12. Strafverteidiger-Frühjahrssymposium
in Karlsruhe 18./19.4.2008

Staatlicher Zugriff auf elektronische Medien

Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main

I. Die Lage

1. Das Informationszeitalter

Ungeachtet der Möglichkeiten moderner Präzisionszeitmessung, die es uns erlaubt, selbst 1000stel Bruchteile von Sekunden darstellbar zu machen, haben wir daneben das Bedürfnis, die Menschheitsgeschichte „messtechnisch“ wesentlich „grober“, nämlich allein nach ihren verbindenden und trennenden signifikanten Merkmalen zu kategorisieren, um jenseits von numerischen Datums- und Jahresangaben ganze Epochen in „Zeitalter“ einzuteilen. Gegenwärtig befinden wir uns – so wird gesagt - im Informationszeitalter. Es hat das Industriezeitalter abgelöst. Das Informationszeitalter ist geprägt von Errungenschaften der Kommunikations- und Informationstechnologie – allen voran das Internet - die unseren privaten und beruflichen Alltag beherrschen und für nahezu alle Menschen unentbehrlich geworden sind. Geprägt wird diese Zeitepoche aber auch von der atemberaubenden Geschwindigkeit, in der wir dem Zustand immer näher kommen, dass jedes menschliche Wissen zu jeder Zeit an jedem Ort augenblicklich für alle Nutzer der immer leistungsfähiger und schneller werdenden IT-Systeme verfügbar ist. Dadurch besteht sehr viel früher als während der beinahe 200 Jahre des vergangenen Industriezeitalters Veranlassung, sich schon jetzt, nach knapp drei Jahrzehnten Gedanken darüber zu machen, welches die nächste Epoche sein wird, in die das Informationszeitalter dereinst einmünden wird. Denn so, wie die Maschinen und Verkehrsmittel des Industriezeitalters in der Vergangenheit das Leben der Menschen und ihr Zusammenleben verändert haben, so werden auch die Computer, das Internet und das Zusammenwachsen von individueller Informationsverarbeitung, Informationsaustausch und öffentlicher Informationsdienste, aber auch die rechtlichen Vorgaben über das Schicksal von Infor-

mations- und Datenmüll entscheidend dafür sein, unter welchen Bedingungen sich in Zukunft menschliche Individualität überhaupt noch entwickeln und behaupten kann. Das nächste Zeitalter wird die Konsequenz dessen sein, was wir jetzt und in naher Zukunft mit der Informationstechnologie anfangen, was wir ihr, uns gegenseitig und insbesondere auch dem Staat erlauben, wo immer er behauptet, das Informationsverhalten der Bürgerinnen und Bürger kennen und beeinflussen zu müssen, um aus den unterschiedlichsten Anlässen und Gründen die Einhaltung der Rechtsordnung durchzusetzen.

2. Ubiquitäre Technologie – ubiquitäre Information – ubiquitäre Datenerfassung

Daran muss sich die Frage anschließen, ob angesichts der Dynamik, in der sich die ubiquitär verfügbaren IT-Systeme entwickeln, sich auch die rechtsstaatlichen Garantien und Grundrechte der Individuen noch werden behaupten können, sobald theoretisch und immer mehr auch praktisch jeder über jeden *alles* erfahren kann. Und damit sind nicht nur diejenigen Informationen gemeint, die der Eine beispielsweise bei Eingabe des Namens des Anderen in die Suchmaschine Google über die betreffende Person abrufen kann.

Die technologischen Entwicklungen, von denen hier die Rede ist, sind mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden, die das Verhalten, die Lebensgewohnheiten und Vorlieben ihrer Nutzer vielfältig jedem, der Zugang zu seinen Festplatten hat, verraten. Bei den Vorgängen, bei denen solche aufschlussreichen Datensätze entstehen, muss man unterscheiden:

- Es gibt personenbezogene Daten, von denen derjenige, der sie als Spur der Nutzung von Informationstechnik hinterlassen hat, deshalb nichts weiß, weil er sie - im Gegensatz zu seinem Computer – schlicht vergessen hat, oder auch, weil er sie - z.B. eine latente Erbkrankheit - nie erfahren hat, aber hätte erfahren können, weil er selbst die ohne weiteres mögliche Verknüpfung von einzelnen an verschiedenen Stellen gespeicherten Daten nicht vorgenommen hat.

