Humanistische Union

Die Ortungswanze in der Hosentasche

Maßnahmen nach §§ 100 StPO zum Ermitteln des Aufenthaltsorts und der Kennung von Mobiltelefonen. In: vorgänge Nr. 227 (3/2019), S. 85-94

Der technologische Wandel und die dadurch ausgelösten Diskussionen um neue Überwachungstechnologien und deren Regulierung zeigt sich kaum so deutlich wie im Bereich der Telekommunikation. Die Ablösung der Festnetz- durch die Mobilkommunikation, die rasante Verbreitung von Smartphones und der Wechsel von der leitungsbezogenen zur IP-gestützten Datenübertragung (die mittlerweile für nahezu alle digitalen Serviceangebote genutzt wird) sind nur einige Merkmale dieser Entwicklung. Der folgende Beitrag von Matthias Monroy zeigt, welche verschiedenen Überwachungsmaßnahmen an diesen Technologien anknüpfen, die weit über das klassische Abhören von Gesprächen hinausreichen. Er erläutert die einzelnen Maßnahmen und gibt einen Überblick, wie oft diese von den verschiedenen Sicherheitsbehörden angewandt werden.

Neben der Telekommunikationsüberwachung (§ 100a StPO) und der Online-Durchsuchung (§ 100b StPO) nutzen Polizeibehörden im Rahmen der §§ 100 StPO technische Mittel, um den Aufenthaltsort von Mobiltelefonen zu ermitteln. Hierzu gehören die sogenannte Stille SMS, IMSI-Catcher und Funkzellenabfragen. Auch der Zoll und die Geheimdienste sind teilweise dazu befugt. Halbjährliche parlamentarische Anfragen im Bundestag dokumentieren, dass sich die Zahl der Maßnahmen für Bundesbehörden in den letzten Jahren in etwa auf gleichem Niveau bewegt. Den Zahlen einzelner Länder zufolge werden die Ermittlungsmethoden nach §§ 100 StPO dort teilweise deutlich häufiger genutzt als bei Bundesbehörden. Manche Maßnahmen zur Lokalisierung von Telefoninhaber_innen bewegen sich in einem Graubereich und zogen rechtliche Anpassungen nach sich. Ein Urteil des Bundesgerichtshofes vom vergangenen Jahr könnte ursächlich sein, dass die Zahlen für „Stille SMS“ plötzlich stark rückläufig sind. Einige Bundesländer schließen sich derzeit zu Gemeinsamen Kompetenz- und Dienstleistungszentren auf dem Gebiet der polizeilichen Telekommunikationsüberwachung (GKDZ) zusammen, die in Hamburg und Leipzig/ Dresden errichtet werden. Möglicherweise wird mit diesen zentralisierten GKDZ die Anzahl der Maßnahmen zur Telekommunikationsüberwachung im Rahmen der §§ 100 StPO weiter zunehmen.

„Stille SMS“

„Stille SMS“ sind auf dem Mobiltelefon nicht sichtbar. Als „Ortungsimpulse“ erzeugen sie bei den Mobilfunkanbietern Verbindungsdaten, ohne dass die Nutzer_innen dies bemerken. Die durch die „Stille SMS“ generierten und gespeicherten Standortdaten der Telefone werden von den Behörden abgefragt und zur Erstellung von nachträglichen oder Echtzeit-Bewegungsprofilen genutzt. Das BKA versendet „Stille SMS“ zur Gefahrenabwehr (§ 53 i. V. m. § 51 bzw. § 52 BKAG) und zur Strafverfolgung. Die Standortdatenausleitung in Echtzeit erfolgt auf eine richterliche Anordnung nach § 100i Absatz 1 Nummer 2 StPO. [1] Auch die Bundespolizei und der Zoll holen vor Durchführung der Maßnahme eine Anordnung nach § 100i StPO ein, ebenso der Generalbundesanwalt (GBA). Der Bundesnachrichtendienst (BND) versendet die „Stille SMS“ aufgrund des BND- und des G10-Gesetzes, auch das Bundesamt für Verfassungsschutz (BfV) und der Militärische Abschirmdienst (MAD) stützen ihre „Stille SMS“ darauf. Die Behörden nutzen die Methode in unterschiedlichem Maße. So werden „Stille SMS“ auf Bundesebene vor allem vom BfV versandt, die Zahlen bewegen sich stets um die 100.000 „Ortungsimpulse“ pro Halbjahr. Im 2. Halbjahr 2017 stiegen die heimlichen Textnachrichten beim BfV auf einen Spitzenwert von fast 180.000. Die Zahlen für die Bundespolizei liegen deutlich niedriger (2. Halbjahr 2018: 50.654; 1. Halbjahr

