DIGITALE GESELLSCHAFT

«QUICK FREEZE» STATT VORRATSDATENSPEICHERUNG

POSITIONSPAPIER DER DIGITALEN GESELLSCHAFT

Die Digitale Gesellschaft stellt sich gegen die Massenüberwachung in der Schweiz. Das bekannteste Beispiel ist die Vorratsdatenspeicherung. Aufgrund einer Beschwerde der Digitalen Gesellschaft wird der Europäische Gerichtshof für Menschenrechte (EGMR) über die schweizerische Vorratsdatenspeicherung urteilen. Im Hinblick auf das erwartete Urteil empfiehlt die Digitale Gesellschaft den «Quick Freeze» als Alternative zur heutigen Vorratsdatenspeicherung. Mit dem «Quick Freeze» können Strafverfolgungsbehörden in begründeten Fällen auf digitale Daten zugreifen, während die Grund- und Menschenrechte gewahrt bleiben. Voraussetzung dafür ist eine rechtsstaatliche und transparente Umsetzung des «Quick Freeze».

DIGITALE GESELLSCHAFT / CH-4000 BASEL
OFFICE@DIGITALE-GESELLSCHAFT.CH / DIGITALE-GESELLSCHAFT.CH

Was ist die Vorratsdatenspeicherung in der Schweiz?

Die Vorratsdatenspeicherung ist das Sammeln der Daten der Kommunikation aller Menschen auf Vorrat, nämlich ohne Anlass oder Verdacht.

In der Schweiz erfolgt die Sammlung durch Telekommunikationsunternehmen wie Salt, Sunrise und Swisscom, aber auch durch Internet-Provider und Onlinedienste mit Sitz in der Schweiz. Die Unternehmen sind gesetzlich verpflichtet, die sogenannten Metadaten oder Randdaten der Kommunikation während sechs Monaten zu speichern. Diese Daten können Polizei und Staatsanwaltschaften sowie die Geheimdienste in der Schweiz für Ermittlungen nutzen. Die Daten werden auf Vorrat gespeichert, das heisst, die Bevölkerung in der Schweiz wird ohne Anlass unter den Generalverdacht gestellt, gefährlich oder kriminell zu sein.

Diese sogenannten Vorratsdaten zeigen, wer wann, wie und wo mit wem für wie lange kommuniziert hat, sei es direkt, sei es durch die Nutzung von Apps, Onlinediensten und Websites. Die Daten zeigen die beruflichen und sozialen Netzwerke der erfassten Personen. Die Daten ergeben aber auch ein Bewegungsprofil der letzten sechs Monate. Aus diesen Vorratsdaten lassen sich entsprechend umfassende Schlüsse über das Verhalten der gesamten Bevölkerung ziehen, auch wenn die Inhalte der Kommunikation bislang nicht gespeichert werden.

Das erklärte Ziel von Behörden und Politik ist, mit der Vorratsdatenspeicherung die Aufklärung von Straftaten zu erleichtern und zu verbessern. Gängige Schlagworte sind die «Modernisierung der Kriminalitätsbekämpfung» und «gleich lange Spiesse wie Kriminelle».

Wieso ist die Vorratsdatenspeicherung rechtswidrig und unverhältnismässig?

Die Vorratsdatenspeicherung ist eine Form der Massenüberwachung, denn sie betrifft ohne Anlass und Verdacht die gesamte Bevölkerung. Es gibt kein Entrinnen vor der Vorratsdatenspeicherung, zum Beispiel auch nicht für Anwält:innen, Ärzt:innen und Journalist:innen. Entsprechend kann das Berufsgeheimnis oder der Quellenschutz der Medien nicht gewahrt bleiben. Alle Menschen stehen unter Generalverdacht und bleiben im Netz der Vorratsdatenspeicherung hängen.

Gleichzeitig ist die Wirksamkeit der Vorratsdatenspeicherung nicht erwiesen. Ein Vergleich der Aufklärungsquoten zeigte schon vor Jahren, dass die Vorratsdatenspeicherung in der Schweiz nicht zu einer häufigeren Aufklärung von Straftaten führt. Das Gleiche zeigte eine Studie des Wissenschaftlichen Dienstes des Europäischen Parlaments mit Blick auf die Aufklärungsquoten und Kriminalitätsraten in den untersuchten Mitgliedstaaten der Europäischen Union (EU).

