Was die Polizei kann und was sie darf

Massenabfragen von Handydaten durch die Polizei

Thomas Feltes & Dirk Burczyk

11.03.2021 doi: 10.17176/20210311-153928-0

Seit einigen Monaten ermittelt die Sonderkommission BAO-Janus („Besondere Aufbau Organisation Janus") der Polizei Nordrhein-Westfalen gegen 24 Polizeibeamt*innen aus Essen und Mülheim an der Ruhr wegen rechtsextremer Chats. Mitte September 2020 hatte das Innenministerium erstmals mitgeteilt, dass auf dem Handy eines Polizisten im Zuge einer anderen Ermittlung volksverhetzende Bilder gefunden worden waren, darunter Hakenkreuze, gelegt aus Dienstmunition.

Am 18. Februar 2021 ließ die BAO-Janus in einer Massendatenabfrage mehr als 12.700 Rufnummern prüfen, in die die Handydaten der 24 unter Verdacht stehenden Beamt*innen einflossen. Alle dort gespeicherten Telefonkontakte gingen an den Bundesnachrichtendienst, alle Landeskriminalämter, die Bundespolizei und das Bundeskriminalamt, das Bundesamt für Verfassungsschutz, an das Zollkriminalamt und Polizeidienststellen. Ziel der Anfrage war es, herauszufinden, ob den Dienststellen zu den aufgeführten Rufnummern "weiterführende Erkenntnisse (…) im Zusammenhang mit der politisch motivierten Kriminalität rechts" vorliegen. Das zuständige LKA NRW kommentierte die Abfrage: „Aufgrund der derzeitigen Erkenntnislage lässt sich eine netzwerkähnliche Struktur sowie weitergehende Verbindungen in die rechte / rechtsorientierte Szene […] weder konkret verifizieren, noch mit an Sicherheit grenzender Wahrscheinlichkeit ausschließen. Daher wird hiermit eine Erkenntnisverdichtung hinsichtlich weiterer, möglicher Kontakte angestrebt". Da man davon ausgehen darf, dass angesichts der großen Anzahl von Rufnummern etliche Telefonnummern von unverdächtigen Personen darunter waren, stellt sich die Frage, ob bei dem Verdacht von Straftaten, bei denen es weder um schwere Gewalttaten noch um terroristische oder staatsgefährdende Aktivitäten geht, eine solche Anzahl von Telefonnummern überprüft werden darf.

Die Massenabfragen von Handydaten durch die BAO-Janus stellen Vorfeldermittlungen unterhalb der Schwelle des Verdachtes dar und sind daher rechtswidrig. Auch die Begründung, dass damit eine „Erkenntnisverdichtung" angestrebt werde, kann diesen Eingriff in die Grundrechte der betroffenen Anschlussinhaber nicht rechtfertigen, ebenso wenig wie „kriminalistisches Gespür". Es ist an der Zeit, dass das Bundesverfassungsgericht sich auch mit solchen Vorfeldermittlungen beschäftigt und der Polizei dort rechtsstaatliche Grenzen aufzeigt.

Was genau ist der Anlass der Abfrage?

Vor dem Hintergrund der aktuellen politischen Situation in NRW kann man sich des Eindrucks nicht erwehren, dass hier eine Polizeibehörde mit dem Rücken zu Wand steht und einen Rundumschlag macht, um unbedingt Ermittlungsergebnisse zu präsentieren. In solchen Fällen werden aber, und das haben die polizeilichen Maßnahmen im Zusammenhang mit dem Fall Lügde gezeigt, oft polizeiliche Fehler gemacht. "Unverdächtige werden in die Nähe von Rechten gebracht" titelte der Journalist Ahmet Senyurt vom SWR, der den Vorgang öffentlich machte. Nach Aussage eines dort zitierten Journalisten bleiben die Anfragen und ihr Kontext für zwei Jahre gespeichert. Da es mit dem Programm „Polizei 2020" gerade Bestrebungen von Bund und Ländern gibt, in einem „data ware house" der Deutschen Polizei polizeilich gespeicherte Daten aus Vorgangs- und Fallbearbeitungssystemen möglichst umfassend verfügbar zu machen, steigt die Gefahr solcher möglicherweise präjudizierenden Zuordnungen in der Zukunft eher noch.

