Geheime Ermittlungsmaßnahmen

Auskunft über Daten einer Nachrichtenübermittlung, Überwachung von Nachrichten, Beschlagnahme von Briefen, optische und akustische Überwachung von Personen, automationsunterstützter Datenabgleich.

Im 4. bis 6. Abschnitt des 8. Hauptstücks des Strafprozessreformgesetzes sind die so genannten „geheimen" Ermittlungsmaßnahmen geregelt. Die Bezeichnung leitet sich von dem Umstand ab, dass der Betroffene erst im Nachhinein Kenntnis von den Maßnahmen erlangen soll.

Die Befugnisse des 4. Abschnitts (Observation, verdeckte Ermittlung und Scheingeschäft) wurden in der letzten Ausgabe dieser Serie näher beschrieben. Die anderen „geheimen" Ermittlungsmaßnahmen (Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Überwachung von Nachrichten, optische und akustische Überwachung von Personen) sind im 5. Abschnitt geregelt.

Auch der im 6. Abschnitt geregelte, politisch heiß diskutierte automationsunterstützte Datenabgleich („Rasterfahndung") soll dargestellt werden.

Grundsätzlich sind alle Ermittlungsmaßnahmen (5. und 6. Abschnitt) von der Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung anzuordnen. Eine Ausnahme stellt die optische und akustische Überwachung dar, und zwar im Fall der Geiselnahme am Ort der Freiheitsbeschränkung; Sie darf von der Kriminalpolizei aus eigenem vorgenommen werden.

Wie bei jeder Befugnisausübung ist der Grundsatz der Gesetz- und Verhältnismäßigkeit (§ 5) zu beachten.

Wie erfolgt die Anordnung dieser Ermittlungsmaßnahmen? In der Anordnung und gerichtlichen Bewilligung dieser Ermittlungsmaßnahmen sind anzuführen: die Bezeichnung des Verfahrens, die Namen des Beschuldigten, die Tat, deren er verdächtig ist und ihre gesetzliche Bezeichnung sowie die Tatsachen, aus denen sich ergibt, dass die Anordnung oder Genehmigung zur Aufklärung der Tat erforderlich und verhältnismäßig ist.

Bei einer Auskunft über Daten einer Nachrichtenübermittlung, einer Überwachung von Nachrichten und optischen und akustischen Überwachung von Personen sind darüber hinaus weitere, in § 138 Abs.1 genannte Konkretisierungsmerkmale in die Anordnung aufzunehmen (z. B. Art der Nachrichtenübermittlung), um die Vollziehung zu ermöglichen.

Welche Pflichten und Rechte begründen diese Anordnungen? Betreiber von Post- und Telegrafendiensten sind verpflichtet, an der Beschlagnahme von Briefen mitzuwirken und auf Anordnung der Staatsanwaltschaft solche Sendungen bis zum Eintreffen einer gerichtlichen Bewilligung zurückzuhalten; ergeht eine solche Bewilligung nicht binnen drei Tagen, so dürfen sie die Beförderung nicht weiter verschieben. Anbieter und sonstige Diensteanbieter sind verpflichtet, Auskunft über Daten einer Nachrichtenübermittlung zu erteilen und an einer Überwachung von Nachrichten mitzuwirken.

Diese Verpflichtung und ihren Umfang sowie die allfällige Verpflichtung, mit der Anordnung und Bewilligung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, hat die Staatsanwaltschaft dem Anbieter mit gesonderter Anordnung unter Anführung der entsprechenden gerichtlichen Bewilligung aufzutragen.

Auf Antrag der Verpflichteten sind ihnen dafür die angemessenen und ortsüblichen Kosten, die durch die Vollziehung der Anordnungen entstanden sind, zu ersetzen.

Sind diese Ermittlungsmaßnahmen zeitlich zu befristen? Sämtliche Ermittlungsmaßnahmen des 5. Abschnitts dürfen nur für einen solchen künftigen, in den Fällen der Auskunft über Daten einer Nachrichtenübermittlung 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.

A) Die Überwachung der Kommunikation auf dem Fernmeldeweg (Auskunft über Daten einer Nachrichtenübermittlung, Überwachung von Nachrichten)

Schon nach der geltenden Strafprozessordnung ist es unter bestimmten Voraussetzungen möglich, den Telefon- und E-Mail-Verkehr zu überwachen (vgl. § 149a ff). Das Strafprozessreformgesetz hat diese Bestimmungen teilweise übernommen und dort, wo es auf Grund technischer Neuerungen Auslegungsschwierigkeiten gab oder Regelungsbedarf bestand, neue Bestimmungen geschaffen und dem System des Gesetzes entsprechend strukturiert. Die nunmehrigen Eingriffsvoraussetzungen und -möglichkeiten sind – soweit dies möglich war – technikneutral formuliert und betreffen jede Form der Nachrichtenübermittlung.