2018: 38.990; 1. Halbjahr 2019: 20.152) [2]. Eine Abnahme verzeichneten im vergangenen Jahr die Stillen SMS des Bundeskriminalamts (BKA). In der zweiten Jahreshälfte hatte die Behörde 21.337 versandt, rund ein Drittel weniger als zuvor, im 1. Halbjahr 2019 waren es nur 6.302.

Die Schwankungen erklären sich im Polizeibereich durch besondere Ermittlungsverfahren. So hatte die Bundespolizei in 2016 in einem Fall wegen des *„banden- und gewerbsmäßigen Diebstahls zum Nachteil der Deutschen Bahn*“ ermittelt. [3] Zu den Gründen des „Ausreißers“ des BfV in 2017 ist nichts bekannt. Die Zahlen zu den einzelnen Maßnahmen sind jedoch nur bedingt aussagekräftig und müssen mit den Ermittlungsverfahren und davon betroffenen Personen ins Verhältnis gesetzt werden. Diese werden nicht immer statistisch erfasst. So können beispielsweise die Zahlen von „Stillen SMS“ deutlich zurückgehen, dabei aber trotzdem mehr Personen überwacht werden.
Während die Bundesregierung zwar Angaben zu „Stillen SMS“ des BKA und der Bundespolizei macht, unterbleibt hinsichtlich des BND schon immer jede Angabe. Eine ähnliche Verschwiegenheit entwickelte das BMI vor sechs Jahren für das Finanzministerium, dessen Zollkriminal- und Zollfahndungsämter ebenfalls massenhaft Stille SMS verschicken. Im Jahr 2012 erzeugten die Zollbehörden fast 200.000 „Ortungsimpulse“, im darauf folgenden Halbjahr zeigte sich eine weiter stark steigende Tendenz.

Seit diesem Jahr hat das BMI auch die Zahlen für das BfV als geheim eingestuft. Zur Begründung heißt es, die Informationen seien besonders schutzbedürftig, da sich *„durch die regelmäßige halbjährliche Beantwortung […] Einzelinformationen zu einem umfassenden Lagebild verdichten können*“. Die halbjährlichen Abfragen führten zu solche einer „Verdichtung“, auf diese Weise könnten Rückschlüsse auf die „technischen Fähigkeiten“ des Geheimdienstes gezogen werden. [4] Das mag zwar aus Sicht der Behörde zutreffen. Jedoch hätte die Angaben auch als „*VS – Nur für den Dienstgebrauch*“ hochgestuft werden können, womit sie weiterhin per Hauspost an die Abgeordneten versandt würde. Mit der Einstufung als „VS – Geheim“ darf die Antwort nur von Abgeordneten und anderen, besonders berechtigten Personen in der Geheimschutzstelle eingesehen werden. Die Wissenschaftlichen Dienste des Bundestages betonen, dass derartige Auskunftsbeschränkungen dem verfassungsrechtlichen Verhältnismäßigkeitsgebot unterliegen. [5] Die Bundesregierung muss demnach mildere, gleich geeignete Mitteln suchen, anstatt die vorher offen mitgeteilten Informationen nunmehr als „VS –Geheim“ einzustufen. Auch die Verschlusssachenanweisung (VSA) bestimmt in § 15 S. 3, dass ein geringerer Einstufungsgrad oder ein anderes, einer Geheimhaltung gleich geeignetes, Mittel Vorrang haben muss.