Die Abfrage vor dem Hintergrund des Urteils des Bundesverfassungsgerichts vom Mai 2020

Im Mai 2020 hatte das Bundesverfassungsgericht entschieden, dass Abfragen sog. „Bestandsdaten“ zwar grundsätzlich zulässig sind, der Gesetzgeber dabei aber auf die Verhältnismäßigkeit achten müsse. Eingriffsgrundlagen müssen eine hinreichend konkretisierte Gefahr verlangen und in den Regelungen muss insbesondere der Verwendungszweck dieser Daten hinreichend begrenzt und die Tiefe des Eingriffs in die Privatsphäre an den jeweiligen Tatbestand angepasst werden. In dem Verfahren ging es konkret um die Zugriffsmöglichkeiten von Strafverfolgern und Nachrichtenbehörden auf die sogenannten Bestandsdaten der Inhaber von Telefon- und Internetanschlüssen, die in § 113 des Telekommunikationsgesetzes (TKG) sowie mehreren Fachgesetzen des Bundes geregelt sind. Nach dem Bundesverfassungsgericht sind Auskünfte über Daten, die nicht konkret begründet sind, unzulässig. Im Bereich der Strafverfolgung könne eine unterhalb des Anfangsverdachts liegende Eingriffsschwelle nicht genügen, um grundrechtsrelevante Eingriffe vorzunehmen.

Zwar geht es im vorliegenden Fall nicht um die Abfrage von Bestandsdaten, sondern um einen eher allgemeinen Datenabgleich. Allerdings ist dies die Vorstufe zur Abfrage von Bestandsdaten. Spätestens bei Übereinstimmungen wird eine Abfrage von Bestandsdaten erfolgen, mit der Begründung, dass dies zur weiteren Erforschung des Sachverhalts erforderlich ist (§ 100j Abs. 1 S. 1 StPO). Mit „Sachverhalt“ ist gemeint, dass es zumindest irgendeinen Verdacht auf eine Straftat gibt.

Genau dieser Verdacht liegt aber zum Zeitpunkt des Datenabgleichs durch die „BAO Janus“ mit den anderen Behörden nicht vor. Es ist weder nachvollziehbar noch von der Behörde vorgetragen, dass es konkrete Hinweise darauf gibt, dass alle Personen, die sich hinter den 12.700 Telefonnummern im In- und Ausland verbergen, verdächtigt werden, an den Straftaten, die den 24 Polizeibeamt*innen vorgeworfen werden, beteiligt zu sein, noch dass die Kenntnis ihrer Identität zur Erforschung des Sachverhalts beitragen könnte. Im Gegenteil schreibt die „BAO Janus“, dass weitergehende Verbindungen in die rechte Szene nicht konkret zu verifizieren sind. Sie lassen sich, so die Behörden allerdings nicht mit an Sicherheit grenzender Wahrscheinlichkeit ausschließen, und daher wird zur „Erkenntnisverdichtung“ diese Abfrage gestartet. Letztlich geht es also um die Erschließung sozialer Kontakte und Netzwerke mit Personen, die polizeilich irgendwie in Erscheinung getreten sind (hier reicht schon ein bloßer Anfangsverdacht einer Straftat, um in polizeilichen Informationssystemen zu landen), um daraus überhaupt erst Erkenntnisse zur Verbindung der Polizeibeamten zu polizeibekannten Rechtsextremisten erlangen zu können – was an sich noch keine Straftat ist, sondern allenfalls Anhaltspunkte für eine manifeste politische Motivation der Verbreitung verfassungsfeindlicher Kennzeichen liefert. Wir bewegen uns hier also genau in diesem Bereich unterhalb des Anfangsverdachtes, den das Bundesverfassungsgericht ausdrücklich für die Abfrage von Bestandsdaten als nicht ausreichend erklärt hat.

Das Bundesverfassungsgericht hat in einem Beschluss vom Mai 2020 auch deutlich gesagt, dass eine Massendatenabfrage immer verhältnismäßig und zielgerichtet sein muss. Beide Kriterien sind im vorliegenden Fall nicht erfüllt. Wenn die Sonderkommission selbst einräumt, dass man spezielle Verdachtsmomente weder konkret verifizieren noch mit an Sicherheit grenzender Wahrscheinlichkeit ausschließen kann, dann liegt gerade keine zielgerichtete Abfrage vor, was auch schon aus der großen Anzahl der anzufragenden Nummern hervorgeht. Letztlich wird durch einen massenhaften Datenabgleich mit polizeilichen und nachrichtendienstlichen Datensammlungen das Verbot einer Massendatenabfrage in den Regelungen zur Bestandsdatenauskunft umgangen.

