Bürgerrechte & Polizei

Cilip 114
November 2017

Die Cyberpolizei

Digitale Migrationskontrolle
Polizeikooperation mit Ägypten
Militarisierung des Protest Policing

Inhalt

Schwerpunkt: Die Cyberpolizei

Redaktionsmitteilung

„Es wäre doch keinem zu erklären, wenn wir zum Beispiel die Polizei bei Nachrichten über Messengerdienste blind und taub lassen würden“, erklärte der baden-württembergische Innenminister Thomas Strobl am 13. November 2017 – zwei Tage bevor eine ganz große Koalition aus Grünen, CDU und SPD im Landtag die Polizei zur präventiven Überwachung der Telekommunikation und zur Nutzung von Trojanern ermächtigte.

Mit dem Verweis auf die Messengerdienste bewegt sich der Minister zwar auf dem neuesten Stand der Technik, die Kernaussage seines Statements ist jedoch von vorgestern. Sie besagt, dass es erstens keine überwachungsfreie Kommunikation geben dürfe und dass zweitens die Polizei stets rechtlich in die Lage versetzt werden müsse, alle vorhandenen Überwachungstechniken auch nutzen zu dürfen.

Die 1968 in der BRD erstmals legalisierte Telefonüberwachung ist rasch von der Ausnahme zur Normalität geworden. Dafür sorgten sowohl die wachsende Telefondichte als auch die ständige Ausweitung des entsprechenden Deliktkatalogs. Noch in den frühen 1990er Jahren jammerte die Polizei, die neue Mobiltelefonie sei nicht zu knacken. Das Gegenteil war der Fall. Die Überwachung mobiler Kommunikation hat nicht nur enorme quantitative Ausmaße erreicht, sondern der Polizei zudem eine Vielfalt neuer Methoden beschert – von der Standortüberwachung über die Funkzellenabfrage bis hin zur Stillen SMS. Ende 2008 legalisierte der Bundestag den Einsatz von Trojanern bei der präventiven Terrorbekämpfung des BKA, im Sommer 2017 folgten die Rechtsgrundlagen für die Nutzung solcher Schadsoftware zur Strafverfolgung. Die Bundesländer ziehen nun sukzessive in ihren Polizeigesetzen nach. Darf's noch etwas mehr sein?

***

„Polizei und Stadt“ ist der Arbeitstitel für den Schwerpunkt der nächsten Ausgabe von Bürgerrechte & Polizei/CILIP.
(Heiner Busch)

Der digitale Wilde Westen

Kleine Übersicht zur entgrenzten Überwachung

von Benjamin Derin

Die stets voranschreitende Digitalisierung und Auffächerung von Kommunikationswegen und ihrer Kontrolle hat eine Proliferation der Überwachungsmethoden in tatsächlicher wie rechtlicher Hinsicht mit sich gebracht. Gleichzeitig werden die bestehenden Möglichkeiten immer häufiger und intensiver genutzt.

Eine der größten Ängste aller Sicherheitsbehörden und Ermittler ist es, nicht jedes der durch den technologischen Fortschritt ständig neu geschaffenen Kommunikationsmittel vollumfänglich kontrollieren zu können. Mit der Begründung, hier Schritt halten zu müssen, wird eine Ausweitung der Überwachungsbefugnisse auf alle erdenklichen Lebenssachverhalte betrieben, die von hektischen Gesetzgebungsmaßnahmen begleitet ist. Diese Entwicklung macht aber nicht bei der Einbeziehung moderner Kommunikationsformen in den herkömmlichen Surveillance-Apparat halt, sondern führt zur Entstehung gänzlich neuer Überwachungsmittel. Die technologischen Errungenschaften werden zur sicherheitstechnischen Erschließung bisher unangetasteter Sphären genutzt, bevor die damit verbundenen Risiken abgeschätzt werden können. In diesem Wilden Westen der digitalen Überwachung toben sich behördliche DatensammlerInnen aus, ohne sich zur Rechenschaft verpflichtet zu fühlen. Der ausufernde Einsatz technischer Möglichkeiten steht deshalb einer abnehmenden Transparenz für den Bürger/ die Bürgerin gegenüber. Die allgemeine Digitalisierung des Lebens führt dazu, dass der technische Zugriff für die ErmittlerInnen immer leichter wird, während die Eingriffsintensität für die Betroffenen zunimmt. Das Auseinanderfallen von technisch Machbarem und rechtlich Erlaubtem resultiert zudem in juristischen Auseinandersetzungen über Rechtsgrundlagen und Voraussetzungen der einzelnen Maßnahmen, die nicht nur von KritikerInnen, sondern teils auch von den Behörden selbst unterschiedlich bewer-

tet werden. So entsteht eine Atmosphäre der Unverbindlichkeit, in der für Betroffene nur schwer nachvollziehbar ist, welcher rechtliche Maßstab für Eingriffe in ihre Rechte angewendet wurde. Diese wachsende Beliebigkeit bringt nicht nur erhebliche Gefahren für die Datensicherheit der Allgemeinheit, sie ist auch mit den grundgesetzlichen Anforderungen an Dateneingriffe kaum noch in Einklang zu bringen.

