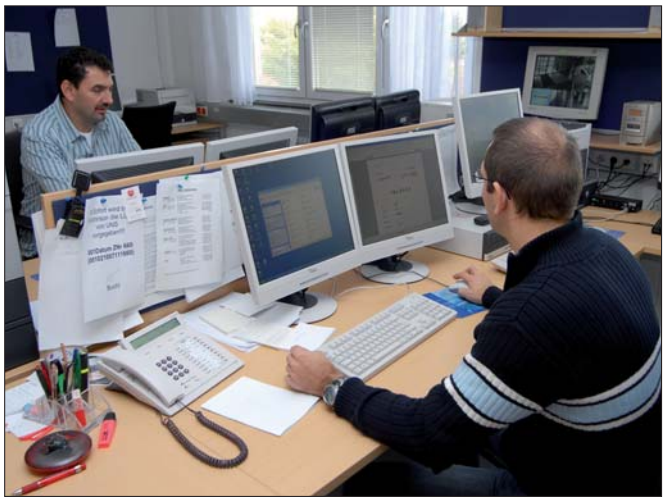
IP-Adressen und Handyortung

Die SPG-Novelle 2008 wurde in zwei Bundesgesetzblättern kundgemacht. BGBl. I Nr. 114/2007 enthält unter anderem Änderungen bei der Auskunftsverpflichtung von Betreibern öffentlicher Kommunikationsdienste und anderer Diensteanbieter und Regelungen zu den sicherheitspolizeilichen Datenanwendungen.

Wegen der Änderungen des § 53 Abs. 3 a und 3 b SPG ist die SPG-Novelle 2008 mit Schlagzeilen wie „Internetüberwachung durch Polizei ohne richterliche Kontrolle“ ins Zentrum der medialen Berichterstattung gerückt. Neben der bereits bisher bestehenden Ermächtigung zur Ermittlung von Name, Anschrift und Nummer eines bestimmten Anschlusses (Abs. 3 a Z 1) sind nunmehr die Sicherheitsbehörden ausdrücklich ermächtigt (Abs. 3 a Z 2 und Z 3), Auskunftsverlangen in Zusammenhang mit IP-Adressen zu stellen.

Danach können bei Vorliegen von Tatsachen, die die Annnahme einer konkreten Gefahrensituation rechtfertigen, anhand relevanter Abfragekriterien (etwa Nickname, Forum und Zeitraum) unbekannte IP-Adressen und zu einer bekannten IP-Adresse Name und Anschrift des Benutzers erfragt werden.

Im zweiten Satz hat sich im Vergleich zur alten Rechtslage nicht viel geändert. Es handelt sich um eine punktuelle Rufdatenrückerfassung, bei der die Sicherheitsbehörde für die Leistung erster allgemeiner Hilfe oder die Abwehr gefährlicher Angriffe unter Angabe eines „möglichst genauen Zeitraumes“ und der Nummer des Angerufenen (passive Teilnehmernummer) Daten zum Anschluss des Anrufers erfragen kann. Die Beauskunftung von Standortdaten ist nunmehr ausdrücklich in



Die Sicherheitsbehörden sind ausdrücklich ermächtigt, Auskünfte in Zusammenhang mit IP-Adressen zu stellen.

Foto: Egon Weissheimer

Absatz 3 b geregelt und bezieht sich ausschließlich auf Fälle gegenwärtiger Gefahrensituationen für Leben oder Gesundheit von Menschen. Dabei kann es sich zum Beispiel um einen verirrten Wanderer oder um ein Entführungsopfer handeln.

In den genannten Fällen ist die Beauskunftung von Standortdaten und der internationalen Mobilteilnehmerkennung (IMSI) durch den Betreiber vorgesehen und zur Lokalisierung der gefährdeten Person darf die Sicherheitsbehörde technische Mittel (IMSI-Catcher) einsetzen.