- Dann gibt es unzählige Speicher- und automatische Protokollierungsvorgänge, von denen der Nutzer überhaupt nichts mitbekommt. Zum einen, weil der Staat sie heimlich z.B. durch Onlinezugriffe auf unsere bei den Kreditinstituten ge-

speicherten Bank- und Finanzdaten vornimmt[1], oder aber auch, weil sie aufgrund der bestehenden Gesetze und Verordnungen zur Ermöglichung der Telekommunikationsüberwachung gesammelt und vorrätig gehalten werden[2]. Das sind beispielsweise bei Telefonverbindungen: die Rufnummer und Anrufzeit; bei Handys: die IMEI-Nummer[3] sowie die Funkzellen, in denen von wann bis wann unsere mobilen Geräte aktiv geschaltet waren; bei Computern: die IP-Adresse und der Verbindungsaufbau mit dem Internet; bei e-Mails: der Absender, Empfänger sowie der Zeitpunkt jeden Zugriffs auf das Postfach; die Fax- und SMS-Nachrichten, und bei letzteren auch der jeweilige Standort durch Speicherung der Mobilfunkzelle.

- Und schließlich sind es auch unsere eigenen elektronischen Geräte, die die Spuren ihrer Verwendung online oder auch offline vollkommen automatisch und unbemerkt anlegen. Davon wissen die wenigsten Leute etwas, und wenn sie es denn erfahren, sind diese Datensätze für sie, als nicht IT-Spezalisten unerreichbar. Sie sind nämlich auf der Festplatte an für den User unzugänglichen Stellen abgelegt. Neben den Betriebssystemen und Programmen des eigenen Computers und den privaten Firmennetzwerken speichern auf diese Weise z.B. auch die Suchmaschinen wie Google von Anbeginn ihrer Existenz und unaufhörlich jede unserer Suchanfragen, die Suchbegriffe, Themen und die von uns besuchten Seiten. Und derzeit wirbt dieser Suchmaschinen-Anbieter auch noch völlig unverblümt damit, dass er mit "Google Web History"[4] sein Dienstleistungs-Angebot im Internet dadurch erweitert hat, dass er unsere sämtlichen „Webaktivitäten“ online inklusive sämtlicher Suchanfragen einschließlich der Webseiten, Bilder, Videos oder Nachrichten, auf die ein User bisher geklickt hat, selbständig „verwaltet“. Daneben werden unsere getätigten Einkäufe im Teleshoping werden erfasst, und schließlich zeichnet der Internetprovider die IP-Adressen und unsere

---

1 Vgl. Gesetz zur Förderung der Steuerehrlichkeit vom 23.12.2003, BGBl. S. 2928, in Kraft seit 1.4.2005.

2 Telekommunikationsüberwachungsgesetz, BGBl. 2007, S. 3198 ff.

3 = International Mobile Equipment Identity. Es handelt sich um eine 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät (Mobilstation) eindeutig identifiziert werden kann.

4 https://www.google.com/accounts/ServiceLogin?hl=de&continue=http://www.google.com/psearch&nui=1&service=hist. Hier wird u.a. mit folgendem geworben: „Welche Websites rufen Sie häufig auf? Wie viele Suchen haben Sie zwischen 10:00 Uhr und 14:00 Uhr durchgeführt? Webprotokoll gibt Auskunft hierüber und enthält weitere Informationen zu interessanten Trends Ihrer Webaktivität.“

gesamten WEB-Aktivitäten auf. Es wird alles erfasst und gespeichert, und wir können nichts dagegen tun.

Auch die Europäische Union, das sei in diesem Zusammenhang angemerkt, schaut nicht nur zu. Sie plant, in einem Rahmenbeschluss die Verwendung von Fluggastdatensätzen zu Strafverfolgungszwecken zu regeln.[5] Nicht weniger als 19 verschiedene Daten[6] sollen bei jeder Flugreise in oder aus der EU über alle Fluggäste gespeichert werden. Bei Kindern als Fluggäste sind es noch 6 Daten mehr. Sie könnten ja später und damit länger noch als wie „Alte" eine „Gefahr" darstellen. Aufbewahrt werden können sollen die Daten 13 Jahre lang.

