Das Quick-Freeze-Verfahren

Informationspapier

Was ist das Quick-Freeze-Verfahren und welche Ziele werden damit verfolgt?

- Das Quick-Freeze-Verfahren ist ein neues Instrument der Strafverfolgung. Konkret geht es dabei um das „Einfrieren“, also die Sicherung von Verkehrsdaten zum Beispiel IP-Adressen, die Telefonnummern der an einem Anruf beteiligten Anschlüsse und andere Daten, die zum Aufbau einer Verbindung erforderlich sind. Die Strafverfolgungsbehörden sollen diese Verkehrsdaten bei den Telekommunikationsanbietern sichern lassen können. Dafür muss ein konkreter Anlass – der Verdacht, dass eine erhebliche Straftat geschehen ist – bestehen; zudem müssen die „einzufrierenden“ Daten im Zusammenhang mit dieser Straftat stehen können.

Was sind sogenannte Verkehrsdaten, die mit Quick-Freeze gesichert werden können?

- Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Sie werden also beim Betrieb eines Telekommunikationsmittels wie des Handys oder des Computers generiert. Sie lassen zum Beispiel erkennen, wer mit wem, wann und wie lange telefoniert oder SMS austauscht. Diese Daten können auch Rückschlüsse auf den Standort des genutzten Mobiltelefons zulassen. Es handelt sich dabei explizit nicht um die Telekommunikations*inhalte*.
- Bei mobilen Endgeräten gehören auch die über eine Funkzelle vermittelten Standortdaten dazu. Auch die IP-Adresse, die einem Telekommunikationsanschluss für den Zugang ins Internet zu einer bestimmten Zeit zugeordnet war, gehört dazu.

Warum ist die Einführung des Quick-Freeze-Verfahrens sinnvoll?

- Bei der Aufklärung von Straftaten können Verkehrsdaten in bestimmten Fällen hilfreich sein. Das Quick-Freeze-Verfahren soll ermöglichen, die Daten schon zu einem frühen Zeitpunkt der Ermittlungen unter deutlich geringeren Voraussetzungen und in einem deutlich größeren Umfang zu sichern als es bisher möglich ist.

Wie soll das neue Instrument des Quick-Freeze-Verfahren funktionieren?

Das neue Quick-Freeze-Verfahren soll in zwei Stufen ablaufen.

- **Erste Stufe („Einfrieren“):** Die erste Stufe spielt sich regelmäßig in einem frühen Ermittlungsstadium ab. Sobald der Verdacht einer erheblichen Straftat vorliegt, sollen die Strafverfolgungsbehörden relevante Verkehrsdaten schnell und einfach beim

Telekommunikationsanbieter sichern lassen können („Einfrieren“). Dazu sollen sie eine gerichtliche Sicherungsanordnung beantragen können.

- Eine solche Sicherungsordnung setzt nach dem Gesetzentwurf nicht voraus, dass sich der Verdacht bereits gegen eine bestimmte Person richtet. Es reicht, dass die Verkehrsdaten *im Zusammenhang mit* dem Verdacht einer Straftat von erheblicher Bedeutung stehen. Das können zum Beispiel Standortdaten sein, also mit welchem Mobiltelefon zum vermutlichen Tatzeitpunkt an einem bestimmten Ort telefoniert wurde. Auch die Daten des Opfers können damit zunächst einmal gesichert werden. Ist eine Sicherungsanordnung erlassen, dürfen die Telekommunikationsanbieter diese Daten vorerst nicht mehr löschen.
- **Zweite Stufe („Auftauen“):** Erst im weiteren Verlauf der Ermittlungen, wenn sich etwa der Verdacht gegen eine bestimmte Person konkretisiert, dürfen die relevanten Daten auf Grundlage einer weiteren richterlichen Anordnung auf der zweiten Stufe vom Provider an die Strafverfolgungsbehörden übermittelt werden („Auftauen“). Die Strafverfolgungsbehörden können sie dann auswerten und für die Ermittlungen verwenden.

Soll das Quick-Freeze-Verfahren eine gerichtliche Anordnung voraussetzen?

