Kindesentführung und die Haager Übereinkommen zum Schutz von Kindern und Erwachsenen. Dieses Versehen soll nun durch eine Ergänzung von *Artikel 269 Absatz 2 Buchstabe a* Strafprozessordnung korrigiert werden.

Art. 270bis Abfangen und Entschlüsselung von Daten *(neu)*

Absatz 1 bildet die ausdrückliche gesetzliche Grundlage, um auf Anordnung der Staatsanwaltschaft eine Methode mit Hilfe von speziellen Überwachungsinstrumenten anzuwenden. Dazu muss in das überwachte Datenverarbeitungssystem eingedrungen werden, um ein oder mehrere spezielle Informatikprogramme einzuführen, damit zum einen das Abfangen ermöglicht wird und zum anderen die Daten unverschlüsselt gelesen werden können. Werden die in *Artikel 270bis* festgelegten Bedingungen eingehalten, stellt dieser Artikel einen gesetzlichen Rechtfertigungsgrund für die jeweilige Überwachung dar, die andernfalls unter Artikel 143bis des Strafgesetzbuchs[153] fallen könnte; unter diesen Bedingungen ist eine solche Überwachung somit rechtmässig (Art. 14 des Strafgesetzbuchs[154]).

Von besonderer Bedeutung ist diese Methode im Bereich der Überwachung der Internettelefonie (Voice over IP [VoIP]), insbesondere bei der Internettelefonie vom Typ Peer-to-Peer, bei der über zwei Computer kommuniziert wird. Denn bei dieser Art von Telefonie sind die ausgetauschten und abgefangenen Daten verschlüsselt, womit sie nicht lesbar sind und nicht direkt verwendet werden können. Die betreffende Überwachungsmethode besteht darin, dass ein spezielles Informatikprogramm in das überwachte Datenverarbeitungssystem eingeführt wird, um die ausgetauschten Daten zu entschlüsseln und damit Zugang zu den Informationen zu erhalten. Diese Methode wird auch in jenen Fällen verwendet, in denen eine Kommunikation, auch wenn sie nicht verschlüsselt ist, ohne die betreffende Methode nicht abgefangen werden könnte. Dies ist beispielsweise bei Instant Messaging der Fall, das ab einem portablen Computer oder Mobiltelefon mit verschiedenen Prepaid-SIM-DATAS-Karten erfolgt. In diesen Fällen kann die Kommunikation, auch wenn sie nicht verschlüsselt ist, nur abgefangen werden, wenn ein Programm in den portablen Computer oder in das Mobiltelefon eingeführt wird. Falls das eingeführte Informatikprogramm in den beiden oben erwähnten Fällen seine Wirkung nicht entfalten kann, weil das überwachte Datenverarbeitungssystem mit einem Antivirusprogramm ausgestattet ist, welches das eingeführte Informatikprogramm neutralisiert, kann mit der in *Artikel 270bis* erwähnten Überwachungsmethode ein zusätzliches Programm in das überwachte Datenverarbeitungssystem eingeführt werden, mit dem das Antivirusprogramm umgangen wird. Auf diese Weise kann das oben erwähnte Informatikprogramm seine Wirkung trotzdem entfalten, womit die Daten abgefangen werden können und darauf zugegriffen werden kann.

Die in *Artikel 270bis* aufgeführte Überwachungsmethode erfordert ein stärker invasives Vorgehen als die anderen Methoden. Während bei den anderen Überwachungsmethoden die erfassten Informationen aus gespeicherten Datenbeständen stammen oder ganz einfach umgeleitet werden, muss bei einer Anwendung der in *Artikel 270bis* aufgeführten Methode für den Zugriff auf die

153 SR **311.0**
154 SR **311.0**

entsprechenden Daten aktiv in das überwachte Datenverarbeitungssystem eingedrungen werden. Angesichts der besonderen Merkmale dieser Methode stellen sich im Zusammenhang mit deren Anwendung nicht nur technische Fragen. Aus diesem Grund ist die Anwendung dieser Methode nicht im neuen BÜPF, sondern in der Strafprozessordnung[155] geregelt. Im Zusammenhang mit der Überwachungsmethode nach *Artikel 270bis* werden die speziellen Pflichten von Personen, die Überwachungen des Fernmeldeverkehrs nach dem BÜPF durchführen (Art. 2 Abs. 1 VE), jedoch im neuen BÜPF aufgeführt, d. h. in Artikel 21 Absatz 4 VE.

Mit der betreffenden Überwachungsmethode kann auf das gesamte Datenverarbeitungssystem zugegriffen werden, in welches das Informatikprogramm eingeführt wird. Es kann somit auch auf Daten zugegriffen werden, die in keinem Zusammenhang mit den Beweggründen stehen, welche eine Überwachung rechtfertigen, d. h. je nach Fall beispielsweise auf Korrespondenz, Fotos und Filme, die zur Privat- oder sogar Intimsphäre gehören. Um den Zugriff auf Daten zu vermeiden, die von vornherein nutzlos sind, wird *im letzten Satz von Absatz 1* verlangt, dass die Staatsanwaltschaft die Art der Daten angibt, auf die sie im Rahmen der von ihr angeordneten Überwachung zugreifen möchte.