Die Datenspuren, die jedes E-Mail, jeder Telefonanruf, jeder Klick im Internet, jeder mit aktiviertem Navigationssystem gefahrene Kilometer, jeder Einkauf mit Kreditkarte oder mit den neuen elektronisch selbst lesenden Ladenkassen hinterlässt, sind, sobald sie nicht mehr benötigt werden (und das ist schon gleich nach dem betreffenden bewussten Vorgang) sozusagen die informationellen Abfallhalden. Wir *könnten* sie automatisch löschen oder sie allein den Technikern überlassen, z.B. zur Weiterentwicklung der Programme oder Fehleroptimierung. Aber das machen wir nicht, und wir vergessen dabei gerne, dass wir auf diese Weise einen immer größer werdenden Schürfgrund für staatliche und private Interessen bereithalten.

Werden diese „Datenschätze" mit it-kriminalistischen Mitteln „gehoben", können sie Rückschlüsse auf die Gewohnheiten und Vorlieben nicht nur des Users, sondern auch seines familiären und gesellschaftlichen wie beruflichen Umfeldes ermöglichen. Wer solche Datensätze auch noch miteinander verknüpft, erfährt Dinge über den Benutzer einer informationstechnischen Anlage, die dieser bisher über sich selbst noch nicht gewusst hat. Das klingt überraschend für uns, für manchen vielleicht sogar befremdlich – es ist aber wirklich so.

---

5 Gesetzesentwurf der EU-Kommission vom 22.10.2007, COM (2007) 654.

6 Darunter die Sitzplatznummer, den Sachbearbeiter des vermittelnden Reisebüros, die Namen derjenigen, die Minderjährige am Flughafen abholen, etc.

Das zeigt der folgende Fall aus der Praxis:

Im Zuge der kürzlich gestarteten Großfahndung mit angeblich 12.000 Beschuldigten, die (besser: deren IP-Adressen) schon ein- oder mehrmals im Internet Seiten besucht haben sollen, die kinderpornographische Abbildungen beinhalten („Aktion Himmel"), haben die Landeskriminalämter bei den Beschuldigten gewöhnliche richterlich nach § 102 StPO angeordnete Hausdurchsuchungen durchgeführt, die auch die vorgefundenen PC´s und Laptops mit umfassten. Dabei stieß man bei der Auswertung der Festplatten der Computer mitunter auch dort, wo man *keine* kinderpornografischen Bilder oder Filme fand, in der Tiefe der dem gewöhnlichen Nutzer nicht mehr zugänglichen Datenwurzelwerke auf so genannte „Thumbnails". Diese Dateien sind – wie schon der Name es ausdrückt - Daumennagel große Miniaturbilddateien, die bei dem Computerprogramm Windows Vista auch dann zurückbleiben, wenn die ursprünglich einmal gespeichert gewesenen oder auch nur angeschauten oder auch nicht angeschauten Originalbilder gelöscht wurden. Das Computerprogramm hat dabei ausschließlich die Bequemlichkeit seiner Nutzer „im Sinn". Es will vorbereitet sein, wenn diese zu einem späteren Zeitpunkt erneut auf eines der Bilder zugreifen möchten. Dann will das Programm den Vorgang möglichst schnell durchführen können. [7]

In einem dieser Ermittlungsverfahren der „Aktion Himmel" wird derzeit untersucht, ob die Einlassung des Beschuldigten richtig sein kann, dass sich solche Thumbnails auch dann im PC einnisten können, wenn z.B. beim versehentlichen Klicken auf eine gar nicht gesuchte WEB-Seite dort die Vorschaubilder zu sehen sind. Wohlgemerkt, ohne dass die Seite oder die eigentlichen („großen") pornographischen Fotos auch wirklich aufgerufen wurden.

Derartige Miniaturbilddateien – ggf. eben auch mit strafrechtlich relevantem Inhalt - können im Übrigen auch „problemlos" bei der Übermittlung völlig harmloser Bilder oder Texte mittels eines USB-Sticks einer anderen Person auf die Festplatte des eigenen Laptop transportiert werden. Mit den unverdächtigen Urlaubsfotos, die man austauscht, überträgt man also auf dieses Weise, ob man nun will oder nicht, automatisch die näm-

[7] Zum Thema der Rekonstruktion gelöschter Daten allgemein, Alexandra Harrison, Rise of the machines: The growing importance of computer forensics in criminal cases, Journal of European Criminal Law, 2008, 39 ff./47 f.

lichen Miniaturbilddateien allein durch den Aufruf des Dateiverzeichnisses auf die für den Nutzer unerreichbaren und unsichtbaren Teile der Festplatte.

