HmbBfDI

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Datenerhebung durch polizeiliche Ermittlungsbehörden bei Internet-Dienstanbietern

Ulrich Kühn / Dr. Moritz Karg

Sommerakademie 2014
„Supergrundrecht Sicherheit“ contra digitale Menschenrechte
25. August 2014

Hamburg

HmbBfDI

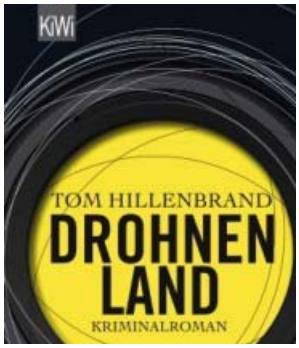
Gliederung

Hamburg

1. **Einleitung**
2. **Risikobetrachtung von Nutzungsdaten**
3. **Praktische Auswertung eines Nutzungsdatenbestandes**
4. **Rechtlicher Rahmen der Auskunftserteilung**
5. **Rechtspolitische Forderungen & Diskussion**

Risikobetrachtung von Nutzungsdaten

ÜBER DIE SENSIBILITÄT SCHEINBAR UNSENSIBLER DATEN



Terry erzählt gerade etwas über Pazzis Verdienste um die Reform der Agrarpolitik. Ich unterbreche ihn. »Du sagtest, er habe keine Familie. War der Typ schwul?«

Der Fahndungscomputer hört auf zu reden, es entsteht eine kurze Pause. Wenn ich es nicht besser wüsste, würde ich glauben, dass er peinlich berührt ist.

»Es gibt diesbezüglich keine offiziellen Statements von Vittorio Pazzi, Hauptkommissar.«

»Mag sein. Aber du kannst doch bestimmt eine Kongruenzanalyse vornehmen.«

»Ich weise Sie darauf hin, dass derartige Daten im Falle von MEPs durch den Enhanced Privacy Act vor behördlichen Zugriffen geschützt sind.«

»Er ist tot, Terry. Und dies ist eine Mordermittlung.«

Wieder eine kurze Pause. »Der Zugriff auf derartige Daten wird protokolliert und in den Gerichtsakten vermerkt.

14

Ferner muss ein unmittelbares Ermittlungsinteresse vorliegen. Ich bin verpflichtet, darauf hinzuweisen, dass laut Artikel 23 der Strafprozessordnung …«

»Reg dich ab.«

»Bitte formulieren Sie die Frage neu.«

»Beantworte meine Frage nach Pazzis sexueller Präferenz und protokolliere, was du willst.«

Auf dem Bildschirm erscheint ein Foto, das Pazzi im Kreise anderer Menschen zeigt. Was man im Hintergrund vom Veranstaltungsort sehen kann, ist unfassbar hässlich. Das lässt mich vermuten, dass es sich um das EU-Parlamentsgebäude handelt. Ein Mann Ende dreißig, der ein Stück von dem Toten entfernt steht, wurde markiert. Er ist strohblond und etwas feist. Seine Wangen sind gerötet, vermutlich von dem Rotwein, den er in seiner Rechten hält.

»Es liegen keinerlei offizielle Informationen zu Vittorio Pazzis sexueller Orientierung vor. Eine Auswertung von Sprachduktus, Semantik, Musikgeschmack, frequentierten Orten und weiteren Datenquellen legt jedoch eine homosexuelle Neigung nahe.«

»Wie sicher ist das?«

»Die Wahrscheinlichkeit beträgt 95,1 Prozent. Die markierte Person auf dem Foto heißt Peter Heuberger, Parlamentsassistent bei der Konservativen Sammlung. Teile von Pazzis Mailverkehr sind aufgrund seines Abgeordnetenstatus derzeit versiegelt und müssen zunächst durch richterliche Anordnung für die digitale Forensik freigegeben werden. Verfügbare private Kommunikationsmuster sowie gemeinsame Airport-Check-ins in Brüssel, Berlin und Lissabon deuten jedoch auf eine partnerschaftliche Beziehung hin.«

15

Realitätscheck:

- "Social networking Web sites, e–mail, instant messaging, telephone, and VoIP are all technologies steeped in network data — data relating one person to another. Network data shifts the locus of information control away from individuals, as the individual's traditional and absolute discretion is replaced by that of his social network. Our research demonstrates a method for accurately predicting the sexual orientation of Facebook users by analyzing friendship associations. After analyzing 4,080 Facebook profiles from the MIT network, we determined that the percentage of a given user's friends who self–identify as gay male is strongly correlated with the sexual orientation of that user …"

(Gaydar: Facebook friendships expose sexual orientation
by Carter Jernigan and Behram F.T. Mistree.
First Monday, Volume 14, Number 10 - 5 October 2009
http://firstmonday.org/ojs/index.php/fm/article/view/2611/2302)

HmbBfDI
Über die Sensibilität scheinbar unsensibler Daten
Hamburg

"Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content…. [It's] sort of embarrassing how predictable we are as human beings."

(Stewart Baker, von 1992-1994 Justiziar der National Security Agency)

"We kill people based on metadata."
(Michael Hayden, von 1999-2005 Direktor der NSA; April 2014)

Auskünfte in DE (jew. 2. HJ 2013) gemäß Transparenzberichten der Unternehmen

Anbieter	Anfragen	Nutzer/Konten	Anfragen erfüllt
Facebook	1687	1950	37,9%
Google	2660	3255	40%
Microsoft	5204	8895	79,9% (Bestands- und Nutzungsdaten)
Twitter	< 10	< 10	33%
Yahoo	3,186	4,164	4,5% Inhaltdaten 63% Bestands- und Nutzungsdaten

Vergleich Dt. Telekom in DE 2013 gesamt

Anschlussüberwachungen	49.796
Verkehrsdatensätze	436.331
Teilnehmerbestandsdaten	28.162
IP-Adressinhaberdaten	946.641

Na gut, dann eben ohne Personenbezug ?

- Was scheinbar ohne personenbezogene Daten funktioniert (keine Bestandsdaten, keine Cookies, keine IP-Adress-Speicherung), ist nicht immer ohne Datenschutzbezug
- Stichwort: Device Fingerprinting, User Tracking

„Canvas fingerprinting, a recently developed form of browser fingerprinting, has not previously been reported in the wild; our results show that over 5% of the top 100,000 websites employ it."

(The Web never forgets: Persistent tracking mechanisms in the wild, Aug. 2014, https://securehomes.esat.kuleuven.be/~gacar/sticky/the_web_never_forgets.pdf)

„Das aktuelle Datenschutzrecht, in seiner Zielsetzung die Persönlichkeitsrechte der Betroffenen auch bei der Nutzung des Internets zu schützen eindeutig, erfasst diese Technologie nicht ausreichend. Einschlägig allerdings sind die Vorgaben zu Transparenz, Erforderlichkeitsprinzip und der Beachtung der Betroffenenrechte des TMG. Telemedienanbieter, die solche Techniken nutzen (sie es in eigener Verantwortung oder durch Dritte), müssen die Nutzer daher umfassend informieren und ihnen zumindest wirksame Opt-out-Möglichkeiten einräumen."

(Karg, Kühn; Datenschutzrechtlicher Rahmen für Device Fingerprinting, ZD 6/2014)

Aus der Datenschutzerklärung eines Internetangebots

Grundsätzlich können Sie das XYZ-Internet-Angebot nutzen, ohne dass wir personenbezogene Daten von Ihnen benötigen. Wir erfahren nur die üblicherweise bei der Internetnutzung anfallenden Verbindungsinformationen. Dazu gehören unter anderem das Zugriffsdatum, die Webseiten, die Sie bei uns besuchen und Ihre IP-Adresse.

IP-Adressen werden von uns als Teil der Schutzmaßnahmen gegen Angriffe von außen für einige Stunden gespeichert und automatisch wieder gelöscht, wenn es im fraglichen Zeitraum keine Auffälligkeiten gab. Ansonsten werden die anfallenden Verbindungsinformationen nur zu statistischen Zwecken ausgewertet. Ein Rückschluss auf einen bestimmten Nutzer ist dabei nicht möglich.