Ein Blick auf die Bundesländer zeigt eine deutliche Zunahme dort verschickter „Stiller SMS“. So hat die Polizei Berlin im Jahr 2015 noch rund 138.000 heimliche Textnachrichten erstellt, 2018 hat sich die Zahl mehr als verdreifacht. [6] In Schleswig-Holstein wurden im Jahr 2016 rund 45.000 „Stille SMS“ genutzt, diese Zahl wurde 2018 schon im ersten Halbjahr erreicht. [7] Eine ähnliche Steigerung zeigt sich in Rheinland-Pfalz [8] und in Brandenburg [9]. Dort wird die Methode als „0-SMS“ bezeichnet. Weitere Informationsfreiheits-Anfragen zur Zahl „Stiller SMS“ liefen ins Leere. [10] Bundesländer wie Bayern haben kein solches Gesetz erlassen, das Saarland oder Sachsen-Anhalt verlangen trotz Informationsfreiheitsgesetz auch bei Nichtauskunft abschreckende Gebühren. Die meisten Ministerien halten Angaben zu den Landesämtern für Verfassungsschutz unter Verschluss. Dort, wo sie mitgeteilt werden, sind die Zahlen vergleichsweise niedrig. Daraus lässt sich schließen, dass unter den Inlandsgeheimdiensten vor allem das BfV für die heimliche Ortung zuständig ist. Nicht immer bekannt ist die Zahl der Ermittlungsverfahren, für die in den Bundesländern „Stille SMS“ eingesetzt werden. Nur manche Behörden müssen protokollieren, in welcher Frequenz (etwa täglich oder stündlich) eine Person heimlich verfolgt wird. Im Land Brandenburg konnte die Häufigkeit der Maßnahme nur „*anhand der Rechnungsführung*“ beziffert werden.

Funkzellenabfrage

Zur Geolokalisierung von Mobiltelefonen können die Polizei, der GBA und die Zollbehörden nicht-

individualisierte Funkzellenabfragen durchführen. [11] Dabei erkundigt sich die Polizei bei den Netzbetreibern, welche Mobiltelefone in einem konkreten Zeitraum in einer bestimmten Funkzelle genutzt wurden. Funkzellenabfragen werden auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet. § 100g Absatz 3 StPO erlaubt die Maßnahme für Ermittlungen zu schweren oder staatsgefährdenden Straftaten oder auch wegen des Einschleusen von Ausländern und Verstößen gegen das Betäubungsmittelgesetz. Nach einer Gesetzesänderung von 2017 können Funkzellenabfragen auch nach einem Wohnungseinbruch erfolgen. [12]

Eine Funkzelle bestimmt sich über den Sendemast, der einen bestimmten Radius abdeckt. Im urbanen Raum ist eine Funkzelle wenige Hundert Meter groß, auf dem Land kann sie viele Kilometer umfassen. Anhand der Verkehrsdaten können die Polizei und der Zoll anschließend die zugehörigen Anschlussdaten abfragen. Auch ohne ein Gesetz zur Vorratsdatenspeicherung heben die Firmen die Verkehrsdaten ihrer Kund_innen für mehrere Wochen auf. Sie werden bei jedem Telefonat, jeder gesendeten oder empfangenen SMS sowie bei der Internetnutzung des Geräts (auch im Hintergrund) erzeugt. Protokolliert wird der Zeitpunkt einer ausgehenden oder eingehenden Verbindung, ihre Dauer sowie die Rufnummer des Kommunikationspartners. Laut dem Amtsgericht Dresden erhalten die Behörden außerdem Informationen zum Abstrahlungswinkel des sich in der jeweiligen Funkzelle befindlichen Telefons. [13]

Für die Bundespolizei sind die Funkzellenabfragen nicht immer ordentlich protokolliert worden, bis Mitte 2015 sollen sie „weniger als 50“ betragen haben. Im Durchschnitt nimmt die Bundespolizei rund 40 Abfragen pro Halbjahr vor, im 2. Halbjahr 2018 hat sich dieser Wert auffällig verdoppelt. Äußerst selten wird die Methode vom BKA genutzt, die Zahlen liegen stets im niedrigen einstelligen Bereich. Auffällig ist deshalb ein „Ausreißer“ im 2. Halbjahr 2017 mit 149 Maßnahmen. Funkzellenabfragen des BKA werden auch in Ermittlungsverfahren des GBA angeordnet, das BMI verweist hierzu auf vergangene Ermittlungen wegen „verfassungsfeindliche(r) Sabotage“ und „Bildung einer kriminellen Vereinigung“. [14] Auch die Landeskriminalämter (LKÄ) erledigen Funkzellenabfragen für den GBA, in den letzten Jahren erfolgte dies beispielsweise durch Bayern, Berlin, Nordrhein-Westfalen und das Polizeipräsidium Bochum.