Da es sich bei dem Beschuldigten, von dem hier die Rede ist, um einen bisher unbescholtenen Bürger handelt, der glaubwürdig versichert, die „Daumennagelbilder“ erstmals in seiner Strafakte gesehen zu haben, geht die Staatsanwaltschaft diesen Fragen im Sinne ihrer Verpflichtung, auch das Entlastende zu ermitteln, derzeit erfreulich bereitwillig nach. Uns jedenfalls ist als Verteidiger jenes Beschuldigten an diesem Beispiel erstmals bewusst geworden, dass unsere Computer mehr mitbekommen, sich vor allem mehr von uns merken, als wir wahrhaben, und uns selbst merken wollen oder können - und sich vor allem auch etwas „merken“, was gar nicht wir, sondern unser Computer „getan“ hat.

Das bedeutet aber auch, dass wir in unserem eigenen unmittelbaren informationellen Umfeld unser Handeln und unsere Interessen sehr viel weitergehend, als es in der Zeit der analogen Dokumentation in handgeschriebenen Briefen, Tagebüchern oder Notizblocks der Fall war, in „fremde Hände“ legen. Was heute in den Festplatten und Servern über uns hängen bleibt, selbst wenn wir die ursprünglichen Inhalte angewidert gleich wieder gelöscht oder gar nicht angesehen haben, ist nicht mehr von uns selbst beherrschbar.

II. Die Entscheidungen des Bundesverfassungsgerichts

1. Volkszählungsurteil

Deshalb hilft hier auch das schon fast etwas angestaubte Grundrecht auf „informationelle Selbstbestimmung“ aus dem Volkszählungsurteil nicht mehr weiter. Mit dem Volkszählungsurteil von 1983[8] nahm das Bundesverfassungsgericht unter den damaligen Bedingungen der Datenverarbeitung die Individuen gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten in Schutz mit diesem damals neuen Grundrecht. In dieses Recht darf seitdem nur auf der Grundlage einer klaren gesetzliche Ermächtigung mit einer eindeutigen Verwendungsregelung eingegriffen werden.

[8] BVerfGE 65, 1 ff.

Dieses Urteil war maßgeblich an der Entwicklung des Datenschutzes beteiligt mit dessen drei Hauptzielrichtungen: Datensparsamkeit und Datenvermeidung, Erforderlichkeit der Speicherung und eine enge Zweckbindung. Hieraus resultieren im Ergebnis - nach beinahe jahrzehntelangem Zögern des Gesetzgebers - auch die Vorschriften des 8. Buches der StPO über die Verarbeitung von personenbezogenen Informationen im Strafverfahren bzw. deren Löschung. Dass dessen ungeachtet die in den §§ 483 ff. StPO enthaltenen „Dateiregelungen“ in der Praxis wenig präsent sind, konnte ich kürzlich daran erkennen, dass es erst durch die Anrufung des OLG Frankfurt am Main[9] gelungen ist, ein nachweislich aufgrund eines Irrtums eingeleitetes – und mit dieser Begründung dann auch eingestelltes - Ermittlungsverfahren in der zur Archivierung geführten „Vorgangsverwaltung“ nach § 485 StPO unkenntlich zu machen.

2. Urteil zur Online-Durchsuchung

Die EDV hat sich in den vergangenen Jahren anders entwickelt, als dies in der Zeit des Volkszählungsurteils befürchtet wurde, nämlich statt zu den zentralen staatlichen Großcomputern in Richtung auf individuell genutzte dezentrale, aber global vernetzte IT-Anlagen und Kleinst-Einheiten wie Blackbarrys und Laptops. Es ist deshalb nur folgerichtig und erfreulich, dass das Bundesverfassungsgericht mit seinem am 27.02.2008 verkündeten Urteil[10] zur heimlichen Online-Durchsuchung[11] entschied, dass dafür ein wiederum neu definiertes Grundrecht zu gelten hat. Die Nutzung informationstechnischer System bei den heutigen Gegebenheiten ist nun einmal nicht mehr allein mit der informationellen Selbstbestimmung (Art. 2 GG) und auch nicht mehr mit dem Schutz der Wohnung (Art. 13 GG) und dem Schutz des Fernmeldegeheimnis (Art 10 GG) gegen unbefugte Eingriffe abzusichern. Die automatische Speicherung von Protokolldaten über die Nutzung von Suchmaschinen im Laptop auf einer Parkbank im Schlossgarten von Karlsruhe ist genauso wenig Telekommunikation, wie sie innerhalb einer Wohnung stattfindet, und bei Google und bei Windows Vista habe ich außer der Auswahl meines Suchbegriffs schon lange nichts mehr selbst zu bestimmen.