In der Folge stellt die Vorratsdatenspeicherung einen unverhältnismässigen Eingriff in die Grund- und Menschenrechte aller Menschen dar, insbesondere in das Grundrecht auf Privatsphäre. Viele höchste Gerichte in Europa, darunter der Europäische Gerichtshof für Menschenrechte (EGMR), erklärten die Vorratsdatenspeicherung deshalb für unzulässig. Wenn überhaupt, ist die Vorratsdatenspeicherung nur ausnahmsweise zulässig, wenn die Datenspeicherung auf das absolut Notwendige beschränkt ist. Im Grundsatz ist die Vorratsdatenspeicherung aber rechtswidrig, gerade auch die Vorratsdatenspeicherung in der Schweiz, die alle Menschen betrifft und eine Aufbewahrung aller Daten während sechs Monaten vorsieht.

Die Digitale Gesellschaft gelangte 2018 mit einer Beschwerde gegen die schweizerische Vorratsdatenspeicherung an den Europäischen Gerichtshof (EGMR). Vorher hatte die Digitale Gesellschaft den Rechtsweg innerhalb der Schweiz ausgeschöpft. Die Digitale Gesellschaft geht davon aus, dass der EGMR im Einklang mit seiner bisherigen Rechtsprechung die schweizerische Vorratsdatenspeicherung als rechtswidrig und unzulässig erklären wird.

Was gilt gemäss dem schweizerischen Datenschutzgesetz?

Die bestehende Vorratsdatenspeicherung in der Schweiz hebelt das Datenschutzgesetz (DSG) aus. Gemäss dem Grundsatz der Zweckbestimmtheit dürfen die Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft und bearbeitet werden. Gemäss dem Grundsatz der Erforderlichkeit müssen Personendaten vernichtet oder anonymisiert werden, sobald sie für den Zweck der Bearbeitung nicht mehr erforderlich ist.

E-Mail-Anbieter, Onlinedienste und Telekommunikationsunternehmen müssen aufgrund der Vorratsdatenspeicherung auch Personendaten bearbeiten, die sie selbst gar nicht benötigen. Sie speichern die Daten der schweizerischen Bevölkerung während sechs Monaten auf Vorrat, weil sie gesetzlich dazu verpflichtet sind.

Wie funktioniert der vorgeschlagene «Quick Freeze»?

Der «Quick Freeze» ist ein Verfahren zur Sicherung der digitalen Daten tatverdächtiger Personen. Das Verfahren ist aus dem Übereinkommen über Cyberkriminalität vom 23. November 2001 bekannt (Budapest-Konvention[1] unter «Umgehende Sicherung»). Der «Quick Freeze» soll eine schnelle und wirksame erste Reaktion auf Cyberkriminalität ermöglichen.

1. Übereinkommen über Computerkriminalität: https://rm.coe.int/168008157a

Beim «Quick Freeze», wörtlich «Schockgefrieren», dürfen Strafverfolgungsbehörden digitale Daten vorsorglich sichern lassen, die aus berechtigten Gründen über tatverdächtige Personen bereits bei Unternehmen vorhanden sind. Bei einem Internet-Provider kann es sich beispielsweise um Daten für die Gewährleistung der Datensicherheit oder für die Rechnungsstellung handeln. Bei einem Online-Dienst kann es sich beispielsweise um Standort-Daten handeln, welche Nutzer:innen freiwillig und informiert geliefert haben, um gewünschte Funktionen nutzen zu können.

Im begründeten Verdachtsfall kann nun eine Strafverfolgungsbehörde «auf Zurufen» die datenschutzrechtlich erforderliche Vernichtung oder Anonymisierung von Daten über tatverdächtige Personen unterbrechen. Die Daten müssen – unter bestimmten Voraussetzungen – umgehend gesichert werden, um allenfalls in einem Strafverfahren verwendet werden zu können.