- Ja. Auf beiden Stufen des Quick-Freeze-Verfahrens soll zunächst ein Richter über die Rechtmäßigkeit des Erlasses einer sogenannten Sicherungsanordnung entscheiden. Dieser Richtervorbehalt soll dem Schutz der Grundrechte der betroffenen Personen dienen. Daran hat die Rechtsprechung in den letzten Jahren mit Nachdruck erinnert.
- Die Effektivität des Quick-Freeze-Verfahrens wird durch den Richtervorbehalt nicht beeinträchtigt. Die Gerichte haben vielfach Bereitschaftsdienste eingerichtet, um auch außerhalb der üblichen Geschäftszeiten eine gerichtliche Kontrolle von Ermittlungsmaßnahmen sicherzustellen.
- Für besonders gelagerte Ausnahmefälle, insbesondere bei Gefahr im Verzug, wird zudem eine Eilkompetenz der Staatsanwaltschaft vorgesehen.

Was wäre eine solche „Straftat von erheblicher Bedeutung“, bei der Quick-Freeze-Verfahren zur Anwendung kommt?

- Der Gesetzentwurf sieht vor, dass die Straftat auch im Einzelfall erhebliche Bedeutung haben muss und verweist dazu insbesondere auf den für die Telekommunikationsüberwachung in der Strafprozessordnung (StPO) vorgesehenen Straftatenkatalog (siehe § 100 a Absatz 2 StPO).
- Dort sind unter anderem Raub oder Erpressung, Bandendiebstahl oder bestimmte Formen der Geldwäsche, aber auch Mord und Totschlag sowie sexueller

Kindesmissbrauch und die Verbreitung, der Erwerb und der Besitz kinder- und jugendpornographischer Inhalte aufgelistet.

Wie lange dürfen die Daten eingefroren bleiben?

- Die Sicherung ist zeitlich begrenzt auf höchstens einen Monat, sie kann aber zweimal um jeweils bis zu einen Monat verlängert werden.

Müssen die Betroffenen benachrichtigt werden?

- Die Betroffenen müssen immer dann benachrichtigt werden, wenn ihre Daten an die Strafverfolgungsbehörden übermittelt wurden. Die Benachrichtigung erfolgt erst dann, wenn die Ermittlung dadurch nicht mehr gefährdet werden kann.
- Wenn es beim „Einfrieren" der Daten geblieben ist, ist eine Benachrichtigung ebenfalls vorgeschrieben, wenn die betroffene Person den Strafverfolgungsbehörden bekannt ist.

Die Verkehrsdaten können nur dann gesichert werden, wenn sie bei den Telekommunikationsanbietern noch vorhanden sind. Wie lange ist das der Fall?

- In der Regel speichern die Anbieter die Daten zumindest für einige Tage, manchmal auch länger. Das gilt auch für IP-Adressen. Die Telekom gibt zum Beispiel an, diese Angabe für sieben Tage zu speichern. Dies geschieht in der Regel zu Zwecken der IT-Sicherheit oder zu Abrechnungszwecken.
- Die Strafverfolgungsbehörden haben sich spätestens seit dem Ende der Vorratsdatenspeicherung darauf eingestellt, möglichst schnell an die Anbieter heranzutreten, sodass in den meisten Fällen die fraglichen Daten noch vorhanden sind. Zudem erlauben die bewusst niedrigen Hürden für das „Einfrieren" der Daten, schnell zu handeln.

Wie sehen typische Beispiele aus, in denen das neue Instrument helfen kann?