Was möglich ist, muss erlaubt sein: stille SMS

Symptomatisch für die Entgrenzung von Überwachungsmaßnahmen ist etwa die sog. stille SMS. Sie ermöglicht durch das Provozieren eines Datensignals jederzeit und mit geringem Aufwand die Ortung eines Mobiltelefons, ohne dass die betroffene Person hiervon Kenntnis erlangt. Weil das so einfach und unkompliziert ist, wird die Methode in gewaltigem Umfang eingesetzt. 2015 haben BKA, Bundesamt für Verfassungsschutz und Bundespolizei über 311.000 stille SMS verschickt, 2016 mehr als 418.000.[1] Hinzu kommt der Einsatz in den Ländern. Die Berliner Polizei nutzte das Mittel 2015 beispielsweise über 137.000 Mal, die Polizei in NRW verschickte 2016 mehr als 178.000 stille SMS.[2] Zugang zu diesen Zahlen vermittelt aber keine einsehbare Statistik – sie stammen aus parlamentarischen Anfragen, die wiederum nur teilweise und nach eigenem Gutdünken beantwortet werden. Während beispielsweise für das Zollkriminalamt und die Zollfahndungsämter die Nutzung für 2012 noch mit etwa 200.000 und für das erste Halbjahr 2013 mit beinahe 139.000 beziffert wurde,[3] ist die Auskunft seither versagt worden. Meist geht zudem nicht hervor, wie viele Personen in wie vielen Ermittlungsverfahren betroffen waren. Nicht nachvollziehbar ist des Weiteren, wie oft die Maßnahme in Amtshilfe für eine andere Behörde durchgeführt wurde. Inwieweit auf diese Weise beispielsweise der BND, wie es Medien berichtet hatten, stille SMS indirekt einsetzt, lässt sich deshalb nicht überprüfen.[4] Bereits das Ausmaß der Nutzung wird somit nur in Ansätzen bekannt. Anders als diese eher nonchalante Anwendungspraxis vermuten ließe, ist die stille SMS aber mit äußerst intensiven Grund-

1 BT-Drs. 18/5645 v. 24.7.2015; BT-Drs. 18/7285 v. 15.1.2016; BT-Drs. 18/9366 v. 9.8.2016; BT-Drs. 18/11041 v. 30.1.2017
2 Abgh. Berlin, Drs. 17/17721 v. 26.1.2016, LT NRW, Drs. 16/14528 v. 17.3.2017
3 BT-Drs. 17/14714 v. 6.9.2013
4 Süddeutsche Zeitung v. 17.10.2014

rechtseingriffen verbunden. Die Daten ermöglichen die Erstellung umfassender Bewegungs- und Verhaltensprofile und gehen damit zum Teil sogar über das hinaus, was durch klassische, besser regulierte Maßnahmen wie das Anbringen von Peilsendern an Fahrzeugen oder langfristige Observationen in Erfahrung gebracht werden kann. Da die Maßnahme heimlich erfolgt, erfahren die Betroffenen zunächst nicht, dass sie überwacht werden und können keinen Rechtsschutz suchen. Eine nachträgliche Benachrichtigung ist zwar gesetzlich vorgeschrieben, erfolgt aber häufig nicht.[5] Obwohl der Einsatz stiller SMS derart weit verbreitet ist und einen erheblichen Eingriff in die Rechte des Betroffenen darstellt, ist nach wie vor nicht geklärt, auf welcher Rechtsgrundlage sie überhaupt zulässig ist. Eine eigene rechtliche Regelung für den Einsatz existiert weder in der Strafprozessordnung (StPO) noch im Polizeirecht. Ob andere Eingriffsgrundlagen dafür herangezogen werden können und auf welche Vorschrift die Maßnahme genau zu stützen ist, ist umstritten.[6] Die angesichts dessen weiter zunehmende Nutzung der stillen SMS zeigt, dass für die Ermittlungspraxis nicht das rechtliche Dürfen, sondern das technische Können der Maßstab bleibt.

Funkzellenabfrage: Auf dem Weg zur Standardmaßnahme

Inzwischen geklärt ist die Ermächtigungsgrundlage für eine weitere umstrittene Maßnahme: die Funkzellenabfrage. § 100g Abs. 3 StPO erlaubt die Abfrage im Rahmen der Strafverfolgung, legt aber ganz bestimmte Voraussetzungen fest wie etwa eine auch im Einzelfall schwerwiegende Tat und ein angemessenes Verhältnis der Maßnahme zur Bedeutung der Sache. Umso bedenklicher ist, dass sie sich mittlerweile zu einer Art Standardmaßnahme entwickelt hat. So führten BKA, Zollfahndungsdienst und Bundespolizei 2015 insgesamt 174 Funkzellenabfragen durch, 2016 waren es 240 und im ersten Halbjahr 2017 bereits 259.[7] Die Berliner Polizei machte 2015 in 256 Verfahren davon Gebrauch, 2016

5 Berliner Beauftragte für Datenschutz und Informationsfreiheit: Abschlussbericht zur datenschutzrechtlichen Überprüfung des Einsatzes von Stillen SMS in strafrechtlichen Ermittlungsverfahren v. 28.7.2016, S. 13 f.

6 vgl. Bär, W. in: Graf, J.P. (Hg.): Beck'scher Online-Kommentar StPO (BeckOK-StPO), 27. Ed. 2017, § 100g Rn. 24 f.; Eisenberg, U.; Singelnstein, T.: Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS", in: NStZ 2005, H. 2, S. 62-67 (65)

7 BT-Drs. 18/5645 v. 24.7.2015, 18/7285 v. 15.1.2016, 18/9366 v. 9.8.2016, 18/11041 v. 30.1.2017 und 18/13205 v. 28.7.2017