Deutlich öfter werden Funkzellenabfragen in den Bundesländern vorgenommen. 2012 hat die Polizei in Sachsen in 104 Verfahren Funkzellendaten abgefragt, 2017 waren es bereits 427 Verfahren. [15] In Berlin haben Ermittler_innen 2016 bei 491 Einsätzen Funkzellenabfragen anordnen lassen [16], die Polizei erhielt daraufhin 112 Millionen Verkehrsdatensätze. Neben schweren Straftaten wie Bandendiebstahl, Raub, Mord und Herbeiführen einer Sprengstoffexplosion finden sich auch Maßnahmen wegen Landfriedensbruch, Betrug sowie Nötigung. In 2017 Fällen ermittelte die Polizei anschließend 2.222 Inhaber_innen der Telefone.

IMSI-Catcher

Mobile oder stationäre IMSI-Catcher simulieren eine Funkzelle, in die sich die Mobilfunkgeräte der Umgebung wegen der Signalstärke des Geräts automatisch einbuchen. Strafverfolgungsbehörden und Geheimdienste nutzen IMSI-Catcher, um einer observierten Zielperson ein Telefon zuordnen zu können. Dabei werden die Gerätenummern (IMEI) und Kartennummern (IMSI) ermittelt. Daraufhin können bei den Telefonanbietern weitere Auskünfte angefragt werden, darunter Bestandsdaten zu den Besitzer_innen, Verkehrsdaten oder auch Inhalte von Textnachrichten. Einige IMSI-Catcher erlauben auch das Mithören von Gesprächen. Laut dem BMI wird diese Funktion von den Bundesbehörden aber nicht genutzt.

IMSI-Catcher sind seit 2002 im Rahmen des § 100i StPO als Einsatz „technischer Mittel“ für bestimmte Zwecke zugelassen. Bei der Bundespolizei werden sie ausschließlich in strafprozessualen Ermittlungsverfahren eingesetzt, das BKA nutzt sie auch zur Gefahrenabwehr. Während die Bundespolizei IMSI-Catcher pro Halbjahr zwischen 19 und 61 Mal genutzt hat, liegt die Zahl für das BKA zwischen einem und 24 Einsätzen. [17] In 2014 hatte das BfV 13 Ermittlungen mit IMSI-Catchern durchgeführt, die

Zollkriminalämter 51. [18] Der Zoll verfügt über keine eigenen IMSI-Catcher und bedient sich der Amtshilfe anderer Bundes- oder Landesbehörden. Das Gleiche gilt für den GBA, der das BKA, einzelne LKÄ, das Landesamt für Zentrale Polizeiliche Dienste Nordrhein-Westfalen oder auch Polizeipräsidien beauftragt.

Die neue, fünfte Mobilfunkgeneration (5G) ermöglicht Verbindungen mit etappenweiser Verschlüsselung. Für mehr Sicherheit soll die Verschlüsselung bislang der offen übertragenen IMSI und IMEI sorgen. In einigen Jahren werden die unter 3G und 4G genutzten IMSI-Catcher deshalb unbrauchbar. Die Bundesregierung prüft derzeit, welche „*technischen und rechtlichen Anpassungen*“ der noch zu beschließende neue 5G-Standard enthalten soll. [19] Zuständig ist hierfür das *Europäische Institut für Telekommunikationsnormen* (ETSI), das im Dezember den finalen Release #16 beschließen will. Möglich wäre, im geplanten Release #16 dafür zu sorgen, dass die Verschlüsselung der übertragenen IMSI- oder IMEI-Daten, die bei den Netzanbietern an bestimmten Punkten entschlüsselt werden, für eine Abfrage mit richterlichem Beschluss aufgehoben werden muss. Das ETSI kooperiert mit dem weltweiten *3rd Generation Partnership Project* (3GPP), einer Einrichtung der *Internationalen Telekommunikationsunion* (ITU) der Vereinten Nationen, die ebenfalls eine Arbeitsgruppe für behördliche Abhörmaßnahmen betreibt. Die Bundesregierung beteiligt sich mit dem BKA, dem BfV und der Bundesnetzagentur an beiden Arbeitsgruppen. [20] Vermutlich um den Druck auf die Standardisierungsgremien zu erhöhen, hat das BMI seit Juli diesen Jahres auch die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (ZITiS) entsandt. [21]