- Es besteht zum Beispiel der Verdacht eines bandenmäßig begangenen Betrugs. Mehrere Personen könnten damit in Verbindung stehen. Es ist jedoch noch unklar, ob diese Personen im Einzelnen als Täter oder Zeugen in Betracht kommen. In diesem Fall könnten alle Verkehrsdaten der mit der Tat in Verbindung gebrachten Personen bis zur weiteren Aufklärung des Sachverhalts vorläufig gesichert werden.
- Ein anderes Beispiel: Eine Person wird vermisst. Es besteht zwar der Verdacht für einen strafrechtlich relevanten Hintergrund. Aber konkrete Tatsachen, die diesen Verdacht stützen, konnten noch nicht ermittelt werden. In diesem Fall können

beispielsweise Funkzellendaten, also Standortdaten des letzten bekannten Aufenthaltsortes der vermissten Person gesichert werden. Funkzellendaten können auch Aufschluss über die Personen geben, die sich zu einer bestimmten Zeit an einem bestimmten Tatort aufgehalten haben.

Wie erweitert das Quick-Freeze-Verfahren die Befugnisse der Strafverfolgungsbehörden?

- Auch nach geltendem Recht können Strafverfolgungsbehörden Verkehrsdaten erheben. Allerdings gelten dafür höhere Voraussetzungen als nach dem Quick-Freeze-Verfahren. Die derzeitige Übermittlung von Verkehrsdaten an die Strafverfolgungsbehörden (Erhebung nach § 100g Abs. 1 und 3 Satz 1 StPO) setzt den Verdacht einer erheblichen Straftat *gegen eine bestimmte Person* voraus.
- Die neue Sicherungsanordnung auf der ersten Stufe setzt zeitlich früher an. Es genügt dabei, dass die Verkehrsdaten *im Zusammenhang mit* dem Verdacht einer erheblichen Straftat stehen können. Der Verdacht muss sich noch nicht gegen eine bestimmte Person richten. Auch die Daten des Opfers können so gesichert werden.
- Erst im weiteren Verlauf der Ermittlungen werden die Rollen der beteiligten Personen typischerweise klarer. Wenn sich etwa der Verdacht gegen eine bestimmte Person konkretisiert, dürfen die Daten – wie bisher – auf Grundlage einer weiteren richterlichen Anordnung vom Provider an die Strafverfolgungsbehörden übermittelt werden. Daran ändert sich nichts.

Was ist der wesentliche Unterschied zwischen Quick-Freeze-Verfahren und der Vorratsdatenspeicherung?

- Bei der Vorratsdatenspeicherung werden Telekommunikations- und Internetzugangsdienste gesetzlich verpflichtet, Verkehrsdaten massenhaft und ohne konkreten Anlass flächendeckend zu speichern: Internetanbieter müssen also zum Bespiel die für den Zugang zum Internet vergebenen IP-Adressen aller Bürgerinnen und Bürger für die Zwecke der Strafverfolgung speichern. Die frühere Vorratsdatenspeicherung umfasste sogar die anlasslose Speicherung von Verbindungs- und Standortdaten.
- Das Quick-Freeze-Verfahren darf hingegen nur dann zur Anwendung kommen, wenn der Verdacht einer erheblichen Straftat vorliegt. Anders als bei der Vorratsdatenspeicherung muss es also einen konkreten Anlass geben. Es können eben nicht anlasslos alle Daten aller Bürgerinnen und Bürger in Deutschland gespeichert werden.

Warum schlägt das Bundesjustizministerium nicht die Einführung der Vorratsdatenspeicherung vor?