Aus der Datenschutzerklärung eines Internetangebots

Zum Zwecke der Strafverfolgung durch Polizeibehörden, zur Erfüllung der Aufgaben des Verfassungsschutzes, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes sowie zur Durchsetzung des Rechts am geistigen Eigentum behalten wir uns das Recht vor, angeforderte Nutzerdaten an die zuständigen Behörden zu übermitteln.

Ulrich Kühn / Dr. Moritz Karg 25. August 2014 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Aus der Datenschutzerklärung eines Internetangebots

Sie können dieses Portal besuchen, ohne Angaben über Ihre Person zu machen. Um die Qualität unseres Angebots zu verbessern und für Zwecke der statistischen Auswertung erfassen wir die Anzahl der Zugriffe auf die Website, die IP-Adressen, sowie die besuchten Seiten. Diese Daten werden ausschließlich anonym erfasst und erlauben keinen Rückschluss auf Ihre Person. Auf der Grundlage diesen Daten werden auch keine individuellen Bewegungs- oder sonstige Profile erstellt.

Aus der Datenschutzerklärung eines Internetangebots

Wenn Sie unsere Websites besuchen, zeichnet unser Web-Server temporär folgendes Serverprotokoll auf: die IP-Adresse, den Namen der abgerufenen Datei, Datum und Uhrzeit des Abrufs, die übertragene Datenmenge, die Meldung über erfolgreichen Abruf, den Browsertyp nebst Version, das Betriebssystem des Nutzers, die Referrer-URL (die zuvor besuchte Seite) und den anfragenden Provider. Die Erhebung und Verwendung dieser Protokolldaten erfolgt durch uns zum Zweck der Systemsicherheit und der bedarfsgerechten Gestaltung der Webseite. Soweit dies nicht der Fall ist, werden IP-Adressen durch uns vor einer weiteren Verwendung so gekürzt, dass ein eventueller Personenbezug nicht mehr möglich ist. Treten Sie mit uns in ein Vertragsverhältnis, erfolgt die Erhebung und Verwendung der Protokolldaten für Zwecke der Vertragsdokumentation und der Begegnung von Missbrauch.

Rechtlicher Rahmen der Auskunftserteilung

DER ÜBERMITTLUNGSTATBESTAND DES TELEMEDIENGESETZES

Nutzungsdaten im rechtlichen Sinn

Legaldefinition des Telemediengesetzes

- personenbezogene Daten eines Nutzers die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen
- Erforderlichkeit der Verwendung wird durch Zweck des Dienstes bestimmt
  - keine (betriebswirtschaftlichen) Nützlichkeits- oder Zweckdienlichkeitserwägungen
- Beispiele
  - Merkmale zur Identifikation des Nutzers,
  - Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
  - Angaben über die vom Nutzer in Anspruch genommenen Telemedien

Zweckbindung im Telemediengesetz (TMG)

Datenschutzschutzziel „Zweckbindung“

- **Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet und genutzt werden, zu dem sie erhoben worden sind.**
  - § 12 Abs. 2 TMG
    *„Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für **andere Zwecke** nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.“*
    - Verwendung personenbezogener Nutzungsdaten zu anderen als ursprünglichen Erhebungszweck bedarf eine Rechtsgrundlage
    - Erhebungs- und Verwendungszwecke im TMG für Nutzungsdaten
      - Erbringung und Abrechnung des Dienstes (§ 15 Abs. 1, 2 und 4 TMG)
      - unter Pseudonym Werbung, Marketing und Gestaltung des Angebots (§ 15 Abs. 3 TMG)
      - Betrugsprävention und - verfolgung (nur bei Bezahldiensten § 15 Abs. 8 TMG)
      - Strafverfolgung, Gefahrenabwehr -> **Wer sucht der findet!**