Für das BMI kommt die Einführung von 5G zur Unzeit, denn erst in 2017 hat das BKA Forschungen zur Verbesserung seiner IMSI-Catcher begonnen. [22] Unter dem Namen „Catch“ unterstützt die Europäische Kommission ein vierjähriges Projekt im Rahmen des EU-Fonds zur Inneren Sicherheit mit 338.580 Euro, weitere Partner sind nicht beteiligt. Durch Mehrfachmessungen soll die Ortung von Mobiltelefonen unter 3G und 4G genauer werden. Schließlich wird das Forschungsprojekt auch mit der „*Eigensicherung der eingesetzten Polizeibeamten*“ begründet, da die Polizist_innen stets „*im Nahbereich der Zielperson agieren*“ müssten. Weitere Erläuterungen liefert das Bundesinnenministerium hierzu nicht.

Bürgerrechte und Transparenz

Die Nutzung von Telefonen als Ortungswanze ist rechtlich umstritten und lässt sich nur schwer einhegen. Dies zeigt sich besonders beim Versand der „Stillen SMS“. Eine Telekommunikationsüberwachung darf eigentlich nur als „passive Tätigkeit“ ausgeführt werden. Das Erzeugen eines Kommunikationsvorgangs mittels „Stiller SMS“ ist aber eine aktive Maßnahme, die nicht von den Betroffenen der Maßnahme stammt. Dies kritisiert unter anderem Tobias Singelnstein, Professor für Kriminologie an der Juristischen Fakultät der Ruhr-Universität Bochum, seit einigen Jahren. [23] Im letzten Jahr hatte der Bundesgerichtshof (BGH) dazu geurteilt und sich der Auffassung Singelnsteins teilweise angeschlossen. [24] Der Einsatz „Stiller SMS“ und die Erhebung daraus generierter Standortdaten können demnach nicht auf § 100a der Strafprozessordnung gestützt werden, da die erzeugten Standortdaten nicht im Rahmen der Telekommunikation anfallen. Bei einer „Stillen SMS“ fehlt es laut dem BGH „*an einem menschlich veranlassten Informationsaustausch*“.

Trotzdem hat das Gericht festgestellt, dass die „Stille SMS“ bei einem Verdacht auf Straftaten von „erheblicher Bedeutung“ genutzt werden darf. Diese Eingriffsbefugnis ergebe sich aus § 100i Abs. 1 Nr. 2 StPO. Die Vorschrift regelt den Einsatz technischer Mittel zur Ermittlung des Standorts eines Mobilfunkgerätes und war bei ihrer Verabschiedung 2002 auf IMSI-Catcher zugeschnitten. Ob das Urteil die Hürde für den Einsatz der Ortungsimpulse in der Praxis höher legt, ist aber unklar. Dazu schreibt das BMI, dass für die Bundespolizei nach dem Urteil die Einholung einer Anordnung nach § 100i StPO verfügt worden sei. [25] Im 2. Halbjahr 2018 waren daraufhin noch keine nennenswerten Änderungen der Praxis zu verzeichnen, im Halbjahr darauf haben sich die Maßnahmen von Bundespolizei und BKA jedoch –

womöglich als Folge des BGH-Urteils – mehr als halbiert.

Im Gegensatz zur „Stillen SMS“ geraten über eine Funkzellenabfrage massenhaft Unbeteiligte ins Raster der Polizei. Im Bereich linker sozialer Bewegungen wurde dies zuerst in 2011 offenkundig, nachdem das LKA Sachsen Funkzellenabfragen bei Demonstrationen durchgeführt hat. In Ermittlungen gegen eine antifaschistische Gruppe erhielt die Polizei insgesamt 1.145.055 Verkehrsdatensätze zu 330.00 Personen, deren Telefone sich in den abgefragten Funkzellen eingebucht hatten. Darunter befanden sich nicht nur Demonstrationsteilnehmer_innen, sondern vorwiegend Einwohner_innen und Besucher_innen der betreffenden Stadtteile. In Dresden hatte das LKA in drei verschiedenen Verfahren anschließend zu 58.911 Personen Namen und Adressen herausverlangt und im Fallbearbeitungssystem der sächsischen Polizei gespeichert. Mithilfe der Software wurden in einem Datamining-Verfahren 1.210 Personen und Telefone herausgefiltert, die zu „*bei Ermittlungshandlungen sichergestellten oder beschlagnahmten Mobiltelefonen, Speichermedien, oder schriftlichen Unterlagen*“ gehören könnten. Der Abgleich mit Funkzellenabfragen mit anderen Ereignissen ergab weitere 844 verdächtige Telefoninhaber_innen an mindestens vier von 17 „Ereignis- bzw. Tatorten“. Als besonders verdächtig galten dabei Telefone, bei denen ein Gerät in der Vergangenheit mehr als eine SIM-Karte verwendet hatte.