Die Frage der Verhältnismäßigkeit

Zwar ist der Eingriff in individuelle Grundrechte gering, zumal die Telefonnummern nicht mit Namen versehen sind. Diese Zuordnung Name-Nummer lässt sich aber einfach herstellen. So hätte eine gründliche Auswertung der Chatverläufe und Telefonbücher sowie der weiteren Social-Media-Aktivitäten der 24 Verdäch-

tigen auch Namen zu einzelnen Telefonnummern ergeben können. Zudem lassen sich die Namen problemlos über die jeweils zuständigen Provider ermitteln – wo wir dann wieder bei der Abfrage von Bestandsdaten wären, zu der sich das BVerfG geäußert hat. Wenn es darum geht, Hintergründe von Chatgruppen aufzudecken, dann ist als erstes kriminalistisches Handwerk und nicht Bauchgefühl gefragt. Weitere, konkrete Recherchen anhand des vorhandenen Datenmaterials, auch wenn dies wohl sehr umfangreich ist, hätten durchgeführt werden müssen, um den Verdacht gegen bestimmte Personen zu erhärten, oder eben auszuschließen. Es verwirrt auch, dass zwar alle Nummern, mit denen die Beschuldigten in Kontakt standen, abgefragt wurden, nicht aber die persönlichen Rufnummern der 24 beschuldigten Polizisten selbst, es sein denn, dies ist schon zuvor geschehen. Dann aber hätte man genau diese Ansatzpunkte gehabt, denen man hätte nachgehen können – mit kriminalistischer Kleinarbeit. Wenig hilfreich ist in diesem Zusammenhang der Verweis auf die „kriminalistische Erfahrung". Sie ist nicht operationalisierbar und damit für Anwälte und Gerichte auch nicht überprüfbar – genau das ist aber Kern rechtsstaatlicher Verfahren. Und doch verbreitet sich der Verweis auf „Erfahrung" von Polizeibeamten immer weiter: ob es um die Zurechnung bestimmter Straftaten zur „Rockerkriminalität" oder um den „grenzpolizeilichen Erfahrungsblick" bei der Auswahl der Reisenden geht, die einer genauen Kontrolle bei der Einreise aus einem anderen Schengen-Staat unterzogen werden. Genau in diesem Graubereich polizeilicher Vorgehensweisen ist auch eine solche Massendatenabfrage als „Fischen im Trüben" anzusiedeln.

Auch wenn die Telefonnummern selbst nicht elektronisch gespeichert werden, sofern es keine Treffer sind, bleibt unklar, was mit den Dateien geschieht. Sie müssten vernichtet werden in dem Moment, wo die Abfrage durchgeführt wird. Nachdem sie aber auf so vielen Computern und bei so vielen Dienststellen gelandet sind, darf man berechtigte Zweifel haben, dass sie wirklich sauber gelöscht wurden. Die Stellungnahe des Landesdatenschutzbeauftragten auf die Anfrage des SWR fällt erstaunlich zurückhaltend aus. Zwar sei der Umfang der abgefragten Daten „erheblich". Die Zulässigkeit richte sich jedoch nach der Erforderlichkeit für die konkreten Ermittlungen, die im „ermittlungstaktischen Ermessen" der zuständigen Polizeibehörde liege. Hinweise auf eine offensichtlich fehlende Erforderlichkeit seien anhand der vorliegenden Informationen nicht ersichtlich. Wie konkret eine „Ermittlungstaktik" aussieht, die ohne konkrete Verdachtshinweise mal so eben 12.700 Telefonnummern abgleichen lässt, dazu äußert sich der Datenschutzbeauftragte nicht. Es ist nämlich keine „Taktik", sondern schlicht Hilflosigkeit oder Bequemlichkeit. Man will oder kann keine anderen Ermittlungen durchführen, und deshalb setzt man auf einen solchen Rundumschlag.