HmbBfDI

Zweckänderung „Öffentliche Sicherheit“

Hamburg

Rechtgrundlage zur Übermittlung von Nutzungsdaten

- § 14 Abs. 2 TMG; § 15 Abs. 5 S. 4 TMG
- Verfolgung von Straftaten, Gefahrenabwehr, Aufgabenerfüllung Verfassungsschutz, Geheimdienste und (!) Verfolgung von Urheberrechtsverstößen
- nicht jedoch Persönlichkeitsrechtsverletzungen (BGH Urt. v. 01.07.2014, VI ZR 345/13)
- Keine eigene Übermittlungsvorschrift („Auskunft“/“darf“)
- maßgeblich sind spezialgesetzliche Ermittlungs- und Erforschungstatbestände
  - StPO, BVerfSchG, MADG, BNDG

Adressaten

- **Auskunftsberechtigte § 14 Abs. 2 TMG**
  - Polizei- und Strafverfolgungsbehörden des Bundes und der Länder
  - Verfassungsschutz des Bundes und der Länder
  - BND, MAD
  - Urheberrechtsinhaber (!)
- **Normadressat**
  - Host-Provider, Content-Provider
  - nicht jedoch E-Mail und Access-Provider wg. § 11 Abs. 3 TMG aber ggfs. Geltung des Telekommunikationsgesetzes (§§ 110 – 113a TKG)

Übermittlungsbefugnis

Übermittlung von Nutzungsdaten an Strafverfolgungsorgane

- grds. keine Übermittlungspflicht ohne entsprechende „Anordnung“
- TMG statuiert **keinen Anspruch** der Strafverfolgungsorgane auf Übermittlung
- Recht auf Übermittlung leitet sich aus Aufgabennorm der erhebenden Stelle ab
  - § 8a Abs. 1, 2 Nr. 5 BVerfSchG, § 2a BNDG, § 4a MADG
  - *„Da die Daten auf Grund einer Anordnung einer öffentlichen Stelle erfolgen, liegt die datenschutzrechtliche Verantwortung für die Zulässigkeit der Datenübermittlung nach allgemeinen datenschutz- rechtlichen Grundsätzen bei der öffentlichen Stelle, die die Übermittlung angeordnet hat.“* (BT Drs. 16/3078, S. 16)
- Existenz einer Anordnung impliziert Übermittlungspflicht
  - z.B. § 8b BVerfSchG
    […] (6) Die in § 8a Absatz 1 und 2 Satz 1 genannten Stellen sind verpflichtet, die Auskunft unverzüglich, vollständig, richtig und in dem Format zu erteilen, das durch die auf Grund von Absatz 8 Satz 1 bis 3 erlassene Rechtsverordnung oder in den in Absatz 8 Satz 4 und 5 bezeichneten Rechtsvorschriften vorgeschrieben ist. […]

Realitätsabgleich – Tatbestand

- **„auf Anordnung“ – konkrete Definition im Gesetz fehlt**
  - „gerichtliche“ Anordnung nicht erforderlich
  - Prüfung des Erhebungstatbestandes der erhebenden Stelle?
    - § 8a Abs. 2 BVerfSchG

      Das Bundesamt für Verfassungsschutz darf im Einzelfall Auskunft einholen bei […]

      Nr. 5 denjenigen, die geschäftsmäßig Teledienste erbringen oder daran mitwirken, zu

      a) Merkmalen zur Identifikation des Nutzers eines Teledienstes

      b) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und

      c) Angaben über die vom Nutzer in Anspruch genommenen Teledienste,

      soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist und Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 genannten Schutzgüter vorliegen.
  - Prüfung der Einhaltung der formalen Vorgaben der Anordnung -> § 8b BVerfSchG

Formale Anforderungen an die Anordnung nach BVerfSchG

§ 8b BVerSchG

§ 8b Verfahrensregelungen zu besonderen Auskunftsverlangen

(1) Anordnungen nach § 8a Absatz 2 und 2a werden vom Behördenleiter oder seinem Vertreter beantragt; der Antrag ist schriftlich zu stellen und zu begründen. Zuständig für die Anordnungen ist das Bundesministerium des Innern. Die Anordnung einer Auskunft über künftig anfallende Daten ist auf höchstens drei Monate zu befristen. Die Verlängerung dieser Anordnung um jeweils nicht mehr als drei Monate ist auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Auf die Anordnung der Verlängerung finden die Sätze 1 und 2 Anwendung.