Es ist darauf hinzuweisen, dass diese Überwachungsmethode angesichts ihrer oben beschriebenen Merkmale subsidiär zu anderen Überwachungsmassnahmen des Fernmeldeverkehrs in Anspruch genommen wird. Das ist gerechtfertigt, weil es dabei um deutlich einschneidernde Massnahme handelt als bei den übrigen Überwachungsmassnahmen. Diese Art von Überwachung ist nur unter ganz bestimmten, zusätzlichen Voraussetzungen (im Vergleich zu denjenigen in Art. 269 Strafprozessordung[156]) möglich, d. h. wenn die anderen Überwachungsmassnahmen erfolglos geblieben sind oder die anderen Überwachungsmassnahmen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Die Genehmigungsbehörde muss das Vorliegen dieser Voraussetzungen prüfen (Art. 274 Abs. 2 Strafprozessordnung[157]). In diesem Zusammenhang ist darauf hinzuweisen, dass eine Fernmeldeüberwachung bereits gegenüber den herkömmlichen Untersuchungsmassnahmen nur subsidiär angeordnet wird (Art. 269 Abs. 1 Bst. c Strafprozessordnung[158]). Daraus ergibt sich für die Anwendung der in *Artikel 270bis* vorgesehenen Überwachungsmassnahme im Vergleich zu den herkömmlichen Untersuchungsmassnahmen eine Art „doppelte Subsidarität“. Damit wird sichergestellt, dass die vorliegende Überwachungsmassnahme nur dann zur Anwendung kommt, wenn sie wirklich notwendig ist. Es ist es aber nicht notwendig, zur Beschränkung ihrer Anwendung einen strengeren Deliktskatalog als in Artikel 269 Absatz 2 Strafprozessordnung[159] vorzusehen. Denn alle in dieser Bestimmung aufgeführten Straftaten sind geeignet, im konkreten Fall eine solche Schwere zu erreichen, welche die Anwendung dieser Überwachungsmassnahme rechtfertigt. Artikel 269 Absatz 1 Buchstabe b Strafprozessordnung[160] setzt bereits voraus, dass die Schwere der Straftat eine Fernmeldeüberwachung rechtfertigt, was insbesondere auch für die Anwendung der vorliegenden Überwachungsmassnahme gilt.

155 SR ... (BBl **2007** 6977)
156 SR … (BBl **2007** 6977)
157 SR … (BBl **2007** 6977)
158 SR … (BBl **2007** 6977)
159 SR … (BBl **2007** 6977)
160 SR … (BBl **2007** 6977)

Die Person, in deren Datensystem ein oder mehrere Informatikprogramme eingeführt wurden, um die angeordnete Überwachung zu ermöglichen, wird nach Artikel 279 der Strafprozessordnung[161] über die Installation dieses oder dieser Programme informiert.

Nach *Absatz 2* bedürfen die in *Absatz 1* aufgeführten Massnahmen wie alle angeordneten Überwachungsmassnahmen der Genehmigung durch das Zwangsmassnahmengericht. Auf Grund der besonderen Merkmale der betreffenden Überwachungsmethode muss eine solche angeordnete Überwachung gemäss Artikel 274 Absatz 4 Buchstabe c Strafprozessordnung[162], bei dem es sich um eine neue Bestimmung handelt, die durch das neue BÜPF eingeführt wird, ausdrücklich vom Zwangsmassnahmengericht genehmigt werden.

Art. 270ter Einsatz von Ortungsgeräten *(neu)*

Absatz 1 bildet die ausdrückliche gesetzliche Grundlage dafür, dass die Polizei auf Anordnung der Staatsanwaltschaft besondere Geräte verwenden kann, um die öffentliche Sicherheit zu gewährleisten. Diese Geräte dienen zur Feststellung von spezifischen Daten, dank denen ein verwendetes Mobiltelefongerät identifiziert werden kann. Bei diesen Daten handelt es sich beispielsweise um die internationale Identifikationsnummer des Geräts (IMEI-Nummer) oder um die Nummer der vom Benutzer verwendeten Identifikationskarte (SIM-Nummer). Die verwendeten Geräte dienen auch zur Ermittlung des Standorts von Mobiltelefongeräten.

Absatz 1 bezieht sich insbesondere auch auf den "IMSI-Catcher". Mit diesem Gerät lassen sich die Auswirkungen der Basisstation eines Mobiltelefonnetzes auf die Mobiltelefongeräte simulieren, die sich in seinem Sendebereich befinden. Dies hat zur Folge, dass sich die Mobiltelefongeräte beim betreffenden "IMSI-Catcher" anmelden und sich bei ihm identifizieren, wie sie dies bei irgendeiner Basisstation eines Mobiltelefonnetzes tun. Dies ermöglicht die Identifikation der bis dahin unbekannten internationalen Identifikationsnummer (IMSI-Nummer) einer bestimmten Person.

Der Dienst und die Anbieterinnen von Fernmeldediensten übernehmen im Zusammenhang mit der Anwendung der betreffenden Überwachungsmethode weder besondere Aufgaben noch haben sie diesbezüglich besondere Pflichten zu erfüllen. Diese Überwachungsmethode muss in diesem Zusammenhang vor allem von jener Art der Überwachung unterschieden werden, bei der es darum geht, von den Anbieterinnen von Fernmeldediensten die Daten von Mobiltelefongesprächen zu erhalten, die während eines bestimmten Zeitraums über ihre Mobiltelefonnetze abgewickelt wurden, damit anhand der geografischen Koordinaten der genaue Standort des betreffenden Mobiltelefons und seines Benutzers bestimmt werden kann. Angesichts der besonderen Merkmale der Überwachungsmethode, auf die sich *Artikel 270ter* bezieht, muss die Anwendung dieser Methode nicht im neuen BÜPF, sondern in der Strafprozessordnung[163] geregelt werden.

Die von der Polizei verwendeten, in Absatz 1 erwähnten Geräte sind geeignet, den Fernmeldeverkehr zu stören. In *Absatz 1* ist daher ausserdem festgehalten, dass die eingesetzten Geräte nur benutzt werden dürfen, wenn sie vorgängig von der

[161] SR ... (BBl **2007** 6977)
[162] SR ... (BBl **2007** 6977)
[163] SR ... (BBl **2007** 6977)