Verbindungsdaten, Inhaltsdaten. Das Strafprozessreformgesetz unterscheidet zwischen einer Auskunft über Daten einer Nachrichtenübermittlung und der Überwachung von Nachrichten.

Eine Auskunft über Daten einer Nachrichtenübermittlung betrifft die Auskunft in Bezug auf Verkehrsdaten, Zugangsdaten und Standortdaten. Die Strafverfolgungsbehörden erhalten dadurch Auskunft darüber, wer mit wem, wann telefoniert oder über E-Mail kommuniziert hat. Da die Betreiber diese Daten für Verrechnungszwecke einige Monate lang speichern müssen, ist auch eine rückwirkende Auskunft möglich. Nach den derzeitigen Bestimmungen des TKG 2003 dürfen die Betreiber diese Daten nur solange speichern, als dies für Verrechnungszwecke erforderlich ist.

Polizeieinsatz bei einer Geiselnahme in der Mariahilfer Straße in Wien: Bei einer Geiselnahme darf die optische und akustische Überwachung am Ort der Freiheitsbeschränkung von der Kriminalpolizei aus eigenem vorgenommen werden.

Foto: Egon Weissheimer

Eine EU-Richtlinie (Vorratsspeicher-RL/Data-Retention-RL) verpflichtet die EU-Mitgliedstaaten hinkünftig dazu, innerstaatlich eine Regelung zu schaffen, nach der Verkehrsdaten auf Vorrat zu speichern sind.

Die Richtlinie gibt einen Zeitraum von sechs Monaten bis zu zwei Jahren vor, innerhalb dessen diese Daten zu speichern sind. Die österreichische Umsetzung dieser Richtlinie betrifft das Bundesministerium für Verkehr, Innovation und Technologie. Derzeit liegt ein Entwurf zur Novellierung des TKG 2003 vor, der eine Speicherverpflichtung von sechs Monaten vorsieht.

Standortdaten geben im Mobilfunkbereich Auskunft darüber, innerhalb welcher Funkzelle (Masten) sich ein Mobiltelefon eingebucht hat. Die Überwachung von Nachrichten (Inhaltsdaten) ist kurz gesprochen das Ermitteln des Inhalts von Nachrichten. Gemeint ist damit, das aktuelle Mithören von Telefongesprächen oder das Lesen des Inhalts elektronischer Post.

Eine Auskunft über Verkehrs- und Standortdaten ist nach den Bestimmungen des § 135 Abs. 2 Z 1 im Fall einer Geiselnahme zulässig, wenn sich die Auskunft auf Daten beschränkt, die vom Beschuldigten während der Freiheitsentziehung übermittelt, empfangen oder gesendet werden.

Stimmt der Inhaber der technischen Anlage, die Ursprung oder Ziel einer Nachrichtenübermittlung war oder sein wird, der Auskunft ausdrücklich zu, ist die Auskunft über Daten einer Nachrichtenübermittlung zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlichen Straftat, die mit mehr als sechs Monaten Freiheitsstrafe bedroht ist, gefördert werden kann (§ 135 Abs. 2 Z 2). Beispielsweise die Aufklärung einer gefährlichen Drohung, wenn auf diese Weise der Urheber der Nachricht ermittelt werden kann.

Ist zu erwarten, dass die Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist, gefördert werden kann, ist die Auskunft über Verkehrs- und Standortdaten zulässig, wenn anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können (§ 135 Abs. 2 Z 3).

Eine Inhaltsüberwachung ist gemäß § 135 Abs. 3 Z 1 und 2 wie in den Fällen der Auskunft über Verkehrs- und Standortdaten zulässig (Geiselnahme oder Vorsatztat mit einer Strafdrohung von mehr als sechs Monaten Freiheitsstrafe und Zustimmung des Inhabers der technischen Einrichtung).

Darüber hinaus soll die Überwachung des Inhalts einer Nachricht zulässig sein, 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 278 b StGB) begangenen oder geplanten strafbaren Handlung ansonsten wesentlich erschwert wäre und der Inha-

DATENAUSWERTUNG

Auswertung beschlagnahmter Datenträger

Der OGH stellte in einer Entscheidung am 19.12.2005, 14 Os 103/05m, fest, dass die Ablesung von Daten aus einem beschlagnahmten Beweismittel selbst dann keiner gesonderten Genehmigung bedarf, wenn sie unter Verwendung eines zur Telekommunikation nutzbaren Gerätes erfolgte.

Die vorliegende Entscheidung ist insofern von Interesse, weil sie unter anderem die Frage behandelt, ob das Auslesen von Daten aus einem beschlagnahmten Datenträger nach den Beschlagnahmeregelungen zulässig ist oder ob noch eine zusätzliche Genehmigung erforderlich ist, wenn es sich um Daten handelt, die in einem Mobiltelefon gespeichert sind, und insofern die Regelungen für eine „Telekommunikationsüberwachung“ Platz greifen.