Welche Voraussetzungen müssen für den «Quick Freeze» gelten?

Der «Quick Freeze» darf aber kein Freipass für die Strafverfolgungsbehörden werden. Die Digitale Gesellschaft fordert deshalb, dass der Eingriff in die Grund- und Menschenrechte der einzelnen betroffenen Personen nur mit einem richterlichen Beschluss unter Wahrung der Justizöffentlichkeit möglich ist. Polizei und Staatsanwaltschaften dürfen die vorsorglich gesicherten Daten nur verwenden, wenn ein Gericht in einem rechtsstaatlichen Verfahren die Verwendung ausdrücklich erlaubt hat. Der «Quick Freeze» darf dabei nur von Strafverfolgungsbehörden eingesetzt werden, nicht aber von Geheimdiensten. Der «Quick Freeze» muss auf ausgewählte schwere Straftaten beschränkt bleiben.

Der «Quick Freeze» als Zwangsmassnahme muss statistisch erfasst und einer fortlaufenden Kontrolle der Verhältnismässigkeit unterzogen werden. Ein richterlicher Beschluss zur Verwendung von Daten aus einem «Quick Freeze» muss der Justizöffentlichkeit unterliegen, sobald keine Geheimhaltung mehr erforderlich ist. Alle betroffenen Personen, beschuldigt oder nicht, müssen so bald wie möglich informiert werden, um ihre Rechte wahren zu können. Solange eine Geheimhaltung erforderlich ist, müssen die Interessen der einzelnen betroffenen Personen vor Gericht durch eine:n unabhängige:n Menschenrechtsanwält:in gewahrt werden. Eine öffentliche Prüfung der Beschlüsse ist erforderlich, um Missbrauch und unzureichende Kontrolle zu verhindern.

Wieso ist der «Quick Freeze» eine wirksame Alternative zur Vorratsdatenspeicherung?

Der «Quick Freeze» ist – unter den genannten Voraussetzungen – eine wirksame Alternative zur anlasslosen und verdachtsunabhängigen Vorratsdatenspeicherung. Im Unterschied zur Vorratsdatenspeicherung werden nicht die Daten der gesamten Bevölkerung auf Vorrat gespeichert. Daten, die für berechtigte Zwecke vorhanden sind, werden in Übereinstimmung mit dem Datenschutzgesetz vernichtet oder anonymisiert, ausgenommen die genannten Bedingungen zu einem «Einfrieren» und zur Nutzung für die Strafverfolgung.

Früher erhobene Statistiken zeigten, dass die Befürchtung, den Strafverfolgungsbehörden könnten entscheidende digitale Daten fehlen, nicht zutrifft. Typische Aufbewahrungsfristen von Daten bewegen sich zum Beispiel bei Internet-Providern häufig im Bereich von mehreren Wochen, selten mehreren Monaten.

Der «Quick Freeze» ermöglicht eine wirksame Strafverfolgung bei gleichzeitigem Verzicht auf die menschenrechtswidrige Vorratsdatenspeicherung. Das gilt aber nur, wenn der «Quick Freeze» wirklich einer wirksamen gerichtlichen und öffentlichen Kontrolle unterliegt.

Zusammenfassend stellt die Digitale Gesellschaft fest:

- Die geltende Vorratsdatenspeicherung ist nicht mit den Grund- und Menschenrechten vereinbar.
- Der «Quick Freeze» ermöglicht hingegen eine wirksame Strafverfolgung.
- Der «Quick Freeze» kann gleichzeitig unter bestimmten Voraussetzungen die Grund- und Menschenrechte wahren.
- Der «Quick Freeze» könnte damit die menschenrechtswidrige Vorratsdatenspeicherung ersetzen.

Die Digitale Gesellschaft fordert im Ergebnis:

- Die Vorratsdatenspeicherung wird in der Schweiz durch den «Quick Freeze» ersetzt.
- Für den «Quick Freeze» gelten die genannten Voraussetzungen.
- Die entsprechenden Anpassungen werden im schweizerischen Recht, insbesondere im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und in der Strafprozessordnung (StPO), vorgenommen.