

# Bestandsdatenneuregelung - der Generalschlüssel zur Internetüberwachung

Grundrechte-Report 2014, Seite 34

Nach den Enthüllungen des Whistleblowers Edward Snowden gibt es keinen Zweifel mehr: Das Vertrauen in Privatheit und Datenschutz sind grundlegend in Frage gestellt. Programme wie Prism und Tempora verdeutlichen, in welchem Umfang das telekommunikative und internetgestützte Nutzungs- und Kommunikationsverhalten von Menschen durch Geheimdienste weltweit erfasst und überwacht wird. Das Fernmeldegeheimnis ist unverletzlich (Artikel 10 Absatz 1 GG) - ein wichtiges Schutzversprechen, das durch die Gerichte längst auch auf Online-Sachverhalte ausgedehnt wird. Doch welchen Wert hat dieses Versprechen gegenüber den Geheimdiensten tatsächlich?

## Zugriff auf Bestandsdaten: skandalöse Ausmaße

Angesichts des Ausmaßes an enthüllten Skandalen erscheint dagegen die Auseinandersetzung um die Bestandsdatenneuregelung erstaunlich leise. Seit Juli 2013 können die rund 250 berechtigten Behörden bei ihren Zugriffen auf sog. Bestandsdaten sich auf reformierte Rechtsgrundlagen berufen. Diese nutzen sie ausgiebig: Die bereits seit längerem massenhafte Praxis des Zugriffs - auch die durch Private wie die sog. Abmahnkanzleien des Urheberrechts veranlasste - auf diese Daten, die inzwischen bei sieben Millionen liegt, hat damit skandalöse Ausmaße angenommen. Beruhigen wollen die Behörden, indem sie betonen, es handele sich gerade nicht um die Inhalte von Kommunikation, und auch nicht um die nach wie vor hochumstrittenen Verkehrsdaten. Doch auch Bestandsdaten haben es in sich: Denn es handelt sich immerhin um Name, Anschrift, Kontodaten, Rufnummern, Anschlusskennungen sowie auch Zugangsdaten (PIN/PUK) und um die für das Surfen im Web notwendig zugeteilten sog. dynamischen IP-Adressen.

Die IP-Adressen sind der zentrale Grund der Neuregelung. Oftmals sind Behörden bestimmte dynamische IP-Adressen bekannt, die für sich allein keinen Rückschluss auf die dahinterstehende Person ermöglichen. Zur Identifizierung müssen die Provider erst zur Herausgabe der die Identifizierung ermöglichenden Bestandsdaten angehalten werden, rechtlich bislang stets eine Formalie. Bestandsdaten sind somit u.a. ein Schlüssel für den Zugriff auf die gesamte "dahinterliegende", beim Provider dokumentierte Kommunikation des Betroffenen, wenn die entsprechenden zusätzlichen rechtlichen Voraussetzungen vorliegen. Die Massenpraxis des Zugriffs führte bereits 2005 zu einer Verfassungsbeschwerde gegen die gesetzlichen Grundlagen. Einerseits bestätigte das Bundesverfassungsgericht 2012 die Kläger in der Auffassung, dass dynamische IP-Adressen dem Schutz von Artikel 10 GG unterfallen. Andererseits verwehrte das Gericht jedoch neben dem Erfordernis einer speziellen Rechtsgrundlage die Nennung einer konkreten Zugriffsschwelle wie die des Richtervorbehalts. Die schwarz-gelbe Koalition legte umgehend einen für die IP-Adressdaten gerade noch verfassungsrechtlich zulässigen Entwurf vor. Den von Sachverständigen als auch von Teilen der Opposition geforderten Richtervorbehalt für diese Daten lehnte sie ab und gewährte diesen stattdessen allein für die ebenfalls datenschutzrechtlich hochsensiblen Zugangssicherungs-codes (PIN/PUK).

# Klammheimliche Ausweitung der Befugnisse

Das letztlich verabschiedete Gesetz führte zudem die ungehörige innenpolitische Tradition des "Draufschaufelns" weiter. Statt der vom Bundesverfassungsgericht verlangten Einschränkung verschärfte die Bundesregierung die einschlägigen Sicherheitsgesetze und weitete die Befugnisse noch aus. Denn im Rahmen der ebenfalls vom BVerfG geforderten fachgesetzlichen Rechtsgrundlagen für die jeweiligen Behörden erweiterte die Bundesregierung klammheimlich die Befugnisse einzelner Behörden für den Zugriff auf die Bestandsdaten. Besonders bedenklich erscheint dies für das Bundeskriminalamt: BKA und das Zollkriminalamt erhalten weitgehend voraussetzungsfreie, neue Zugriffsmöglichkeiten auf Bestandsdaten im Rahmen ihrer Zentralstellenfunktion. Das ist in dieser Pauschalität inakzeptabel, durchbricht die föderale polizeiliche Struktur bzw. vertieft die kompetenzrechtlich problematische Zentralisierung und verstößt zugleich gegen die informationelle Selbstbestimmung der Betroffenen. Und: Zukünftig können die Sicherheitsbehörden selbst bei vielen Ordnungswidrigkeitenverfahren Bestandsdatenabrufe durchführen. Damit wurde eine weitere wichtige Schutzschwelle für den Zugriff auf Bestandsdaten herabgesetzt. Dies wiegt umso schwerer, als der Rückgriff auf Bestandsdaten oft nur einen ersten Schritt bei der zunehmend massenhaften Aushöhlung des Fernmeldegeheimnisses, z.B. bei der Funkzellenauswertung, darstellt. Auch bei dieser Neuregelung bestehen konkrete verfassungsrechtliche Bedenken, wie sie etwa der Bundesdatenschutzbeauftragte im Verfahren vortrug.

Inzwischen ist bereits wieder eine Verfassungsbeschwerde gegen die Neuregelung anhängig. Bis zur Entscheidung wird sich das Web längst wieder grundlegend verwandelt haben: noch mehr Informationen über Bürger, noch bessere Recherche- und Analysemöglichkeiten. Und IP-Adressen werden bis dahin jedem Gerät dauerhaft zugeordnet sein. Diese unter dem Stichwort IPv6 bekannte technische Umstellung hatte das BVerfG in seinem Urteil ausdrücklich in die Beobachtungspflicht des Gesetzgebers gestellt: es bleibt zu hoffen, dass sich Karlsruhe schon deswegen deutlicher dem Zugriff auf die Schlüssel zu unseren Datenspuren entgegenstellen wird.

## Literatur

BVerfG vom 24.1.2012, abrufbar unter: [http://www.bverfg.de/entscheidungen/rs20120124\\_1bvr129905.html](http://www.bverfg.de/entscheidungen/rs20120124_1bvr129905.html)

Stellungnahmen der Anhörung des Innenausschusses des Deutschen Bundestages vom 11. März 2013, abrufbar unter:

[http://bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen\\_SV/index.html](http://bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung26/Stellungnahmen_SV/index.html)

---

<https://www.humanistische-union.de/publikationen/grundrechte-report/2014/publikation/bestandsdaten-neuregelung-der-generalschlüssel-zur-internetueberwachung/>

Abgerufen am: 28.05.2022