Problematisch ist auch, dass die Bestandsdaten zu Verkehrsdaten aus Funkzellenabfragen ohne richterlichen Beschluss von den Netzanbietern beauskunftet werden. [26] Das lässt befürchten, dass in Verfahren wie in Dresden sämtliche Namen, Anschriften sowie weitere Daten von Hunderten „verdächtigen“ Telefoninhaber_innen in den Ermittlungsakten landen. Laut dem Jahresbericht der Bundesnetzagentur sind die Zahlen dieser als „Behördentelefonbuch“ bezeichneten Bestandsdatenauskunft abermals stark gestiegen. Im Jahr 2018 wurden demnach 13,94 Millionen Ersuchen bearbeitet. Fast 750.000 dieser automatisierten Auskunftsverfahren stammten vom BfV, in über 11.000 Fällen hat der Geheimdienst andersherum die Telefonnummern einer bestimmten Person abgefragt. [27] Das BKA führt hierzu keine Statistiken.

Die von Funkzellenabfragen Betroffenen werden gewöhnlich nicht über die Erhebung ihrer Verkehrs- oder Bestandsdaten informiert. Aus Sicht der Polizei haben lediglich jene, gegen die sich die Maßnahmen richteten, ein Recht auf Benachrichtigung. Aber auch diese Verdächtigen oder Beschuldigten haben beispielsweise vom LKA Sachsen keine solche Benachrichtigung erhalten. Nur das Land Berlin hat mittlerweile ein sogenanntes *Funkzellenabfragen-Transparenz-System* (FTS) eingeführt. [28] Rund 10.000 Interessierte haben ihre Mobilfunknummer dort in einer Datei hinterlegt. Falls diese Nummer dann bei einer Funkzellenabfrage erfasst wurde, werden die Inhaber_ innen nach Abschluss der Ermittlungen im Falle der Verarbeitung ihrer Verkehrsdaten benachrichtigt.

Gemeinsame Kompetenz- und Dienstleistungszentren

Mehrere Bundesländer schließen sich derzeit zu „*Gemeinsamen Kompetenz- und Dienstleistungszentren*“ auf dem Gebiet der polizeilichen Telekommunikationsüberwachung (GKDZ) zusammen. Zuerst hatte die Innenministerkonferenz von Hamburg, Niedersachsen, Mecklenburg-Vorpommern, Schleswig-Holstein und Bremen in 2008 eine Initiative zur Errichtung eines „TKÜ-Zentrums Nord“ beschlossen. Ein zweites GKDZ wird in Leipzig und Dresden errichtet, beteiligt sind Sachsen, Brandenburg, Thüringen, Sachsen-Anhalt und Berlin. [29] Die GKDZ sollen Bau-, Investitions- sowie Betriebskosten in den beteiligten Ländern einsparen, ihre Finanzierung erfolgt anteilig nach dem Königsteiner Schlüssel. Weitere Einzelheiten sind in einem Staatsvertrag geregelt. [30] Der Wirkbetrieb beider Zentren soll in 2020 starten. [31]

Das Ziel der Einrichtungen besteht laut einer Präsentation des sächsischen Staatsministeriums des Innern im „größtmögliche(n) Zentralisieren“ polizeilicher Überwachungsaufgaben. [32] Die Planung des GKDZ in Leipzig und Dresden erfolgte mithilfe externer Beratung durch die *ESG Elektroniksystem- und Logistik-GmbH*, die im Militärbereich regelmäßig Aufträge der Bundesregierung übernimmt. Daran beteiligt war das

„*Strategie- und Forschungszentrum Telekommunikation*“ (SFZ TK), in dem das Bundeskriminalamt, die Bundespolizei und das Bundesamt für Verfassungsschutz in einer „Kooperationsplattform“ organisiert sind. [33]

Als „zentraler Dienstleister“ sollen die GKDZ alle Formen der operativen Telekommunikationsüberwachung ausführen. Aus der Präsentation des sächsischen Staatsministeriums geht hervor, dass Server zur Ausleitung der bei den Netzanbietern abgehörten Telekommunikationsdaten betrieben werden. Die über diese Schnittstellen gesammelten Daten werden in den GKDZ gespeichert. Hierfür werden Server mit einer „*Speicherfähigkeit im Petabyte-Bereich*“ eingekauft. Sofern technisch möglich, sollen die Zentren auch die „*Analyse verschlüsselter Kommunikation und ggf. deren Entschlüsselung*“ besorgen. Welche technischen Werkzeuge hierfür genutzt werden, bleibt offen.