Datenanwendungen der Sicherheitsbehörden. Eine im Verfassungsrang stehende Bestimmung des Datenschutzgesetzes (§ 61 Abs. 4 DSG 2000) hat Anpassungen im 4. (informationellen) Teil des SPG notwendig gemacht. Danach dürfen Datenanwendungen zum Zwecke der Vorbeugung, Verhinderung oder Verfolgung von Straftaten bei Fehlen einer ausreichenden gesetzlichen Grundlage (nur) bis zum 31. Dezember 2007 geführt werden. Darüber, was unter einer „ausreichenden gesetzlichen Grundlage“ im Sinne des Datenschutzgesetzes zu verstehen ist, geben die Materialien zum DSG 1978 und Rundschreiben des Bundeskanzleramtes-Verfassungsdienst Auskunft: Dem Gesetz müssen im Wesentlichen Datenarten, Betroffenen- und Empfängerkreise zu entnehmen sein. Beispiele für ausreichend determinierte Regelungen im SPG sind etwa § 57 über die Zentrale Informationssammlung und neuere Regelungen wie die §§ 58 a, b und c über den Sicherheitsmonitor, die Vollzugsverwaltung oder die Zentrale Gewaltschutzdatei. Mit der SPG-Novelle 2008 ist als § 58 d die nachfolgend beschriebene „Zentrale Analysedatei über mit beträchtlicher Strafe bedrohte Gewaltdelikte, insbesondere sexuell motivierte Straftaten“ dazugekommen.

Vor diesem Hintergrund ist auch der neue § 53 a SPG zu sehen, der in den Absätzen 1 bis 4 SPG die (großteils schon vorhandenen), teils nur lokal, teils sprengelübergreifend zu führenden Datenanwendungen der Sicherheitsbehörden detailliert beschreibt. Diese wurden bislang lediglich auf den Verarbeitungszweck abstellenden § 53 Abs. 1 SPG gestützt, in dem ohne weitere Präzisierung die Zulässigkeit der Ermittlung und Weiterverarbeitung von Daten für die aufgezählten sicherheitspolizeilichen Aufgabenstellungen verankert ist.

Leitung, Koordination und Administration von Einsätzen und Erfüllung der ersten allgemeinen Hilfeleistungspflicht, sowie Personen- und Objektschutz: Derartige automationsunterstützte Einsatzleitsysteme existieren bereits und sind in einer modernen Einsatzführung unbedingt notwendig. Sie sollen aber nicht nur lokal, sondern anlassbezogen auch sprengelübergreifend (in einem Informationsverbundsystem) geführt werden dürfen. In diesem Fall sind die Daten nach Beendigung und Evaluierung des Einsatzes, längstens aber nach einem Jahr zu löschen. Insbesondere in Hinblick auf die EURO 2008 ist ein solches System ein großer Mehrwert.

Abwehr krimineller Verbindungen und gefährlicher Angriffe sowie deren Vorbeugung mittels Analyse: Zu

diesem Zweck werden operative Analysetools betrieben, die es ermöglichen, beispielsweise durch den Vergleich von Straftaten Serientaten mit ähnlichem Modus Operandi zu erkennen und in komplexen Fällen neue Ermittlungsansätze zu finden, oder Strukturen von kriminellen Verbindungen sichtbar zu machen. Zu diesem Zweck dürfen u. a. die Daten von Tätern/Verdächtigen, Kontaktpersonen aber auch von Opfern und potenziellen Opfern erfasst werden. Auch mehrere Sicherheitsbehörden dürfen bei Bedarf gemeinsame Analysen durchführen und die Regelung sieht je nach Betroffenenkreis unterschiedlich lange Speicherfristen vor. Die Befassung des Rechtsschutzbeauftragten im Zusammenhang mit derartigen Datenanwendungen der Sicherheitsbehörden ist vorgesehen.

Evidenthaltung von Wegweisungen/Betretungsverboten und einstweiligen Verfügungen zum Schutz vor Gewalt in der Familie und von Betretungsverboten in Schutzzonen: Diese Ermächtigungen zur Führung von Datenanwendungen sollen die bislang großteils in Indexordnern abgelegten Meldungen über Vorfälle von Gewalt in der Familie nach § 38 a ersetzen. Darüber hinaus wird die Möglichkeit zur automationsunterstützten Evidenthaltung von Betretungsverboten in Schutzzonen nach § 36 a ausdrücklich geregelt.

