MOBILFUNK

Fahndung mit stiller Post

Die Polizei versendet heimlich SMS-Nachrichten an Tatverdächtige, um ihren Aufenthaltsort zu ermitteln. Datenschützer und Staatsanwälte sind empört.

Markus Zeller* traute seinen Augen kaum, als plötzlich die Polizei an der Tür stand, um seinen Kumpel zu vernehmen – und ihn selbst gleich mit.

Dabei hatte er nur einem Freund helfen wollen: Der hatte unweit von Stuttgart einen Unfall gebaut und neben seinem eigenen auch ein parkendes Fahrzeug beschädigt. Zeller holte den Bruchpiloten ab, das Unglücksauto ließen sie an Ort und Stelle stehen. Die beiden fuhren zu Zeller nach Hause, um sich kurz zu beraten, bevor der Freund sich der Polizei stellen wollte. Doch da klingelte sie bereits an der Tür. Nun läuft gegen Zeller ein Verfahren wegen Beihilfe zur Unfallflucht. Zur Verfolgung hatte den Beamten das Kennzeichen des liegen gebliebenen Wagens gereicht. Im Telefonbuch fanden sie die Handy-Nummer des Halters. Diesen Minuten später aufzuspüren war dann kein Problem mehr.

Die Polizei nutzt in solchen Fällen einen technischen Trick, der Juristen und Datenschützer empört. Er erlaubt es, den gegenwärtigen Aufenthaltsort von jedem Handy-Nutzer zu bestimmen, wenn er nur sein Gerät empfangsbereit bei sich trägt.

Je nachdem, wie dicht die Handy-Masten stehen, ist die Ortung auf bis zu 50 Meter genau.

Um Missbrauch zu verhindern, ist das Erstellen von persönlichen Bewegungsprofilen in der Strafprozessordnung (StPO) eigentlich an die strengen Auflagen des Paragrafen 100 a StPO geknüpft. Nur bei „schweren Straftaten“ darf es richterlich angeordnet werden – dazu zählen Hochverrat, Mord oder schwerer sexueller Kindesmissbrauch, Fahrerflucht hingegen nicht.

Um auch bei Bagatellen die Handy-Ortung einsetzen zu können, berufen sich findige Polizeibeamte auf die Paragrafen 100 g und h, die im Rahmen der Anti-Terror-Gesetzgebung im letzten Jahr wirksam wurden. Darin heißt es, dass Netzbetreiber „unverzüglich Auskunft“ über die Verbindungsdaten einschließlich der Standortkennung geben müssen, und zwar schon bei einer „Straftat von erheblicher Bedeutung“.

So dehnbar die Auslegung dieses Gummiparagrafen auch sein mag, eines ist klar: Er bezieht sich ausschließlich auf tatsächliche „Verbindungen“ eines Handys. Solange der Verdächtige also nicht telefoniert oder SMS verschickt, meinen Kritiker, darf sein Gerät nicht geortet werden.

Diese Hürde überspringen die Ermittler, indem sie so genannte stille SMS an Verdächtige schicken. Die Nutzer bemerken diese geheimen Kurzmitteilungen nicht, denn sie werden nicht angezeigt. Die Spitzel-SMS erzeugen jedoch aktuelle Verbindungsdaten beim Mobilfunkprovider. Diese wiederum kann die Polizei dann unter Berufung auf die Gummiparagrafen „unverzüglich“ einfordern – bei „Gefahr im Verzug“ auch ohne richterliche Anordnung.

VOLKER REBEHN

Datenschützer Weichert: *Endlich die Hosen runterlassen*

Dabei kommen Programme zum Einsatz wie „SMS Blaster“ oder „SmartSMS“, die eigentlich für den Massenversand von Kurznachrichten per PC entwickelt wurden. Zusätzlich bieten sie eine Funktion namens „Stealth Ping“, die normalerweise Netzbetreibern dazu dient, durch unbemerktes „Anklopfen“ bei Kunden-Handys zu testen, ob sie in fremden Partnernetzen per „Roaming“ erreichbar sind. Die Polizei dagegen zweckentfremdet das lautlose Anklopfen („Pingen“), um sich selbst die für die Observation notwendigen Verbindungsdaten zu schaffen. Doch diese Praxis ist umstritten.