Der OGH hielt dazu fest, dass das Adressverzeichnis in einem Mobiltelefon, in dem Namen und Telefonnummern von Personen gespeichert sind, nichts anderes als ein elektronisches Adressverzeichnis ist und der Blick in ein Adressverzeichnis, um eine Telefonnummer zu erfahren, nicht den Wortlaut der Definition der Überwachung einer Telekommunikation erfülle. Auskunft wird nur über Stammdaten (Name, Anschrift, Teilnehmernummer) gegeben, die ohne Telekommunikationsverbindung zum Netzbetreiber verfügbar sind. Werden die Daten aus einem Mobiltelefon gelesen, handelt es sich bloß um einen Blick in ein Verzeichnis, das aus Praktikabilitätsgründen auf dem Mobiltelefon angebracht ist. Das verändere aber nicht den Charakter der Daten (gemeint ist damit, dass es sich um keine Ruf- oder Inhaltsdaten handelt) und insofern dürfen diese Daten im Rahmen der Beschlagnahme ohne weiteres auch ausgelesen werden.

„Verbindungsdaten“: Rufliste in einem Mobiltelefon.

Die in einem Mobiltelefon gespeicherte Rufliste gibt Aufschluss über aus- und eingegangene oder versäumte Anrufe mit entsprechenden Rufnummern und Datumsangaben. Solche Daten fallen zweifellos unter Verbindungsdaten. Reflexartig wird oftmals sofort ein Bezug zum Fernmeldegeheimnis hergestellt und der Schluss gezogen, dass diese Daten nur unter den Voraussetzungen einer Telekommunikationsüberwachung ermittelt werden dürfen. Dabei wird übersehen, dass das Fernmeldegeheimnis des Art 10 a StGG vom Gedanken getragen war, den Teilnehmern einer Kommunikation die Vertraulichkeit des Gesprächs auf dem Übertragungsweg zu gewährleisten. Die Gesprächspartner konnten und können sich auf dem Übertragungsweg selbst nicht ausreichend vor Indiskretionen schützen und sind daher auf die Verschwiegenheit und die technischen Schutzvorkehrungen der Betreiber von Telekommunikationseinrichtungen angewiesen. Vorgänge außerhalb des Übertragungsweges sind nicht vom Fernmeldegeheimnis umfasst.

Die Gesprächspartner haben es selbst in der Hand, diese Daten aus ihren elektronischen Speichern zu löschen. Insofern verhält es sich nicht anders als wenn jemand seine Telefongespräche mit Datum und Uhrzeit penibel genau auf einem Zettel festhält, um nachträglich feststellen zu können, wann er mit wem wie lange telefoniert hat. Rufdaten, die ohne Hilfe eines Betreibers außerhalb des Übertragungswegs gewonnenen wurden sind daher nicht vom Fernmeldegeheimnis iSv Art 10 a StGG umfasst. Wird ein Mobiltelefon beschlagnahmt, können die allenfalls darauf gespeicherten Rufdaten aus dem Titel der Beschlagnahme ausgelesen werden, ohne dass es dazu einer gesonderten Bewilligung für eine Rufdatenrückerfassung bedarf. Ebenso verhält es sich mit den auf dem Mobiltelefon gespeicherten SMS-Nachrichten, denn auch diese können ohne Zuhilfenahme eines Betreibers direkt abgefragt werden. Anders verhält es sich, wenn Daten aus der Mailbox abgehört werden. In diesem Fall ist eine Datengewinnung aus dem Mobiltelefon selbst nicht möglich, vielmehr befinden sich die Daten auf der Mailbox noch beim Netzbetreiber und damit noch auf dem Übertragungsweg.

Im Ergebnis bedeutet die gegenständliche Entscheidung des OGH, dass das Auslesen von Daten, die auf einem Mobiltelefon selbst abgespeichert sind, schon nach den Beschlagnahmeregelungen zulässig ist, und zwar unabhängig davon, ob es sich um Stammdaten (Name, Adresse, Telefonnummer) oder Rufdaten (wer hat wann mit wen telefoniert bzw. nicht angenommene Anrufe) handelt.

FOTO: EGON WEISSHEIMER

ber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, dringend verdächtigt ist, die Tat begangen zu haben oder zu planen."

Soweit die Bestimmung des § 135 Abs. 3 Z 3, die sehr schwer zu lesen ist.