Die Sicherheitsbehörden dürfen bei einer gegenwärtigen Gefahrensituation für Leben oder Gesundheit eines Menschen dessen Standortdaten und IMSI-Nummer erfragen.

Zentrale Analysedatei über mit beträchtlicher Strafe bedrohte Gewaltdelikte, insbesondere sexuell motivierte Straftaten: Bei dieser zentralen Anwendung handelt es sich um eine Datenanwendung, die auf dem in Kanada entwickelten System *VICLAS (Violent Crime Linkage Analysis System)* beruht und dazu dient, schwere Gewaltdelikte und Sexualstraftaten zu analysieren und gegebenenfalls Serienstraftaten auch überregional effektiv und schnell zusammenzuführen. Dies geschieht durch Analyse der vorhandenen Täter- und Opferinformationen, insbesondere des Täterverhaltens und des Modus operandi sowie anhand forensischer Daten mit dem Ziel, die festgestellten Verhaltensmuster der bekannten oder unbekannten Straftäter bei ihrer Tatausführung abzubilden. Darauf aufbauend können dann geschulte polizeiliche Fallanalytiker mit gezielten Recherchen im System Gemeinsamkeiten zu bereits abgespeicherten Fällen herausfiltern und Vorbeugungsstrategien entwickeln.

Weitere Änderungen. Mit der SPG-Novelle 2008 wurden zahlreiche weitere Änderungen vorgenommen, die teilweise von großer praktischer Bedeutung sind:

- Es wurden die im SPG notwendigen Anpassungen an das Strafprozessreformgesetz, BGBl. I Nr. 19/2004 vorgenommen.
- Mit dem Ersetzen des Wortes „Durchführung“ durch das Wort „Bereitstellung“ in § 11 wurde klargestellt, dass Teile der Grundausbildung auch durch Externe, wie beispielsweise Fachhochschulen, durchgeführt werden dürfen. Eine „Bereitstellung“ durch die Sicherheitsakademie ist ausreichend.
- Für den Vorsitzenden des Menschenrechtsbeirats und im Vertretungsfall für dessen Stellvertreter wurde in § 15 b eine Aufwandsentschädigung vorgesehen.
- Im Erkennungsdienst wurde § 65 dahingehend adaptiert, dass hinkünftig eine erkennungsdienstliche Behandlung auch dann zulässig ist, wenn eine für bestimmte Deliktsbereiche typische (statistische) Rückfallsgefahr vorliegt. Konkrete Anhaltspunkte beim Betroffenen selbst, die für die

FOTO: EGON WEISSHEIMER

Wahrscheinlichkeit der Wiederholung oder Begehung anderer gefährlicher Angriffe sprechen, sind in diesem Fall nicht mehr notwendig.

Außerdem dürfen in der erkennungsdienstlichen Evidenz neben anderen notwendigen Daten auch Staatsangehörigkeit, Dokumentendaten und Gefährlichkeitshinweise gespeichert werden. Eine wichtige Änderung betrifft auch jene Fälle, in denen erkennungsdienstliche Daten nach anderen Materien ermittelt wurden, und nunmehr bei Vorliegen der notwendigen Voraussetzungen in der zentralen erkennungsdienstlichen Evidenz nach dem SPG weiterverarbeitet werden dürfen. Davon ist der Betroffene nach Möglichkeit zu verständigen.

• Für den vorbeugenden Schutz von Personen und für Zwecke der verdeckten Ermittlung konnten gemäß § 54 a durch die aufgezählten Behörden schon vor der Novelle Urkunden, z. B. Reisepässe, ausgestellt werden.

Nunmehr dürfen auch andere Rechtsträger, etwa Sozialversicherungsträger, zur Ausstellung der für eine Legendierung notwendigen E-Card herangezogen werden. Darüber hinaus sind Urkunden zum Schutz von Zeugen nicht mehr zwingend nach drei Jahren einzuziehen, sondern die Ausstellung erfolgt nach Maßgabe der im Einzelfall zu prognostizierenden „Schutzzeit" eines Zeugen.