(2) Über Anordnungen nach § 8a Absatz 2 und 2a unterrichtet das Bundesministerium des Innern monatlich die G 10-Kommission (§ 1 Absatz 2 des Artikel 10-Gesetzes) vor deren Vollzug. Bei Gefahr im Verzug kann es den Vollzug der Entscheidung auch bereits vor der Unterrichtung der G 10-Kommission anordnen. Die G 10-Kommission prüft von Amts wegen oder auf Grund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 15 Absatz 5 des Artikel 10-Gesetzes ist mit der Maßgabe entsprechend anzuwenden, dass die Kontrollbefugnis der Kommission sich auf die gesamte Erhebung, Verarbeitung und Nutzung der nach § 8a Absatz 2 und 2a erlangten personenbezogenen Daten erstreckt. Entscheidungen über Auskünfte, welche die G 10-Kommission für unzulässig oder nicht notwendig erklärt, hat das Bundesministerium des Innern unverzüglich aufzuheben. Die Daten unterliegen in diesem Falle einem absoluten Verwendungsverbot und sind unverzüglich zu löschen. Für die Verarbeitung der nach § 8a Absatz 2 und 2a erhobenen Daten ist § 4 des Artikel 10-Gesetzes entsprechend anzuwenden.

(3) Das Bundesministerium des Innern unterrichtet im Abstand von höchstens sechs Monaten das Parlamentarische Kontrollgremium über Anordnungen nach § 8a Absatz 2 und 2a; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen zu geben. Das Gremium erstattet dem Deutschen Bundestag jährlich einen Bericht über die Durchführung sowie Art, Umfang und Anordnungsgründe der Maßnahmen; dabei sind die Grundsätze des § 10 Absatz 1 des Kontrollgremiumgesetzes zu beachten.

(4) Anordnungen sind dem Verpflichteten insoweit schriftlich mitzuteilen, als dies erforderlich ist, um ihm die Erfüllung seiner Verpflichtung zu ermöglichen. Anordnungen und übermittelte Daten dürfen dem Betroffenen oder Dritten vom Verpflichteten nicht mitgeteilt werden.

(5) Dem Verpflichteten ist es verboten, allein auf Grund einer Anordnung nach § 8a Absatz 1 oder 2 einseitige Handlungen vorzunehmen, die für den Betroffenen nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen. Die Anordnung ist mit dem ausdrücklichen Hinweis auf dieses Verbot und darauf zu verbinden, dass das Auskunftsersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten hat oder ein darauf gerichteter Verdacht bestehen müsse.

(6) Die in § 8a Absatz 1 und 2 Satz 1 genannten Stellen sind verpflichtet, die Auskunft unverzüglich, vollständig, richtig und in dem Format zu erteilen, das durch die auf Grund von Absatz 8 Satz 1 bis 3 erlassene Rechtsverordnung oder in den in Absatz 8 Satz 4 und 5 bezeichneten Rechtsvorschriften vorgeschrieben ist.

(7) Für Anordnungen nach § 8a findet § 12 Absatz 1 des Artikel 10-Gesetzes entsprechende Anwendung, mit der Maßgabe, dass § 12 Absatz 1 Satz 5 des Artikel 10-Gesetzes nur für Maßnahmen nach § 8a Absatz 1 und 2 Satz 1 Nummer 4 und 5 Anwendung findet. Wurden personenbezogene Daten an eine andere Stelle übermittelt, erfolgt die Mitteilung im Benehmen mit dieser.

(8) Das Bundesministerium des Innern wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Technologie, dem Bundesministerium der Justiz und dem Bundesministerium der Verteidigung ohne Zustimmung des Bundesrates zu bestimmen, dass Auskünfte nach § 8a Absatz 1 und 2 mit Ausnahme der Auskünfte nach § 8a Absatz 2 Satz 1 Nummer 4, auch soweit andere Vorschriften hierauf verweisen, ganz oder teilweise auf maschinell verwertbaren Datenträgern oder durch Datenfernübertragung übermittelt werden müssen. Dabei können insbesondere geregelt werden 1.die Voraussetzungen für die Anwendung des Verfahrens,

2.das Nähere über Form, Inhalt, Verarbeitung und Sicherung der zu übermittelnden Daten,

3.die Art und Weise der Übermittlung der Daten,

4.die Zuständigkeit für die Entgegennahme der zu übermittelnden Daten,

5.der Umfang und die Form der für dieses Verfahren erforderlichen besonderen Erklärungspflichten des Auskunftspflichtigen und

6.Tatbestände und Bemessung einer auf Grund der Auskunftserteilung an Verpflichtete zu leistenden Aufwandsentschädigung.