Es eröffnen sich einige Fragen: Genügt es als Eingriffsvoraussetzung, dass die Aufklärung einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat im Raum steht oder brauchen die Strafverfolgungsbehörden dazu noch ein weiteres Tatbestandsmerkmal, nämlich die Voraussetzung, dass der Inhaber der technischen Einrichtung, die Ursprung oder Ziel der Nachrichtenübertragung war oder sein wird, dringend verdächtig ist? Mit Blick auf das Fernmeldegeheimnis (vgl. Art 10a StGG) und dem damit verbundenen Grundrechtseingriff wird man wohl zu dem Ergebnis kommen müssen, dass die Eingriffsvoraussetzungen kumulativ zu sehen sind, sonst wäre der Grundrechtseingriff schon dann zulässig, wenn dies zur Aufklärung der Vorsatztat (Strafdrohung mehr als ein Jahr Freiheitsstrafe) erforderlich erscheint. Angesichts der sonst eher restriktiven Gestaltung der Grundrechtseingriffe wäre dies eine relativ „einfach gestaltete" Eingriffsbestimmung.

Diese und andere Interpretationsfragen zu dieser Bestimmung dürften sich erübrigen, wenn der vom Bundesministerium für Justiz ausgearbeitete Entwurf zur Begleitgesetzgebung im Parlament beschlossen wird. Im Zuge dieser Begleitgesetzgebung werden auch einige Bestimmungen des Strafprozessreformgesetzes novelliert; unter anderem § 135 Abs. 3 Z 3, der leichter lesbar wäre.

Wesentlich zum besseren Verständnis trägt bei, dass neben den allgemeinen Eingriffsvoraussetzungen unmissverständlich darauf abgestellt wird, dass der Inhaber der technischen Einrichtung entweder selbst der Straftat verdächtig sein muss oder auf Grund bestimmter Tatsachen anzunehmen ist, dass eine der Tat dringend verdächtige Person die technische Einrichtung benützen werde oder mit ihr eine Verbindung herstellen werde.

Gemäß § 135 Abs. 3 Z 4 ist eine Nachrichtenüberwachung zulässig, wenn dies erforderlich ist, um den Aufenthalt eines flüchtigen oder abwesenden Beschuldigten zu ermitteln, der einer Vorsatztat, die mit mehr

EXKURS: BESONDERER RECHTSSCHUTZ

Rechtsschutz

Der Bundesminister für Justiz hat zur Wahrnehmung besonderen Rechtsschutzes einen Rechtsschutzbeauftragten für die Dauer von drei Jahren zu bestellen. Dieser muss eine besondere fachliche Qualifikation sowie eine ausreichende Berufspraxis aufweisen.

Der Rechtsschutzbeauftragte ist in Ausübung seines Amtes unabhängig, an keine Weisungen gebunden und unterliegt der Amtsverschwiegenheit.

Dem Rechtsschutzbeauftragten obliegt die Prüfung und die Kontrolle einerseits der Anordnung (bzw. der Genehmigung) sowie der Bewilligung andererseits der Durchführung einiger spezieller Formen dieser besonders sensiblen Ermittlungsbefugnisse.

Gegen die Bewilligung einer optischen oder akustischen Überwachung von Personen nach § 136 Abs. 1 Z 3 („großer Späh- und Lauschangriff") und eines automationsunterstützten Datenabgleichs nach § 141 hat Der Rechtsschutzbeauftragte das Recht der Beschwerde, solange die Rechtsmittelfrist des Beschuldigten nicht abgelaufen ist.

Soll eine Auskunft über Daten einer Nachrichtenübermittlung, eine Überwachung von Nachrichten oder eine optische und akustische Überwachung von Personen gegen Geistliche (sofern sie selbst der Tat dringend verdächtig sind) oder in den ausschließlich der Berufsausübung gewidmeten Räumen von den im § 157 Abs. 1 Z 2 bis 4 erwähnten Personen (z. B. Verteidiger, Rechtsanwälte, Patentanwälte, Notare, Wirtschaftstreuhänder, Fachärzte für Psychiatrie, Medieninhaber und andere Personen) vorgenommen werden, ist eine Ermächtigung des Rechtsschutzbeauftragten zur Antragstellung für die Staatsanwaltschaft erforderlich.

Die Erteilung der Ermächtigung ist nur bei Vorliegen besonders schwer wiegender Gründe vorgesehen.

Befassung des Rechtsschutzbeauftragten:

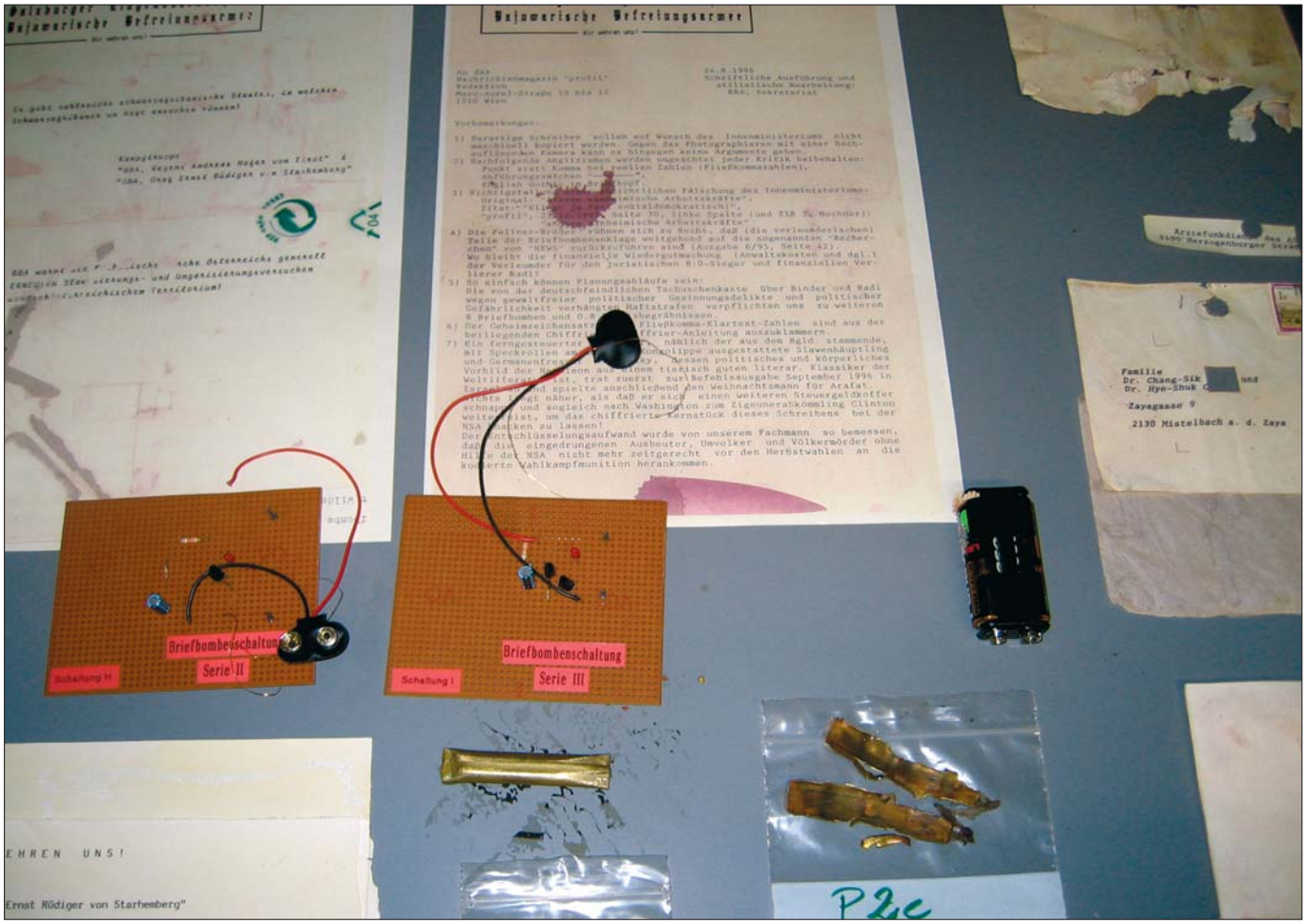
Der Rechtsschutzbeauftragte ist bei bestimmten Ermittlungsbefugnissen dreimal zu befassen: bei der Beantragung der gerichtlichen Bewilligung, nach Einlangen der Bewilligung und nach Beendigung der Ermittlungsmaßnahme.

Gleichzeitig mit der Beantragung der gerichtlichen Bewilligung für eine optische oder akustische Überwachung von Personen nach § 136 Abs. 1 Z 3 („großer Späh- und Lauschangriff") und eines automationsunterstützten Datenabgleichs nach § 141 hat die Staatsanwaltschaft dem Rechtsschutzbeauftragten eine Ausfertigung dieses Antrags samt einer Kopie der Anzeige und der maßgebenden Ermittlungsergebnisse zu übermitteln.

Die gleiche Vorgangsweise ist für jene besonderen Fälle vorgesehen, in denen eine Ermächtigung des Rechtsschutzbeauftragten zur Antragstellung für die Staatsanwaltschaft erforderlich ist.

Die Bewilligung der angeführten Ermittlungsmaßnahme hat die Staatsanwaltschaft samt Kopien aller Aktenstücke, die für die Beurteilung der Anordnungsgründe von Bedeutung sein können, unverzüglich dem Rechtsschutzbeauftragten zu übermitteln.

Nach Beendigung der Ermittlungsmaßnahme ist dem Rechtsschutzbeauftragten Gelegenheit zu geben, die gesamten Ergebnisse einzusehen und anzuhören, bevor diese zum Akt genommen werden. Er ist ferner berechtigt, die Vernichtung von Ergebnissen oder Teilen von ihnen zu beantragen und sich von der ordnungsgemäßen Vernichtung dieser Ergebnisse zu überzeugen. Das Gleiche gilt für die ordnungsgemäße Löschung von Daten, die in einen Datenabgleich einbezogen oder durch ihn gewonnen wurden. Beabsichtigt die Staatsanwaltschaft, einem solchen Antrag des Rechtsschutzbeauftragten nicht nachzukommen, so hat sie unverzüglich die Entscheidung des Gerichts einzuholen.