Vermutlich übernehmen die Zentren aber auch Einsätze von „Stillen SMS“ oder Trojaner-Programmen. Das bestätigt die Antwort des Berliner Senats auf eine Anfrage der Piratenpartei. [34] Wie diese „technische Dienstleistung“ umgesetzt wird, soll erst in einer späteren „Feinplanung“ definiert werden. Derzeit erfolgt der Versand von „Stillen SMS“ bei den Kriminalämtern oder Geheimdiensten mithilfe kommerzieller Software, etwa von der Schweizer Firma *Vadian* oder der deutschen Firma *Syborg*. [35] Andere Behörden wie beispielsweise der GBA und der Zoll greifen auf Anlagen von Bundes- und Landespolizeibehörden zurückgreifen. In einigen Bundesländern werden die „Stillen SMS“ nicht von den Behörden selbst, sondern von privaten Dienstleistern verschickt.

Es ist zu befürchten, dass die Maßnahmen zur Telekommunikationsüberwachung im Rahmen der §§ 100 StPO unter einem zentralisierten GKDZ weiter zunehmen werden. Eine weitergehende Kritik an den Zentren hatte Hartmut Aden vor zwei Jahren in einer Stellungnahme zum Gesetzentwurf der sächsischen Staatsregierung formuliert. Länderübergreifende Strukturen wie ein GKDZ seien nicht grundsätzlich wirtschaftlicher als einzelne Anlagen in den Bundesländern. So erhöhe sich beispielsweise der „*Abstimmungs- und Reisebedarf*“, als komplexe Behörde erwartet Aden für die GKDZ einen „*erheblichen administrativen Aufwand*“. Auch sei nicht belegt, weshalb ausgerechnet die Telekommunikationsüberwachung als länderübergreifendes Kooperationsfeld gewählt wird. Diese wird immer im Auftrag eines der beteiligten Länder durchgeführt, Querverbindungen zwischen den zu bearbeitenden Fällen erwartet Aden nicht. Die dort erlangten Erkenntnisse landeten weiterhin in den dezentralen polizeilichen Vorgangsbearbeitungssystemen der Landespolizeibehörden.

Schließlich sei auch die Verantwortung und Kontrolle der in einer Telekommunikationsüberwachung erhobenen Daten im Staatsvertrag unklar formuliert. Möglich sei, dass die Länder weiterhin für Abhörmaßnahmen zuständig sind und lediglich deren Auswertung in den GKDZ erfolge. Der Staatsvertrag enthalte aber keine Regelung dazu, wer für eine rechtswidrige Datenverarbeitung haftet. Zwar sei mit der dezentralen Zuständigkeit aller Datenschutzbeauftragten der beteiligten Länder eine Datenschutzkontrolle gegeben, eine datenschutzrechtliche klare Regelung für eine „Gesamtbetrachtung“ fehle jedoch. In Einzelfällen könne dies zu einer „*fragmentierten und damit unzulänglichen Kontrolle*“ führen.

MATTHIAS MONROY *ist Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift Bürgerrechte & Polizei/CILIP. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in linken Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, Netzpolitik und in Freien Radios.*

Anmerkungen:

1 I. V. m. § 100g Absatz 1 Satz 3, Absatz 2 StPO.

2 BT-Drucksache 19/7847 vom 18.02.2019, BT-Drucksache 19/3678 vom 03.08.2018.

3 BT-Drucksache 18/9931 vom 07.10.2016.

4 Schreiben des Parlamentarischen Staatssekretärs Günter Krings an den MdB Andrej Hunko vom

11.03.2019.

5 WD 3 - 3000 – 121/19.

6 AGH Berlin, Drucksache 18/17664 vom 07.02.2019.

7 https://fragdenstaat.de/anfrage/versand-stiller-sms-2016-2017-und-2018-8.

