Deutsche Stiftung für Recht und Informatik

Big Brother und das Grundgesetz

Zulässigkeit und Grenzen der strafprozessualen Überwachung des Surfverhaltens

Dirk Meinicke, LL.M.
Gerst & Meinicke Rechtsanwälte

Herbstakademie 2013

Die Realität

Flächendeckende Überwachung der Telekommunikation erfolgt nicht nur durch (ausländische) Nachrichtendienste sondern zunehmend auch durch deutsche Ermittlungsbehörden im Bereich der organisierten Kriminalität.

Mittel: TKÜ gem. § 100 a StPO einschließlich „Überwachung und Aufzeichnung der Internetdaten/ des DSL-Datenstroms“

Auswirkungen für den Betroffenen: Nicht nur lediglich geringfügige Erweiterung einer TKÜ sondern eine Totalüberwachung des Surfverhaltens und damit faktisch gleichwertig zu einer „Online-Überwachung“

Technischer Hintergrund der TKÜ

TKÜ erfolgt unter Mitwirkung des TK-Anbieters gem. § 100b Abs. 3 S. 1 StPO indem der Verpflichtete eine vollständige Kopie der digitalisierten Telekommunikationssignale an die Ermittlungsbehörden ausleitet oder etwaig erforderliche Schaltungen ermöglicht, zu den Einzelheiten vgl. § 110 TKG i. V. m. der TKÜV.

Folge im Bereich der Internetdaten: Es wird der vollständige Datenstrom weitergeleitet, der über den jeweiligen Anschluss abgewickelt wird, d.h. sämtliche IP-basierten Anwendungen des Anschlussnutzers!

De facto erhalten die Ermittlungsbehörden damit Zugriff auf alle Internetaktivitäten des Anschlussinhabers und die TKÜ wird zu einer umfassenden Überwachung des gesamten Surfverhaltens!

Telekommunikation i.S.v. § 100 a StPO?

überwiegende Ansicht im strafprozessualen Schrifttum: jegliche Form der Nachrichtenübermittlung unter Raumüberwindung, unabhängig davon, um welche Art der Übermittlung es sich handelt. Danach eine Subsumtion sämtlicher Internetdaten unter den Telekommunikationsbegriff insofern denkbar, als jede Aktivität im Internet auf einer Kommunikation zwischen Rechnern bzw. Rechnernetzwerken basiert

Bedenken:

Vorschrift zielt offensichtlich auf die Kommunikation zwischen zwei menschlicher Teilnehmern ab, nicht auf die zwischen zwei Rechnern.

Wenn überhaupt allenfalls Kommunikation über E-Mail oder die VoIP-Telefonie (die sog. Quellen-TKÜ) als Telekommunikation zu qualifizieren (rechtliche Zulässigkeit und Rechtsgrundlage str.)

Beachte: In beiden Fällen geht es zumindest insoweit um Kommunikation, als die Inhalte des Datenstroms vom jeweiligen Nutzer intentional darauf gerichtet sind, an einen anderen Kommunikationspartner zu gelangen. Dieses Merkmal fehlt aber mindestens hinsichtlich eines Teils des Datenstroms, wenn kurzerhand sämtliche Internetdaten aufgezeichnet werden.

Kritik

Einordnung als Telekommunikation i. S .v. § 100a StPO, weil hier Rechner bzw. Rechnernetzwerke miteinander „kommunizieren“ widerspricht dem Regelungsgehalt der Norm. § 100a StPO ist originär für die Überwachung der Kommunikation zwischen zwei Individuen konzipiert.

-anders wenn mindestens hinsichtlich eines Teils des Datenstroms sämtliche Internetdaten aufgezeichnet werden, weil dann zwangsläufig auch eine Vielzahl von Daten erfasst, die nichts mit einem Kommunikationsvorgang zwischen zwei Menschen zu tun haben.

-Verständnis des Ersten Senat des BVerfG vom verfassungsrechtlichen Telekommunikationsbegriffs: die „unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs“ , vgl. BVerfG NJW 2008, 822 (825)

Folge: Bereits aus der methodengerechten einfachrechtlichen Auslegung des § 100a StPO folgt, dass diese Vorschrift keine Ermächtigung für eine Aufzeichnung sämtlicher Internetdaten eines Anschlussnutzers bereithält.

Internetüberwachung und „IT-Grundrecht“

IT-Grundrecht als entscheidende Hindernis für eine Überwachung sämtlicher Internetdaten unter Rückgriff auf § 100a StPO?!

Schutzbereich betroffen, wenn sämtliche Internetdaten eines Nutzers laufend überwacht werden.

Punkt erreicht, an dem der Staat „Einblick in Teile der Lebensgestaltung einer Person“ gewinnt oder sogar „ein aussagekräftiges Bild der Persönlichkeit“ erhält.

Faktisch handelt es sich um eine weitreichende Online-Überwachung, die nicht allein an Art.10 GG gemessen werden kann.

Das Verhältnis zu anderen Grundrechten

Besonderheit der grundrechtstypischen Gefährdungslage im Zusammenhang mit informationstechnischen Systemen: durch große Streubreite an verfügbaren Daten und die Möglichkeit der Verknüpfung bedürfen auch solche Daten des Grundrechtsschutzes, die an und für sich nicht der Privatsphäre zuzuordnen seien.