Teile der Briefbomben sowie Bekennerschreiben des Briefbombenattentäters Franz Fuchs: Bei dieser Anschlagsserie hätte erstmals die Rasterfahndung eingesetzt werden sollen. Der Attentäter wurde einen Tag vor dem Inkrafttreten verhaftet.

als einjähriger Freiheitsstrafe bedroht ist, dringend verdächtigt ist.

Diese Bestimmung stellt auf die Inhaltsüberwachung (vgl § 134 Z 3) ab, gemäß Größenschluss wird in diesen Fällen aber auch eine Standortfeststellung (und damit die Auskunft über Daten einer Nachrichtenübermittlung iSv § 134 Z 2) zulässig sein.

Formelle Voraussetzungen: Sowohl für die Auskunft über Verkehrs- und Standortdaten als auch für die Inhaltsüberwachung ist eine richterliche Bewilligung erforderlich. Der Schutz des Fernmeldegeheimnisses ist verfassungsrechtlich verankert und darf in Entsprechung des Art 10a StGG nur auf Grund eines richterlichen Befehls durchbrochen werden. Die Kriminalpolizei darf eine derartige Ermittlungsmaßnahme nur durchführen, wenn sie von der Staatsanwaltschaft angeordnet wurde und dieser staatsanwaltschaftlichen Anordnung eine gerichtliche Bewilligung zugrunde liegt. Mangels einer expliziten Regelung nach dem Muster der Durchsuchung von Wohnungen (vgl. § 99 Abs. 3 iVm § 120 Abs. 1) ist selbst im Falle der Geiselnahme keine Eilbefugnis der Kriminalpolizei vorgesehen.

Ermittlungsmaßnahmen nach § 135 dürfen nur für einen solchen Zeitraum angeordnet werden, der voraussichtlich erforderlich ist, wobei eine neuerliche Anordnung zulässig ist, soweit die weitere Durchführung der Ermittlungsmaßnahme Erfolg versprechend ist.

Die Maßnahme ist sofort zu beenden, sobald die Voraussetzungen dafür wegfallen.

Betreiber und sonstige Diensteanbieter sind gegen Kostenersatz nach der Überwachungskostenverordnung zur Auskunft über Daten einer Nachrichtenübermittlung und zur Mitwirkung an einer Überwachung von Nachrichten sowie zur Verschwiegenheit gegenüber Dritten verpflichtet.

Die Staatsanwaltschaft hat die Ergebnisse der Überwachung zu prüfen und diejenigen Teile in Bild- oder Schriftform übertragen zu lassen, die im Verfahren als Beweismittel verwendet werden dürfen. Die technische Durchführung der Aufgabe obliegt der Kriminalpolizei.

Rechte des Beschuldigten und der von einer Überwachung betroffenen Personen: Nach Beendigung der Ermittlungsmaßnahme hat die Staatsanwaltschaft ihre Anordnungen und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Maßnahme Betroffenen unverzüglich zuzustellen.

Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck des Verfahrens gefährdet wäre. Der Beschuldigte hat nach Beendigung der Ermittlungsmaßnahme das Recht sämtliche Ergebnisse einzusehen und anzuhören. Die Staatsanwaltschaft hat Ergebnisteile, die für das Verfahren nicht von Bedeutung sind, von der Kenntnisnahme des Beschuldigten auszunehmen, soweit berechtigte Interessen Dritter dies erfordern. Auf Antrag des Beschuldigten sind weitere Ergebnisse in Bild-

FOTO: WERNER SABITZER

oder Schriftform zu übertragen, wenn diese für das Verfahren von Bedeutung sind und ihre Verwendung als Beweismittel zulässig ist. Ergebnisteile, die für ein Strafverfahren nicht von Bedeutung sind oder als Beweismittel nicht verwendet werden dürfen, sind von amtswegen oder auf Antrag des Beschuldigten zu vernichten.

Sonstige von der Ermittlungsmaßnahme betroffene Personen (die nicht Ziel der Ermittlungsmaßnahme waren) haben das Recht, die Ergebnisse insoweit einzusehen, als sie betroffen sind. Ihre Gespräche oder Verbindungsdaten sind sozusagen als Nebenprodukt der Ermittlungsmaßnahme angefallen. Diese Personen sind, sofern ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist, von der Staatsanwaltschaft diesbezüglich zu informieren.

Auf Antrag einer solcherart betroffenen Person sind diejenigen Teile der Ermittlungsergebnisse zu vernichten, die für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel verwendet werden dürfen.