8 https://fragdenstaat.de/anfrage/versand-stiller-sms-2016-2017-und-2018-6/109167/anhang/AntwortschreibenHerrNAME_geschwaerzt.pdf.

9 https://fragdenstaat.de/anfrage/versand-stiller-sms-2016-2017-und-2018-5/108552/anhang/20181029_polizei_brandenburg_stille_sms_geschwaerzt.pdf.

10 https://fragdenstaat.de/anfragen/?q=stiller+sms.

11 Der BND, das BfV sowie der MAD verfügen hierfür über keine Rechtsgrundlage.

12 https://www.heise.de/newsticker/meldung/Bundesrat-Polizei-darf-Einbrecher-mit-Vorratsdaten-und-Funkzellenabfragen-jagen-3767230.html.

13 https://cdn.netzpolitik.org/wp-upload/2013-04-04-AG-DD-FZA.pdf.

14 BT-Drucksache 19/505 vom 23.01.2018.

15 https://netzpolitik.org/2018/sachsen-funkzellenabfragen-vervierfachen-sich-in-fuenf-jahren.

16 AGH Berlin, Drucksache 18/1012 vom 24.04.2018.

17 https://netzpolitik.org/2018/halbjahreswerte-fuer-stille-sms-imsi-catcher-und-funkzellenabfragen.

18 BT-Drucksache 18/2257 vom 01.08.2014.

19 BT-Drucksache 19/10535 vom 31.05.2019, vgl. auch ein entsprechendes Papier der rumänischen EU-Ratspräsidentschaft vom 11.04.2019 (http://statewatch.org/news/2019/jun/eu-council-europol-position-paper-5g-8268-19.pdf) und des EU-Anti-Terrorismus-Koordinators vom 06.05.2019 (http://statewatch.org/news/2019/jun/eu-council-ctc-5g-law-enforcement-8983-19.pdf).

20 BT-Drucksache 17/11239 vom 26.10.2012.

21 S. https://netzpolitik.org/2019/5g-bundesregierung-will-anbieter-zur-ueberwachung-zwingen.

22 BT-Plenarprotokoll 18/220 vom 08.03.2017.

23 „Die 'stille SMS' ist nicht durch die Strafprozessordnung gedeckt“, www.heise.de vom 04.04.2012.

24 BGH, 08.02.2018 - 3 StR 400/17.

25 „Seit Bekanntwerden des Beschlusses“ erfolge auch in den beim GBA geführten Ermittlungsverfahren die Versendung von „Stillen SMS“ auf Anordnung gemäß § 100i Absatz 1 Nummer 2 StPO.

26 https://netzpolitik.org/2019/bestandsdatenauskunft-2018-behoerden-haben-alle-zwei-sekunden-abgefragt-wem-eine-telefonnummer-gehoert

.

27 BT-Plenarprotokoll 19/103 vom 05.06.2019.

28 https://fts.berlin.de.

29 https://www.sicherheit.sachsen.de.

30 Das „TKÜ-Zentrum Süd“ wurde Anfang 2018 als rechtsfähige Anstalt öffentlichen Rechts (GKDZ AöR) gegründet, die Gesamtkosten sollen 16 Millionen Euro betragen haben, vgl. https://www.mdr.de/thueringen/start-abhoerzentrum-verzoegert-sich-100.html.

31 Bürgerschaft der Freien und Hansestadt Hamburg, Drucksachen 21/93 vom 24.03.2015, 21/10571 vom 10.10.17 und 21/16107 vom 15.02.19 sowie Sächsisches Staatsministeriums des Innern, Antwort auf die Drucksache 6/15566 vom 03.01.2019.

32 https://cdn.netzpolitik.org/wp-upload/GKDZ_TKUE.pdf.

33 BT-Plenarprotokoll 18/214 vom 25..01.2017.

34 AGH Berlin, Drucksache 17/17 vom 11. Januar 2016.

35 https://www.heise.de/newsticker/meldung/Trojaner-und-stille-SMS-ein-lukratives-Geschaeft-1633724.html, BT-Drucksache 17/10077 vom 02. 07. 2012.

36 https://www.researchgate.net/publication/320711097_Stellungnahme_zum_Gesetzentwurf_der_Staatsregierung_Ges_und_Dienstleistungszentrums_der_Polizeien_der_Lander_Berlin_Brandenburg_Sa.