Mit Hilfe der zentralen Analysedatei VICLAS sollen schwere Gewaltdelikte und Sexualstraftaten analysiert und Serienstraftaten effektiv und schnell zusammengeführt werden.

• Sicherheitsüberprüfungen nach § 55 a Abs. 4 können bei Vorliegen von Anhaltspunkten über die mangelnde Vertrauenswürdigkeit eines Menschen schon vor Ablauf der bislang geltenden Fristen von zwei bzw. drei Jahren wiederholt werden.

• Nach Ergänzung des Ausschreibungsgrundes des § 57 Abs. 1 Z 12 dürfen ausländische Reisepässe nicht nur im Falle des Diebstahls, sondern auch bei Verlust desselben ausgeschrieben werden. Infolge der Streichung des letzten Satzes in § 57 Abs. 2 ist es zulässig, in der Sachenfahndung auch nach dem Namen und anderen personenbezogenen Daten etwa eines Dokumenteninhabers abzufragen.

• Durch die Novellierung des § 7 Polizeikooperationsgesetz ist der Zugriff auf Informationen, die in Datenbanken der internationalen kriminalpolizeilichen Organisation (Interpol) zur Verfügung gestellt werden, nicht mehr nur der Zentralstelle (Bundeskriminalamt) vorbehalten. Damit können besonders geschulte Organe vor Ort ebenfalls Informationen über gestohlene und verlorene Reisedokumente abrufen.

• Im Grenzkontrollgesetz wurde der Verweis auf das SPG zur Befassung des Rechtsschutzbeauftragten beim Einsatz von Bild- und Tonaufzeichnungsgeräten anlässlich von Grenzkontrollen aktualisiert.

Verena Weiss

SPG-NOVELLE 2008

Hintergrund der Änderung

Der nunmehr überarbeitete § 53 Abs. 3 a SPG war mit der SPG-Novelle BGBl. I Nr. 146/1999 eingeführt worden, weil nach der Privatisierung der Post- und Telegraphenverwaltung und dem damit einhergehenden Wegfall der Amtshilfeverpflichtung eine Regelung geschaffen werden musste, die eine Verpflichtung der Betreiber zur Auskunftserteilung normiert. Mit Einführung dieser Bestimmung waren die Sicherheitsbehörden ermächtigt worden, zur Erfüllung ihrer nach diesem Bundesgesetz übertragenen Aufgaben kostenlos Auskunft über Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses von Betreibern öffentlicher Kommunikationsdienste zu verlangen.

Darüber hinaus durften sie in Fällen der ersten allgemeinen Hilfeleistung und zur Abwehr gefährlicher Angriffe anhand der passiven Teilnehmernummer und dem Zeitpunkt des Anrufes erfragen, von welchem Anschluss aus angerufen wurde und wem die entsprechende Teilnehmernummer zuzuordnen ist. Die Beauskunftung von „Standortdaten" war nicht vorgesehen.

Die in der alten Bestimmung verwendete Terminologie ist aus heutiger Sicht überholt, weil auf physische Anschlüsse abgestellt wurde. Die Beauskunftung im Bereich der Mobiltelefonie, vor allem aber von Internet-Adressen (IP-Adressen) war nur durch großzügige Interpretation subsumierbar.

Mit Erkenntnis vom Oktober 2007 hat die Datenschutzkommission in einem konkreten Anlassfall festgestellt, dass die auf das Sicherheitspolizeigesetz gestützte Ermittlung einer IP-Adresse durch die Sicherheitsbehörde mangels tauglicher Eingriffsgrundlage eine Verletzung des Grundrechts auf Geheimhaltung schutzwürdiger personenbezogener Daten darstellt.

Außerdem hat sie angemerkt, dass die Rechtslage im Hinblick auf die Auskunftsverlangen der Sicherheitsbehörden nicht klar und daher im Interesse des Datenschutzes und der Rechtssicherheit verbesserungswürdig sei. Nicht zuletzt deshalb wurde die betreffende Norm präzisiert.

FOTO: EGON WEISSHEIMER