Aktenführung. Sämtliche Ergebnisse einer Nachrichtenüberwachung sind von der Staatsanwaltschaft zu verwahren und dem Gericht beim Einbringen der Anklage zu übermitteln. Anordnungen und Genehmigungen der Maßnahme, ihre gerichtliche Bewilligung sowie die in Bild- und Schriftform übertragenen Ergebnisse sind zunächst getrennt zu verwahren und erst dann zum Akt zu nehmen, wenn die Anordnung rechtskräftig geworden ist, spätestens jedoch beim Einbringen der Anklage.

Solange diese Aktenteile nicht zum Akt genommen werden, sind sie unter Verschluss aufzubewahren. Das Recht des Beschuldigten auf Akteneinsicht kann solange aufgeschoben werden, als die Umstände befürchten lassen, dass durch eine sofortige Kenntnisnahme dieser Aktenstücke der Zweck der Ermittlungen gefährdet wäre.

Auf Grund dieser besonderen Bestimmungen über die Aktenführung ist eine Akteneinsicht in Bezug auf Ermittlungsmaßnahmen gemäß § 135 Abs. 2 und 3 bei der Kriminalpolizei kaum möglich. Die Staatsanwaltschaft hat diese Aktenteile zunächst getrennt und unter Verschluss aufzubewahren und kann sie spätestens beim Einbringen der Anklage zum Akt nehmen. Zu diesem Zeitpunkt ist das Ermittlungsverfahren bei der Kriminalpolizei mit Abschlussbericht beendet und danach eine Akteneinsicht bei der Kriminalpolizei unzulässig (vgl. § 53 Abs. 1, § 145).

B) Beschlagnahme von Briefen

Der Gesetzgeber versteht darunter das Öffnen und Zurückbehalten von Briefen oder anderen Sendungen, die der Beschuldigte abschickt oder die an ihn gerichtet werden.

Anmerkung: Diese Sendungen unterliegen nur solange dem Schutz des Briefgeheimnisses, bis sie vom Empfänger geöffnet worden sind. Geöffnete Briefe unterliegen der Sicherstellung und nicht der „Beschlagnahme von Briefen“.

Diese ist zulässig, wenn sie zur Aufklärung einer vorsätzlich begangenen Straftat, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, erforderlich ist und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine

Vorführung oder Festnahme deswegen angeordnet wurde.

Bei der Beschlagnahme von Briefen sind die Bestimmungen über die Sicherstellung von Datenträgern (§ 112) sinngemäß anzuwenden. Den Betroffenen, die eine Bestätigung über die Beschlagnahme erhalten, steht das Recht auf Beschwerde zu, die aufschiebende Wirkung hat. In diesem Fall sind die Briefe auf geeignete Art und Weise vor unbefugter Einsichtnahme oder Veränderung zu schützen und dem Gericht vorzulegen; zuvor dürfen sie nicht eingesehen werden. Das OLG hat zu entscheiden, ob und in welchem Umfang sie weiterhin beschlagnahmt bleiben oder dem Betroffenen zurückzustellen sind.

C) Optische und akustische Überwachung von Personen

Optische Überwachung von Personen: Eine optische Überwachung kann sowohl mit Filmkameras als auch Fotoapparaten oder anderen technischen Mitteln zur Bildübertragung oder -aufnahme erfolgen.

Keine optische Überwachung im Sinne des Strafprozessreformgesetzes liegt vor, wenn öffentliches Verhalten des Betroffenen gefilmt oder fotografiert wird. Für ein solches Vorgehen muss eine andere gesetzliche Ermächtigung vorliegen, da § 74 auf die Bestimmungen des DSG verweist.

Anmerkung: Die Verwendung dieser technischen Mittel zur „optischen oder akustischen Überwachung" von Personen im Zuge einer Observation, einer verdeckten Ermittlung oder bei einem Scheingeschäft ist gemäß § 133 Abs.3 nur unter den Voraussetzungen des § 136 zulässig.

Die optische Überwachung von Personen zur Aufklärung einer Straftat (§ 136 Abs.3) ist zulässig, wenn sie

1. sich auf Vorgänge außerhalb von durch das Hausrecht geschützten Räume beschränkt und ausschließlich zu dem Zweck erfolgt, Gegenstände oder Örtlichkeiten zu beobachten, um das Verhalten von Personen zu erfassen, die mit den Gegenständen in Kontakt treten oder die Örtlichkeiten betreten, oder
2. mit ausdrücklicher Zustimmung des Inhabers der Räume ausschließlich zum gleichen Zweck in durch das Hausrecht geschützten Räumen zur Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, ansonsten wesentlich erschwert wäre, erfolgt.