---

9 OLG Frankfurt am Main, 3 VAs 47-48/07. Die Entscheidung wird demnächst in der NStZ veröffentlicht.

10 1 BvR 370 und 595/07.

11 die das Verfassungsschutzgesetz von Nordrhein-Westfalen zu präventiven Zwecken vorsah.

Das Bundesverfassungsgericht hat deshalb ergänzend zu den drei bisherigen Grundrechten aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 GG) das *„Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“* abgeleitet und konkretisiert. Das hier begründete neue und im Verhältnis zur *„informationellen Selbstbestimmung“* erweiterte Grundrecht war, so die Verfassungsrichter, umso nötiger, als der Einzelne auf die Nutzung der allgegenwärtigen informationstechnischen Systeme inzwischen geradezu angewiesen ist. Infolgedessen könne durch einen staatlichen Zugriff etwa auf Personalcomputer ein unzulässiger *„Einblick in wesentliche Teile der Lebensgestaltung einer Person oder gar ein aussagekräftiges Bild der Persönlichkeit“*[12] gewonnen werden. Diesen Zugriff - und damit Einblick - dürfe sogar der Gesetzgeber den präventiv Informationen sammelnden Behörden nur erlauben, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestünden, d.h. Leib, Leben, Freiheit, Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Vor wenigen Tagen war in den Zeitungen zu lesen, dass sich das Bundesministerium des Inneren mit dem der Justiz dahin geeinigt habe, wie unter diesen Voraussetzungen eine Online-Durchsuchung im Rahmen der neuen operativen Befugnisse des BKA auszugestalten sei. Genaueres ist noch nicht bekannt, jedenfalls aber, so heißt es, dürfe die entsprechende Wohnung vorher – d.h. zu Zwecken der Installierung eines zur Live-Daten- und Kommunikationsabfrage nötigen technischen Spähprogramms – nicht betreten werden. Das bedeutet, dass ein sogenannter „Bundestrojaner“ online eingesetzt wird.

Wie beim Trojanische Pferd in der griechischen Sage verbergen Computer-Trojaner ihre eigentlichen aggressiven Aufgaben hinter einer tückischen Tarnung.[13] Entweder sollen die Programme, die aus den Rechnern heraus laufend und vom Eigentümer und Nutzer unbemerkt Festplatteninhalte nach Wiesbaden ins BKA senden, als Anhänge scheinbar harmloser E-Mails, oder aber in herunter geladenen Dateien verborgen, eingenistet werden. Die betreffende Zielperson erhält dann z.B. eine E-Mail, in deren Anhang sich für

---

12 Rn. 203.

13 Näheres zu den technischen Voraussetzungen und Wirkweise, s. Bettina Sokol, FS Rainer Hamm, 2008, S. 719 ff., 721.

sie „unsichtbar“ ein „Spähprogramm“ befindet. Öffnet sie den Anhang, aktiviert sie damit immer den digitalen Spion.

Verfügt der auf diese Weise angegriffene PC über Schutzprogramme gegen die vielen Spam- oder Malware-Angreifer, muss das BKA auch irgendwie dafür sorgen, dass die Wirksamkeit dieser Firewalls oder Viren-Protect-Programme durch sogenannte „Backdoors“ herabgesetzt wird. Das sind gewissermaßen „Hintertüren“, die das Computersystem gegenüber dem Internet für Eingriffe öffnet, und durch die weitere Schadprogramme nachgeladen werden. Die Behörden können sich dann direkt im PC der betreffenden Person „umschauen“, so wie wir, wenn wir unseren PC eingeschaltet haben. Dass durch diese Backdoors dann nur amtliche Trojaner mit richterlicher Genehmigung eindringen könnten und nicht auch private Bösewichte, ist bisher eine Hoffnung und ein Versprechen, über das z.B. die Freaks vom CCC (Chaos Computer-Club) nur mitleidig lächeln.