Zudem hätte mit der Möglichkeit, Telefonkontaktdaten aus einschlägigen Verbunddateien aus dem Phänomenbereich Rechtsextremismus (INPOL Innere Sicherheit rechts, INPOL Gewalttäter rechts, evtl. weitere) mit den Kontaktlisten aus den Telefonen abzugleichen – also umgekehrt vorzugehen, eine geeignetere Maßnahme zur Verfügung gestanden. Wenn die „BAO Janus" allerdings davon ausgeht, dass die entsprechenden Kommissariate und Landeskriminalämter nicht alle diesbezüglichen Personen in die Verbunddateien einspeichern, dann liegt dort das Problem.

Tatsächlich ist nicht klar, wozu diese Datenabfrage überhaupt dienen sollte, also ob sie erforderlich war. Festzustellen, dass ein Polizeibeamter die Kontaktdaten zu einem polizeilich bekannten mutmaßlichen Rechtsextremisten privat besitzt, hat an sich erst einmal keine strafrechtliche Relevanz. Es kann sich um einen alten Schulfreund handeln, mit dem einmal im Jahr eine Geburtstags-SMS ausgetauscht wird. Auch da sollten Polizeibeamte sicherlich genauer hinschauen, mit wem sie sich einlassen; hier wird aber regelmäßig nicht einmal die Schwelle zu disziplinarrechtlich relevantem Verhalten überschritten. Es handelt sich, soweit keine Anhaltspunkte vorliegen, dass die Beamt*innen aus politischer Motivation bestimmte Handlungen unternommen oder unterlassen haben, um eine verdachtsgenerierende Maßnahme, bei der noch dazu der generierte Anhalts-

punkt für einen Verdacht eine „Kontaktschuld“ ist. Erst durch die Abfrage sollen Anhaltspunkte für (strafrechtlich möglicherweise sogar irrelevante) Netzwerke generiert werden, die dann als Anhaltspunkte für weitere Ermittlungen dienen.

Skeptisch muss in diesem Zusammenhang auch die Abfrage bei den Verfassungsschutzbehörden gesehen werden. Hier ist nicht nur an das Trennungsgebot von Polizei und Geheimdiensten zu erinnern; es ist auch zweifelhaft, ob die Verfassungsschutzbehörden ihre Erkenntnisse überhaupt vollständig offenlegen. Auch die notorisch mangelnde Informationsehrlichkeit dieser Behörden kann dazu führen, dass polizeiliche Ermittlungen in eine falsche Richtung geführt werden.

Fazit

Insgesamt betrachtet ist die Vorgehensweise der „BAO Janus“, 12.700 Telefonnummern abzugleichen, zumindest kritisch zu sehen und möglicherweise rechtswidrig, weil es sich um unzulässige Vorfeldermittlungen unterhalb der Schwelle des Verdachtes handelt. Die Begründung, dass damit eine „Erkenntnisverdichtung“ angestrebt werde, kann diesen Eingriff in die Grundrechte der betroffenen Anschlussinhaber nicht rechtfertigen, ebenso wenig wie „kriminalistisches Gespür“. Es ist an der Zeit, dass das Bundesverfassungsgericht sich auch mit solchen Vorfeldermittlungen beschäftigt und der Polizei dort rechtsstaatliche Grenzen aufzeigt. Eine unterhalb des Anfangsverdachtes liegende Eingriffsschwelle kann, in Anlehnung an das Urteil des Bundesverfassungsgerichtes vom Mai 2020, auch bei dem Verdacht auf politisch motivierte Straftaten nicht genügen, um grundrechtsrelevante Eingriffe vorzunehmen.

AUTOR*INNEN
Thomas Feltes
Prof. Dr. Thomas Feltes war Professor für Kriminologie, Kriminalpolitik und Polizeiwissenschaft an der Ruhr-Universität Bochum und Strafverteidiger.
Dirk Burczyk
Dirk Burczyk ist Referent für Innenpolitik der Fraktion DIE LINKE im Bundestag und Redakteur der CILIP Bürgerrechte & Polizei.

EMPFOHLENE ZITATION
Feltes, Thomas; Burczyk, Dirk: Was die Polizei kann und was sie darf: Massenabfragen von Handydaten durch die Polizei, Verfassungsblog, 11.03.2021, doi: 10.17176/20210311-153928-0.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20210311-153928-0.