Optische und akustische Überwachung von Personen: Die optische und akustische Überwachung von Personen (§ 136 Abs.1) ist zulässig

1. im Entführungsfall während der Freiheitsentziehung und sich die Überwachung auf Vorgänge und Äußerungen zur Zeit und am Ort der Freiheitsentziehung beschränkt (Eigenkompetenz der Kriminalpolizei!)
2. zur Aufklärung eines Verbrechens, wenn sie sich auf Vorgänge und Äußerungen beschränkt, die zur Kenntnisnahme eines verdeckten Ermittlers oder einer von der Überwachung informierten Person bestimmt sind oder von dieser unmittelbar wahrgenommen werden können,
3. für bestimmte Ermittlungen im Bereich von mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechen und von kriminellen Organisationen oder terroristischen Vereinigun-

Keine optische Überwachung im Sinne des Strafprozessreformgesetzes liegt vor, wenn öffentliches Verhalten des Betroffenen gefilmt oder fotografiert wird.

gen, zur Überwachung einer Person, die solcher Handlungen dringend verdächtig ist oder Kontaktpersonen des Beschuldigten („großer Späh- und Lauschangriff").

Soweit dies zur Durchführung einer Überwachung nach Punkt 3. unumgänglich ist, ist es zulässig, in eine bestimmte Wohnung oder in andere durch das Hausrecht geschützte Räume einzudringen, wenn anzunehmen ist, dass diese vom Beschuldigten benützt werden. Für jedes Eindringen in Wohnungen ist eine gerichtliche Bewilligung erforderlich. Eine Überwachung zur Verhinderung von im Rahmen einer terroristischen Vereinigung oder einer kriminellen Organisation begangenen oder geplanten Straftaten ist überdies nur zulässig, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

Hinsichtlich der Aktenführung gilt das unter Punkt A) näher Ausgeführte.

Die besonderen Verfahrensvorschriften des § 145 kommen zur Anwendung. Die von der Durchführung der Ermittlungsmaßnahme betroffenen Personen haben das Recht, die Ergebnisse insoweit einzusehen, als von ihnen geführte Gespräche oder Bilder betroffen sind, auf denen sie dargestellt sind. Über dieses und ihr Antragsrecht auf Vernichtung der Ergebnisse sind diese Personen, sofern ihre Identität bekannt oder ohne besonderen Verfahrensaufwand feststellbar ist, von der Staatsanwaltschaft zu informieren.

Auf ihren Antrag oder von Amts wegen sind Bilder, auf denen sie dargestellt sind, oder von ihnen geführte Gespräche zu vernichten, wenn diese für ein Strafverfahren nicht von Bedeutung sein können oder als Beweismittel nicht verwendet werden dürfen.

D) Automationsunterstützter Datenabgleich

Was ist ein Datenabgleich?

Datenabgleich ist der automationsunterstützte Vergleich von Daten (§ 4 Z 1 DSG 2000) einer Datenanwendung, die bestimmte, den mutmaßlichen Täter kennzeichnende oder ausschließende Merkmale enthalten, mit Daten einer anderen Datenanwendung, die solche Merkmale enthalten, um Personen festzustellen, die auf Grund dieser Merkmale als Verdächtige in Betracht kommen.

Datenabgleich ist zulässig, wenn die Aufklärung eines Verbrechens ansonsten wesentlich erschwert wäre und nur solche Daten einbezogen werden, die Gerichte, Staatsanwaltschaften und Sicherheitsbehörden für Zwecke eines bereits anhängigen Strafverfahrens oder sonst auf Grund bestehender Bundes- oder Landesgesetze ermittelt oder verarbeitet haben.

Zur Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens nach § 278 a oder § 278 b StGB ist es unter besonderen Bedingungen zulässig, in einen Datenabgleich auch andere Daten einzubeziehen, beispielsweise Daten über Personen, die von einem bestimmten Unternehmen bestimmte Waren oder Dienstleistungen bezogen haben oder z. B. die Mitglieder von Vereinen sind.

Franz Eigner/
Walter Dillinger

SENSIBLE DATEN

Sensible Daten (§ 4 Z 2 DSG 2000) dürfen mit wenigen Ausnahmen in einen Datenabgleich nicht einbezogen werden. Sensible Daten (besonders schutzwürdige Daten) sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit und ihr Sexualleben. Auch Bilder, Lichtbilder und Videoaufzeichnungen können sensible Daten darstellen, wenn sie Auskünfte über die rassische oder ethnische Herkunft oder den Gesundheitszustand (z. B. Behinderungen) der von der Aufzeichnung betroffenen Personen enthalten. Soweit solche Aufzeichnungen einen Rückschluss auf eine politische Meinung (z. B. Teilnehmer einer Demonstration), eine religiöse oder philosophische Überzeugung oder das Sexualleben des Dargestellten zulassen, ist definitionsgemäß und nach Spruchpraxis der Datenschutzkommission von sensiblen Daten auszugehen. Sensible Daten dürfen nur unter den taxativ aufgezählten Voraussetzungen des § 9 DSG 2000 verwendet werden.

FOTO: WERNER SABITZER