Aber damit überhaupt dem Bundestrojaner der Zugang ermöglicht wird, müssen wohl künftig die „Backdoors“ in den Selbstschutzprogrammen eines jeden Computersystems „serienmäßig“ angelegt sein. D.h., wenn sich die harmlosen Bürger einen Computer oder ihren Virenschutz anschaffen, kaufen sie das „kleine Hintertürchen“ automatisch mit. Das ist so, als müssten wir für jedes ausgelieferte Sicherheitsschloss für unsere Haustüren serienmäßig einen Zweitschlüssel für den Staat hinterlegen, und zwar an einem Ort, der auch für Einbrecher zugänglich ist.

Die Frage, ob nicht schon hierdurch, d.h. durch die die Online-Durchsuchung überhaupt erst möglich machenden Vorbereitungshandlungen, flächendeckend und unmittelbar in die Integrität *unser aller* IT-Systeme eingegriffen wird, darf gestellt werden.

3. Urteil zur automatisierten Erfassung von Kfz-Kennzeichen

Mit einem weiteren Urteil vom 11.03.2008 erklärte das Bundesverfassungsgericht die anlasslose und flächendeckende automatisierte Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleichen des Fahndungsbestands mit dem Grundrecht auf „*informationelle Selbstbestimmung*“ (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als unvereinbar.[14] Dabei maß es der Heimlichkeit der Erfassung ein besonderes, die persönliche Freiheit einschränkendes Gewicht bei. Der Bürger würde „eingeschüchtert“ und in der Ausübung

[14] 1 BvR 2074/05 und 1 BvR 1254/07: wenn der Abgleich nicht unverzüglich erfolgt und die Kennzeichen ohne weitere Auswertung sofort und spuren los wie in den „Nicht-Treffer-Fällen“ gelöscht wird.

anderer Grundrechte beeinträchtigt, wenn er nicht erkennt, *„wer was wann und bei welcher Gelegenheit über ihn weiß“*.

4. Urteil zur Vorratsdatenspeicherung

Schließlich hat das Bundesverfassungsgericht durch seine einstweilige Anordnung vom 11. März 2008[15] gezeigt, dass es auch die verfassungsrechtlichen Einwände gegen die kürzlich vom Bundesgesetzgeber bedenkenlos beschlossene[16] Pflicht zur Massenspeicherung von Telefon- und Internetverbindungsdaten auf Vorrat für eine eventuelle spätere Strafverfolgung ernst nimmt. Bis zur Entscheidung in der Hauptsache soll es, so die Verfassungsrichter, zwar vorerst bei der Speicherung und u.U. mehrjährigen Aufbewahrung bleiben. Jedoch ist die Verwendung der Daten zur Strafverfolgung bis zur endgültigen Entscheidung über die Verfassungsbeschwerden deutlich – auf eine schwere Straftat nach § 100a Abs. 2 StPO, die auch im Einzelfall schwer wiegen muss - beschränkt.

III. Konsequenzen aus der Rechtsprechung des Bundesverfassungsgerichts für die Praxis der Strafverfahren

Es stellt sich die Frage, welche Konsequenzen aus diesen Entscheidungen des Bundesverfassungsgerichts, die als solche nicht unmittelbar die Strafverfolgung betreffen, für die Praxis der Strafverfahren bei Durchsuchungen, Beschlagname und Überwachung von IT-Systemen zu ziehen sind.

Um hierauf eine Antwort gegeben zu können, muss man zunächst differenzieren zwischen den Inhalten der in einen Computer eingegebenen oder mit seiner Hilfe vorgenommenen Telekommunikation einerseits und den dabei anfallenden Nutzer- oder Zusatzdaten andererseits.[17]

1. Inhalts- und Kommunikationsdaten

Die Inhaltsdaten sind vor allem Text-Dokumente, Tabellen, Bilder, Töne (z.B. Musik aber auch digitale Diktate und Mitschnitte von Gesprächen oder Konferenzen), Filmsequenzen oder Live-Gespräche. Unter all diesen Inhaltsdaten ist noch einmal die Unter-

---

15 1 BvR 256/08.

16 Die Möglichkeit der Vorratsdatenspeicherung ist im neu geregelten Telekommunikationsgesetz vom 21. Dezember 2007 geregelt, das am 01. Januar 2008 in Kraft trat.

