonment for more than one year or for a criminal offence under §§ 278 to 278b of the Criminal Code, or

b. because of particular material facts it is believed that the person under strong suspicion for the offence (lit. a) will be using or will establish a connection to the technical device;

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat (lit. a) dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde;

4. in den Fällen des Abs. 2 Z 4.

[Überwachung verschlüsselter Nachrichten

§ 135a. (1) Überwachung verschlüsselter Nachrichten ist zulässig:

1. in den Fällen des § 135 Abs. 2 Z 1,

2. in den Fällen des § 135 Abs. 2 Z 2, sofern der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, der Überwachung zustimmt, oder

3. in den Fällen des § 136 Abs. 1 Z 3 sowie wenn die Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre und

a. der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer solchen Straftat dringend verdächtig ist, oder

b. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde.

(2) Eine Überwachung verschlüsselter Nachrichten ist überdies nur dann zulässig,

4. in cases under para. 2 subpara. 4.

[Surveillance of encrypted communication

§ 135a. (1) Surveillance of encrypted communication is permissible:

1. in cases under § 135 para. 2 subpara. 1,

2. in cases under § 135 para. 2 subpara. 2 if the owner or the person with power of disposition over the computer system on which software to monitor encrypted communication is to be installed consents, or

3. in cases under § 136 para. 1 subpara. 3 and if the inquiry about a felony against life or limb or sexual integrity and autonomy punishable by imprisonment for more than five years would otherwise be pointless or would be significantly obstructed and

a. if the owner or the person with power of disposition over the computer system on which software to monitor encrypted communication is to be installed is under strong suspicion for such a crime, or

b. if because of particular material facts it is believed that a person under strong suspicion for such a crime will be using or will establish a connection to the computer system on which software to monitor encrypted communication is to be installed.

(2) Furthermore, surveillance of encrypted communication is only permissible if because of particular material facts it is believed that the software

sig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass das Programm

1. nach Beendigung der Investigationsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt wird, und

2. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt.

(3) Soweit dies zur Durchführung der Investigationsmaßnahme unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, Behältnisse zu durchsuchen und spezifische Sicherheitsvorkehrungen zu überwinden, um die Installation des Programms zur Überwachung verschlüsselter Nachrichten in dem Computersystem zu ermöglichen. Die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener sind soweit wie möglich zu wahren.][4]

4 In Kraft vom 1. April 2020 bis 31. März 2025, BGBl. I No. 27/2018.

1. upon completion of the investigative measure is dysfunctional or will be removed without any damage or interference to the computer system on which it was installed and to any data stored on that system, and

2. does not cause any permanent damage or interference to other computer systems on which no software for the surveillance of encrypted communication has been installed.

(3) It is permissible to enter into a particular dwelling or any other place protected by domiciliary rights, to search compartments, and to overcome specific security contrivances to enable the installation of the software for the surveillance of encrypted communication on the computer system if this is unavoidable to carry out the investigative measure. Rights of ownership and personal rights of the affected persons must be protected insofar as possible.][4]

4 In force from 1 April 2020 until 31 March 2025, BGBl. I No. 27/2018.

Gemeinsame Bestimmungen

§ 137. (1) Eine Überwachung nach § 136 Abs. 1 Z 1 kann die Kriminalpolizei von sich aus durchführen. Eine Anlassdatenspeicherung nach § 135 Abs. 2b ist von der Staatsanwaltschaft anzuordnen (§ 102). Die übrigen Ermittlungsmaßnahmen nach den §§ 135 bis 136 sind von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen, wobei das Eindringen in Räume nach [§ 135a Abs. 3 oder][5] § 136 Abs. 2 jeweils im Einzelnen einer gerichtlichen Bewilligung bedarf.

(2) (aufgehoben, BGBl. I Nr. 27/2018)

(3) Eine Anlassdatenspeicherung nach § 135 Abs. 2b darf nur für jenen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist, längstens jedoch für zwölf Monate; eine neuerliche Anordnung ist nicht zulässig. Sonstige Ermittlungsmaßnahmen nach §§ 135 bis 136 dürfen nur für einen solchen künftigen, in den Fällen des § 135 Abs. 2 auch vergangenen, Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist. Eine neuerliche Anordnung ist jeweils zulässig, soweit auf Grund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Ermittlungsmaßnahme Erfolg haben werde. Im Übrigen ist die Ermittlungsmaßnahme zu beenden, sobald ihre Voraussetzungen wegfallen.

5 In Kraft vom 1. April 2020 bis 31. März 2025, BGBl. I No. 27/2018.

Common provisions

§ 137. (1) Surveillance under § 136 para. 1 subpara. 1 may be conducted by the criminal investigation authority independently. Event-specific data storage under § 135 para. 2b must be ordered by the prosecution authority (§ 102). The other investigative measures under §§ 135 to 136 must be ordered by the prosecution authority with approval by the court; entry into places under [§ 135a para. 3 or][5] § 136 para. 2 requires individualised approval by the court.

(2) (repealed, BGBl. I No. 27/2018)

(3) A direction for event-specific data storage under § 135 para. 2b may only be given for the period of time as expected to be necessary to achieve its purpose and must not exceed 12 months; any further direction is not permissible. Directions for other investigative measures under §§ 135 to 136 may only be given for a future period of time, in cases under § 135 para. 2 also for periods of time in the past, as expected to be necessary to achieve their purpose. Further directions are permissible if, based on particular material facts, it is believed that a continuation of the investigative measure will be successful. In any case, the investigative measure must be stopped as soon as its prerequisites cease to exist.

5 In force from 1 April 2020 until 31 March 2025, BGBl. I No. 27/2018.