Inzwischen sei das „Pingen“ zum Lieblingsspielzeug jedes Dorfpolizisten geworden, ärgert sich ein badischer Richter: „Die beantragen das schon, wenn jemand nur ohne Führerschein Auto fährt.“

„Rechtliche Bedenken“ gegen diese Standortschnüffelei per stiller Post hat nun auch der Leitende Oberstaatsanwalt Stuttgarts angemeldet. In einem Schreiben an den Generalstaatsanwalt mahnt er: „Auskünfte über Standortdaten eines im Standby-Betrieb befindlichen Handys“ seien ausschließlich im strengen Rahmen des Paragrafen 100 a gestattet. Die „Erstellung eines Bewegungsprofils durch heimliches Herstellen einer Verbindung“ halte er andernfalls für „unzulässig“.

Für den Vorsitzenden der Deutschen Vereinigung für Datenschutz, Thilo Weichert, belegt die kreative Verdächtigenortung, „wie sehr der Gesetzgeber den Strafverfolgern hinterherhinkt“. Vor allem aber fordert er eine verstärkte parlamentarische Kontrolle und dass die Polizei ihre Fahndungspraktiken offen legt: „Die müssen endlich die Hosen runterlassen!“

Vorerst bleibt das ein frommer Wunsch. „Keine Auskunft“, heißt es zum Thema verdeckter SMS-Ermittlungen bei Polizeisprechern in Berlin, Frankfurt und Stuttgart. Und der Sprecher des Bundesinnenministeriums sieht „keinerlei Rechtsproblem“ bei der derzeitigen Ortungspraxis.

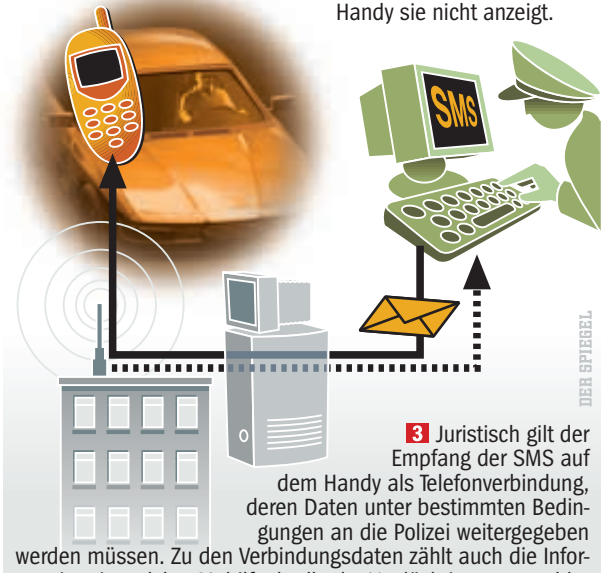
Um also sicherzugehen, dass ein Handy nicht als Peilsender missbraucht wird, gibt es bislang nur eine Methode: Abschalten.

STEFAN KREMPL, HILMAR SCHMUNDT

Verräterische Botschaft Bewegungsprofil per SMS

1 Der Aufenthaltsort eines Tatverdächtigen soll bestimmt werden. Er hat sein Handy eingeschaltet, telefoniert aber nicht.

2 Der ermittelnde Polizist sendet vom Rechner aus eine „stille SMS“ an das Handy des Verdächtigen, der davon nichts mitbekommt, weil das Handy sie nicht anzeigt.



3 Juristisch gilt der Empfang der SMS auf dem Handy als Telefonverbindung, deren Daten unter bestimmten Bedingungen an die Polizei weitergegeben werden müssen. Zu den Verbindungsdaten zählt auch die Information, in welcher Mobilfunkzelle der Verdächtige angemeldet ist. Die Polizei erhält so ein Bewegungsprofil des Verdächtigen.

* Name von der Redaktion geändert.