17 Vgl. zur Differenzierung ziwschen den einzelnen Speichermedien, Bettina Sokol in FS Rainer Hamm, 2008, S. 719 ff., 724 ff.

scheidung zu treffen zwischen gleichsam unilateral genutzten Inhaltsdaten und Kommunikationsinhalten. Die nur für meine eigenen Zwecke – also unilateral - via Tastatur, Fotoapparat oder Mikrofon in meinen PC eingegebenen Inhalte sollen schon ihrer Zweckbestimmung nach nur mich selbst etwas angehen.

Die Telekommunikationsinhalte, das sind die über Internettelefonie (Voice-over-IP oder – meist im Ausland ansässige - Anbieter wie Skype) geführten Ferngespräche und die per E-Mail, Quickmessage oder SMS versandten und empfangenen Mitteilungen – auch wieder unabhängig davon, ob es sich um Textdateien, DSS-Sprachdateien, Pdf- oder JPEG-Bilddarstellungen handelt.

Bei dieser Einteilung nach der IT-System-Nutzung ist allerdings zu beachten, dass der Übergang von den unilateral genutzten Inhaltsdaten und der Telekommunikation nicht trennscharf zu ziehen. Sie ist aber für die rechtlichen Voraussetzungen eines staatlichen Eingriffs z.B. nach § 100a StPO (Überwachung der Telekommunikation) von großer Bedeutung. Es stellt sich insoweit nämlich die Frage, von welchem Augenblick an aus einer unilateralen Inhaltsdatei (also z.B. einem in den PC eingegebenen Text) Telekommunikation wird. Ist dies etwa schon dann der Fall, wenn ich einen Text im Word-Format oder auch bereits im Outlook-Format entwerfe, den ich dann im PC speichere, um erst später zu entscheiden, ob ich ihn einem bestimmten Adressaten als Mail schicke? Oder schützt unabhängig von einer später erst noch umzusetzenden Zweckbestimmung (z.B. als E-Mail) das neue IT-Grundrecht in einem jeden Fall den Nutzer vor staatlichen Eingriffen, solange sich die E-Mail noch auf seinem Rechner befindet?

Und wie stellt man sich dann die Unterscheidung zwischen solchen Quellen-Telekommunikationsdaten von den übrigen auf der Festplatte vorhandenen Dateien vor? Hier liegt auch mein Einwand gegen die These, wonach für die Quellen-Telekommunikationsüberwachung – also der Überwachung im ureigenen System des Nutzers - § 100a StPO als Rechtsgrundlage ausreichen soll, weil in einem solchen Fall in die Integrität des informationstechnischen Systems nicht eingegriffen werde.[18] Wie soll man es technisch schaffen, so frage ich, auf die Inhalte (!) der Quellen-Telekommunikationsdaten zuzugreifen, ohne die Integrität des Gesamtsystems zu tangieren?

---

[18] So OStA Dr. Hornick in seinem Referat auf dem Frühjahrssymposium 2008 in Karlsruhe, in diesem Heft, S. ...

Und schließlich: Wie sieht es beim Telekommunikations-Empfänger aus? Liegt eine Telekommunikation vor, sobald er die an ihn adressierte E-Mail gelesen hat, sie aber auf seinem PC im Outlook oder Outlook-Archiv oder sogar weit weg auf dem Server des Providers gespeichert lässt?

Mit der letzteren Frage wird sich das Bundesverfassungsgericht noch in einer gesonderten Entscheidung befassen, nachdem es bereits am 2.3.2006 im Falle der Heidelberger Richterin für die Auswertung von SMS-Inhalten entschieden hat[19], dass die Grenze zwischen Telekommunikation und Privatsphäre da verläuft, wo ein Handynutzer seine SMS bereits empfangen hat. Wenn er sie nicht löscht, sondern sie in seiner (privaten) Sphäre gespeichert lässt, ist diese Information nicht mehr von dem durch Art. 10 GG geschützten Fernmeldegeheimnisses umfasst. (Aber muss man nicht auch hier fragen: was heißt „löschen"? Was ist, wenn ich die SMS lösche, aber sie ist in „meinem Wurzeldatenspeicher" nach wie vor vorhanden?)