- Gesetzliche Regelungen über eine anlasslose Vorratsdatenspeicherung wurden von Gerichten wiederholt für grundrechts- und europarechtswidrig erklärt. Nachdem das deutsche Umsetzungsgesetz der EU-Richtlinie zur Vorratsdatenspeicherung etwa bereits 2010 vom Bundesverfassungsgericht für nichtig erklärt wurde, erklärte 2014 auch der EuGH die EU-Richtlinie von 2006 für ungültig.
- Auch die gegenwärtig weiterhin existierenden gesetzlichen Regelungen zur Vorratsdatenspeicherung im deutschen Recht sind nicht mit dem Unionsrecht vereinbar. Das hat der EuGH mit Urteil vom 20. September 2022 (C-793/19 und C-794/19) in aller Deutlichkeit klargestellt. Sie sind daher „totes Recht".
- Bislang ist also jeder Versuch, in Deutschland eine umfassende, anlasslose Vorratsdatenspeicherung einzuführen, vor den Gerichten gescheitert. Strafverfolgungsbehörden benötigen aber endlich ein rechtssicheres Instrument zur Sicherung von Verkehrsdaten. Eine anlasslose und flächendeckende Vorratsdatenspeicherung von Verkehrsdaten bietet solche Rechtssicherheit nicht. Die Rechtsprechung des EuGH ist hier sehr eindeutig. Er hat nur einzelne Ausnahmen zugelassen.
- Darüber hinaus gibt es keine empirischen Studien, die belegen, dass eine Vorratsdatenspeicherung die Aufklärungsquote schwerer Straftaten wesentlich erhöhen würde. In den wenigen Jahren, in denen es in Deutschland eine Vorratsdatenspeicherung gab, hat diese zu keinem messbaren Nutzen bei der Aufklärungsquote geführt.[1]
- Im Koalitionsvertrag haben die Regierungsfraktionen der anlasslosen Speicherung von Verkehrsdaten eine Absage erteilt. Dort ist ausdrücklich davon die Rede, dass eine Verpflichtung zur Speicherung von Verkehrsdaten lediglich „rechtssicher anlassbezogen" vorgesehen werden soll.
- Der Bundesjustizminister Dr. Marco Buschmann hat seine Ablehnung einer anlasslosen Vorratsdatenspeicherung wiederholt bekräftigt. So hat er etwa ausgeführt: „Wenn der Staat alle Bürgerinnen und Bürger unter einen Generalverdacht stellt und ihre Kommunikationsdaten speichern lässt, ändern Menschen bereits ihr Verhalten in der Kommunikation und im Netz, weil sie sich nicht unbeobachtet fühlen. Niemand fühlt sich mehr richtig frei".

[1] Vgl. Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht, 2012, abrufbar unter: https://static.mpicc.de/shared/data/pdf/schutzluecken_vorratsdatenspeicherung_12.pdf

Warum wollen Sie nicht wenigstens eine Vorratsdatenspeicherung von IP-Adressen ermöglichen, die der EuGH ausdrücklich zulässt?

- Auch nach den jüngsten Entscheidungen des Europäischen Gerichtshofs besteht erhebliche Rechtsunsicherheit darüber, unter welchen Voraussetzungen eine anlasslose Speicherung von IP-Adressen europarechtskonform wäre. So sagt der EuGH in seinem Urteil Hadopi (C-470/21 vom 30. April 2024), dass eine solche nur für einen „auf das absolut Notwendige begrenzten Zeitraum“ vorgenommen werden darf. Niemand kann genau sagen, wie lange das wäre.
- Jede Regelung über eine anlasslose Speicherung von IP-Adressen wäre also erneut mit der Gefahr behaftet, später von einem Gericht verworfen zu werden. Mit dem Quick-Freeze-Verfahren soll den Strafverfolgungsbehörden daher ein effektives, aber gleichzeitig rechtssicheres Instrument zur Verfügung gestellt werden, auf das sie sich auch verlassen können. Dies wäre nicht der Fall, wenn nun wieder rechtlich ausgetestet würde, „wie viel IP-Datenspeicherung“ der EuGH zulassen würde.
- Auch die massenhafte Speicherung von IP-Adressen ist eine pauschale Überwachungsmaßnahme. Selbst wenn sie rechtlich möglich wäre, heißt das nicht, dass sie auch politisch richtig ist.
- Hinzu kommt: Die Speicherung von IP-Adressen kann durch Kriminelle umgangen werden (z.B. Nutzung von sog. Virtual Private Networks [VPN] oder bestimmter Browser, die die IP-Adresse verschleiern).[2] Der Bundesjustizminister Dr. Marco Buschmann hat sich am 16.05.2024 im Interview mit der Funke Mediengruppe dazu wie folgt geäußert: „Es ist kinderleicht, ein Handy so einzustellen, dass man im Netz keine relevanten Spuren hinterlässt. Dann läuft die Vorratsdatenspeicherung ins Leere. Terroristen wissen das. Dass man ausgerechnet Terroristen mit diesem Instrument das Handwerk legen kann, ist daher nicht sehr plausibel.“

Wie oft scheitern Ermittlungen daran, dass eine IP-Adresse nicht mehr einem bestimmten Anschluss zugeordnet werden kann?