Zur Regelung der Datenübermittlung kann in der Rechtsverordnung auf Veröffentlichungen sachverständiger Stellen verwiesen werden; hierbei sind das Datum der Veröffentlichung, die Bezugsquelle und eine Stelle zu bezeichnen, bei der die Veröffentlichung archivmäßig gesichert niedergelegt ist. Die Vorgaben für die Erteilung von Auskünften nach § 8a Absatz 2 Satz 1 Nummer 4, insbesondere ob und in welchem Umfang die Verpflichteten hierfür Vorkehrungen für die technische und organisatorische Umsetzung der Auskunftsverpflichtung zu treffen haben, bestimmen sich nach § 110 des Telekommunikationsgesetzes und der dazu erlassenen Rechtsverordnung. Die technischen Einzelheiten, die zur Auskunftserteilung sowie zur Gestaltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind, insbesondere das technische Format für die Übermittlung derartiger Auskunftsverlangen an die Verpflichteten und die Rückübermittlung der zugehörigen Auskünfte an die berechtigten Stellen, richten sich nach den Festlegungen in der Technischen Richtlinie nach § 110 Absatz 3 des Telekommunikationsgesetzes.

(9) Für die Erteilung von Auskünften nach § 8a Absatz 2 Satz 1 Nummer 4 hat der Verpflichtete Anspruch auf Entschädigung entsprechend § 23 des Justizvergütungs- und -entschädigungsgesetzes.

(10) Die Befugnisse nach § 8a Absatz 2 Satz 1 Nummer 4 und 5 stehen den Verfassungsschutzbehörden der Länder nur dann zu, wenn das Verfahren sowie die Beteiligung der G 10-Kommission, die Verarbeitung der erhobenen Daten und die Mitteilung an den Betroffenen gleichwertig wie in Absatz 2 und ferner eine Absatz 3 gleichwertige parlamentarische Kontrolle sowie eine Verpflichtung zur Berichterstattung über die durchgeführten Maßnahmen an das Parlamentarische Kontrollgremium des Bundes unter entsprechender Anwendung des Absatzes 3 Satz 1 zweiter Halbsatz für dessen Berichte nach Absatz 3 Satz 2 durch den Landesgesetzgeber geregelt ist. Die Verpflichtungen zur gleichwertigen parlamentarischen Kontrolle nach Absatz 3 gelten auch für die Befugnisse nach § 8a Absatz 2 Satz 1 Nummer 1 und 2. Landesrecht kann für Auskünfte an die jeweilige Verfassungsschutzbehörde des Landes Regelungen vorsehen, die dem Absatz 5 entsprechen, und die auf Grund von Absatz 8 Satz 1 bis 3 erlassene Rechtsverordnung sowie die Vorgaben nach Absatz 8 Satz 4 und 5 für solche Auskünfte für anwendbar erklären.

Staatsanwaltschaftliche und polizeiliche Ermittlungsbefugnisse gemäß StPO

- §§ 100, 100a StPO beziehen sich ausdrücklich nur auf Telekommunikation, nicht Telemedien
- § 161 Abs. 1 StPO beinhalten keine spezialgesetzliche Anordnungsbefugnis für Zugriff auf Nutzungsdaten nach dem TMG