Folge: Recht auf informationelle Selbstbestimmung nicht ausreichend zur Bereitstellung des erforderlichen Schutzes, weil es lediglich dem Schutz des Grundrechtsinhabers im Hinblick auf die Erhebung, Verwendung bzw. Verbreitung personenbezogener Daten dient.

BVerfG: „IT-Grundrecht“ im Verhältnis zu anderen GR´n dadurch gekennzeichnet, dass es den Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnologie auch dann schützt, wenn nicht einzelne Kommunikationsvorgänge oder gespeicherte Daten betroffen sind.

Abgrenzung zu Art 10 GG

IT-GR allein maßgeblich und relevant, weil § 100a StPO – als einzige in Betracht kommende Ermächtigungsgrundlage für die Überwachung von Internetdaten – ausschließlich Eingriffe in dieses Grundrecht legitimieren kann.

BverfG: Schutz von Art. 10 GG greift dann nicht, „wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht“, und zwar unabhängig davon, ob „zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird“, BVerfG NJW 2008, 822, 825.

Aufzeichnung aller Internetdaten ist praktisch nahezu identisch mit Überwachung der Nutzung des Systems als solche und beinhaltet insoweit genau diejenige grundrechtsspezifische Gefährdungslage die den Ausgangspunkt für die Entwicklung des IT-Grundrechts bildete.

Eingriffe und Schranken

heimlicher Zugriff auf IT-Systeme grundsätzlich möglich bedürfen aber aber in einem Rechtsstaat stets in besonderem Maße einer Begründung.

BVerfG: „...ein heimlicher Zugriff auf ein informationstechnisches System […] der handelnden staatlichen Stelle den Zugang zu einem Datenbestand [eröffnet], der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei Weitem übertreffen kann“, BVerfG NJW 2008, 822, 829.

Ein Eingriff von besonderer Schwere liegt vor, wenn „eine heimliche technische Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht“, vgl. BVerfG NJW 2008, 822, 830.

Eingriffe und Schranken

Die Eingriffsintensität ändert sich bei materieller Betrachtung nicht dadurch, dass der Zugriff nicht durch eine „technische Infiltration“ erfolgt. Die aufgezeichneten Daten haben eine vergleichbare Aussagekraft; die Maßnahme ermöglicht die vollständige und laufende Überwachung der gesamten Internetnutzung des betroffenen Anschlussinhabers.

Die vom BVerfG geforderte Schutzintensität kann nicht dadurch umgangen werden, dass der Zugriff nicht auf dem System selbst, sondern über den von diesem ausgehenden Datenstrom erfolgt.

Durch die längerfristigen Überwachung der Internetnutzung besteht erhöhtes Risiko der Bildung von Verhaltens- und Kommunikationsprofilen und damit ein die Eingriffsintensität erhöhender Faktor, vgl. BVerfG NJW 2008, 822, 830.

Ergebnis

Die Überwachung eines DSL- oder eines Mobilfunkanschlusses ist der Sache nach eine laufende Online-Überwachung des gesamten Nutzerverhaltens im Internet.

Als eingriffsintensive Maßnahme ist sie nicht allein am Maßstab von Art. 10 Abs. 1 GG zu messen, da sie über die bloße Erfassung von Telekommunikation deutlich hinausgeht.

Die Maßnahme begründet vielmehr einen (erheblichen) Eingriff in das aus Art. 2 Abs. 1 GG fließende IT-Grundrecht.

Konsequenzen und Fazit

Die Vorschriften über die Telekommunikationsüberwachung enthalten keine ausreichende bereichsspezifische gesetzgeberische Regelung hinsichtlich der laufenden Überwachung der Internetkommunikation. § 100a StPO ermächtigt ausschließlich zu Eingriffen in Art. 10 Abs. 1 GG, während bei der Aufzeichnung sämtlicher Internetdaten eines bestimmten Anschlusses jedenfalls auch in das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i. V. m. Art 1 I GG in seiner Ausprägung als sog. „IT-Grundrecht“ eingegriffen wird.

§ 100a Abs. 4 StPO ist nicht geeignet, den Schutz des Kernbereichs privater Lebensgestaltung zu gewährleisten, der angesichts der großen Streubreite und Eingriffsintensität einer Überwachung sämtlicher Internetdaten erforderlich ist.

Konsequenzen und Fazit

Die herkömmlichen Eingriffsbefugnisse der StPO sind nicht mehr ausreichend.

Gesetzgeber muss den Maßnahmekatalog durch bereichsspezifische Regelungen ergänzen, ansonsten droht eine seitens der Exekutive weiterentwickelte StPO 2.0 unter eklatantem Verstoß gegen Demokratie- und Rechtsstaatsprinzip.

Dirk Meinicke, LL.M.
Rechtsanwalt/ Fachanwalt für Strafrecht

- Gerst & Meinicke Rechtsanwälte
- Holzdamm 28-32
- 20099 Hamburg

- Tel.: 040/ 4130800
- Fax: 040/ 41308011
- Mail: meinicke@gerst-meinicke.de
- Web: www.gerst-meincike.de