- Die Entwicklung im besonders wichtigen Bereich der Verfolgung von Kindesmissbrauchsdarstellungen im Netz zeigt, dass der Anteil auch ohne das eingriffsintensive Instrument der Vorratsdatenspeicherung erheblich reduziert werden konnte.
- Viele Hinweise auf solche Missbrauchsdarstellungen im Netz erhält das BKA aus den USA. Die Zahl der Fälle, in denen Ermittlungen erfolglos bleiben, weil eine IP-Adresse

[2] BfDI, Tätigkeitsbericht 2023, S. 105.

nicht mehr zuzuordnen ist, lag 2021[3] und 2022[4] nur im mittleren einstelligen Prozentbereich. Ob eine Vorratsdatenspeicherung von IP-Adressen in den verbleibenden Fällen tatsächlich zur Aufklärung geführt hätte, ist unklar.

- Noch vor einigen Jahren war der Anteil an Fällen deutlich höher, in denen die Aufklärung an der fehlenden Zuordnung einer IP-Adresse gescheitert ist (2017: knapp 40 %).[5] Diese Verbesserung konnte allein durch eine Optimierung der Abläufe erreicht werden.
- Auch das Quick-Freeze-Verfahren kann die Arbeit der Behörden erleichtern. Eine Sicherungsanordnung kommt auch dann in Betracht, wenn eine verlässliche Quelle eine Missbrauchsdarstellung mit einer IP-Adresse übermittelt. Die Sicherung der entsprechenden Daten gibt dem BKA dann mehr Zeit für die Prüfung des Hinweises.

Gibt es noch Änderungen am Gesetzesentwurf zu Quick-Freeze-Verfahren aus dem Jahr 2022?

- Grundlage des nunmehr in die Ressortabstimmung gegebenen Entwurfs ist der vom BMJ bereits erarbeitete Referentenentwurf aus dem Jahr 2022. Diesen hat das BMJ unter Berücksichtigung der Verständigung innerhalb der Bundesregierung vom April 2024 punktuell angepasst. An dem Quick-Freeze-Verfahren Verfahren selbst hat das BMJ aber keine Änderungen vorgenommen.
- Allerdings werden die Paragrafen zur Vorratsdatenspeicherung, die die StPO weiterhin enthält, aufgrund einer zwischen den Regierungsparteien getroffenen Vereinbarung nicht aus dem Gesetz gestrichen. Es handelt sich dabei um „totes Recht“. Auf dieser Grundlage kann keine anlasslose Speicherung von IP-Adressen erfolgen. Die anlasslose Speicherung von IP-Adressen ist weiterhin nicht Gegenstand des Referentenentwurfs.

Wie sieht der weitere Zeitplan aus?

- Das Bundesministerium der Justiz hat den Gesetzentwurf veröffentlicht und an die Länder und Verbände verschickt. Dies haben bis zum 6. Dezember 2024 Gelegenheit zu dem Gesetzesentwurf Stellung zu nehmen. Das Bundesministerium der Justiz wird Rückmeldungen zu dem Entwurf auswerten. Sodann soll der Entwurf von der Bundesregierung in den Deutschen Bundestag eingebracht werden.

---

[3] BT-Drucksache 20/535, S. 28: 62.300 strafrechtliche relevante NCMEC-Hinweise (von insgesamt 78.600); in 2.150 Fällen IP nicht abfragbar; entspricht 3,5%.

[4] BT-Drucksache 20/6782, S. 82: 89.844 strafrechtlich relevante NCMEC-Hinweise (von insgesamt 136.437); in 5.614 Fällen IP nicht abfragbar; entspricht 6,25%.

[5] Angaben des Bundesinnenministeriums in der Bundestagsdrucksache 20/534 (S. 27 f.), abrufbar unter https://dserver.bundestag.de/btd/20/005/2000534.pdf