- **Gesetzliche Schutzlücke**
  - Nutzungsdaten unterliegen dem Schutz des Fernmeldegeheimnis gemäß § 88 TKG, § 7 Abs. 2 Satz 3 TMG
  - Fehlender Maßstab für Dienstanbieter bezgl. „Prüfung“ der ordnungsgemäßen Anordnung
  - Sensibilität der Nutzungsdaten vergleichbar mit Telekommunikationsdaten oder dem privaten Gespräch im Bad und Schlafzimmer
    - a.A. offenbar LG Oldenburg, Beschluss vom 22.09.2010; 3 Qs 263/10 Anwendung § 161ff StPO – allgemeine Ermittlungsbefugnis

Anforderungsmaßstab des BVerfG, Beschl. v. 13.11. 2010, 2 BvR 1124/10 (Nichtannahmebeschluss)

- „[Der Richtervorbehalt ist nach] … *der Rechtsprechung des BVerfG* [erforderlich]*, wenn sich der Eingriff im Einzelfall als so schwerwiegend darstellt, dass den Anforderungen an die Wahrung der Verhältnismäßigkeit und die Gewährleistung effektiven Rechtsschutzes nur im Wege einer vorherigen richterlichen Kontrolle Rechnung getragen werden kann (BVerfG, NJW 2010, 833). Für die Abfrage und Übermittlung von Telekommunikationsdaten kann dies der Fall sein, wenn diese über einen längeren Zeitraum in großem Umfang gespeichert werden und im Falle ihrer Auswertung detaillierte Rückschlüsse auf das Kommunikations- und Bewegungsverhalten einer Person zulassen würden (BVerfGE107, 299 [319 f.] = NJW 2003, 1787; BVerfG, NJW 2010, 833).“*

Praxisvorschläge

- **Formale Anforderungen**
  - Nur schriftliche Aufforderung durch Strafverfolgungsorgane
    - konkrete Nennung des Vorwurfs
    - Aktenzeichen des Vorgangs
    - Ggfs. „Anordnung“ durch Staatsanwaltschaft
  - keine Ausforschungsermittlung
    - -> § 14 Abs. 2 TMG „im Einzelfall“
    - Eingrenzung Nutzungszeit, Beschränkung der Art der Nutzung, Eingrenzung IP-Adressraum etc.
  - Information der Betroffenen (?)
  - Dokumentation der Gründe für Ablehnung / Durchführung der Übermittlung durch übermittelnde Stelle
- **Materielle Anforderungen**
  - Strenge Erforderlichkeitsprüfung bzgl. Speicherung von Bestands- und Nutzungsdaten
  - Prüfung der Rechtmäßigkeit der Ermittlungsmaßnahme i.d.R. kaum realisierbar
  - Plausibilität bzgl. der Rechtsgüterabwägung vor allem im Bereich der Strafverfolgung

Vielen Dank für die Aufmerksamkeit!

Ulrich Kühn
Stellv. Landesdatenschutzbeauftragter und Referatsleiter Telemedien, Medien und E-Government
Tel.: +49 40 42854 4054
ulrich.kuehn@datenschutz.hamburg.de

Dr. Moritz Karg
Referent für Telemedien, Medien und E-Government
Tel.: +49 40 42854 4051
Moritz.Karg@datenschutz.hamburg.de

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Klosterwall 6, Block C
20095 Hamburg
Tel.: 040 / 428 54-4040
Fax: 040 / 428 54-4000

Fazit &Thesen

1. Nutzungsdaten besitzen hohen Informationsgehalt über Interessen und Nutzungsgewohnheiten der Nutzerinnen und Nutzer. Sind nicht trivial und erlauben zumindest die Erstellung von (partiellen) Persönlichkeitsprofilen
2. Aufgrund der Sensibilität von Nutzungsdaten unterliegen diese dem Fernmeldegeheimnis und damit einem besonderen rechtlichen Schutz.
3. Das Telemediengesetz enthält nur eine Übermittlungsberechtigung für Dienstanbieter, die Verpflichtung ergibt sich aus den Aufgabennormen der jeweiligen staatlichen Ermittlungsbehörden.
4. Zum Zweck der Strafverfolgung fehlen, anders als bei dem Zugriff durch die Geheimdienste oder im Hinblick auf Telekommunikationsdaten, eine bereichsspezifische Anordnungsnorm. Hier besteht (auch) aufgrund der Sensibilität der Nutzungsdaten eine Schutzlücke.