2. Nutzerdaten

Die reinen Nutzerdaten demgegenüber („Datenmüll"), die nicht Inhaltsdaten sind und die ebenfalls, sowohl anlässlich der Telekommunikationsvorhänge, als auch während der Stand-alone-Nutzung von gar nicht mit dem Internet verbundenen PCs entstehen, sind wegen ihrer Aussagekraft zur Person des Users uneingeschränkt ebenfalls von dem neuen Grundrecht geschützt.

3. Folgerungen

Daraus folgt:

1. Auch wenn sich die Entscheidung zur Online-Durchsuchung durch den Verfassungsschutz nur auf heimliche Fernrecherchen bezieht, kann das neue Grundrecht auch bei offenen Durchsuchungen und Beschlagnahmen von informationstechnischen Systemen (Computern, Notebooks, Handys) und bei der Anwendung des § 110 StPO nicht außer Betracht bleiben. Auch diese Maßnahmen haben dem besonderen Schutzzweck des Grundrechts *„auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"* Rechnung zu tragen. Die vorhandenen gesetzlichen Ermächtigungen reichen nicht aus, um den

[19] NJW 2006, 976

Anforderungen der Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung gerecht zu werden, weil sie nur auf die herkömmlichen Grundrechte zugeschnitten sind und die besonderen Gefahren für das Persönlichkeitsrecht, die durch Auswertung der vom PC-Nutzer überhaupt nicht beherrschbaren Spuren seiner Lebensäußerungen und Verhaltensweisen ausgehen, ignorieren.

2. Die uneingeschränkte Durchsicht oder Beschlagnahme ganzer Dateisysteme (z.B. Festplatte des PC) stoßen jedenfalls dort auf verfassungsrechtliche Grenzen, wo hierdurch ein Einblick in den Kernbereich der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglicht wird.

3. Das gleiche gilt, wenn der sichergestellte oder beschlagnahmte Datenbestand eine automatische Be- oder Verarbeitung der erhobenen Daten erlaubt, sofern diese wiederum den grundgesetzlich geschützten Privatbereich tangiert, indem sie z.B. die Erstellung eines Persönlichkeitsprofils ermöglicht. Auch der Beschuldigte – und nicht nur derjenige, der präventiv ausgespäht wird - hat einen Anspruch auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Und er hat auch einen Anspruch darauf, nicht dadurch eingeschüchtert zu werden, dass er nicht (mehr) erkennt, wer, was, wann und bei welcher Gelegenheit etwas über ihn weiß oder erfahren hat.

IV. Trügerische Datenspuren

Bisher war im Wesentlichen vom Grundrecht auf *Vertraulichkeit* der Nutzung von IT-Systemen die Rede. Zum Schluss noch einige Worte zu der von dem neuen Grundrecht auch erfassten *Integrität* der IT-Systeme. Damit sind nämlich u.a. die möglichen Fehlerquellen und Verfälschungsgefahren *infolge* der Erhebung von IT-„Beweisen“ angesprochen.

Bei allem bisher Gesagten bin ich noch davon ausgegangen, dass die von den Strafverfolgungsbehörden aus den IT-Systemen erhobenen Informationen – soweit diese denn gesetzlich und verfassungskonform legitimiert werden sollten – wenigstens *geeignet* zur Wahrheitsermittlung seien. Aber die Warner aus den informationstechnischen Fachgebieten haben bereits dem Bundesverfassungsgericht erklärt, wie groß - über die rechtlichen Einwände hinaus - die Gefahr ist, dass gerade auch *infolge* der Eingriffe in die Festplatten, Server und Programme zum Zwecke der Infiltration und des Auslesens

Veränderungen bewirkt werden, die zu einem Verlust an Authentizität führen können. Zwar hat das Bundesverfassungsgericht zu Recht dazu bemerkt, dass unter den engen Voraussetzungen, unter denen die Maßnahme der (präventiven) heimlichen Online-durchsuchung nur verfassungsgemäß sein kann, die Verfälschungsgefahr kein prinzipieller Einwand gegen diese Methode der Verhütung schwerster Gefahren für wichtige Rechtsgüter sein darf. Aber das heißt doch nur, dass die Fehlerquellen hingenommen werden dürfen, wo immer das Irrtumsrisiko nur darin besteht, dass die Gefahrenlage eben nicht bestanden hat und auch nichts zu verhüten war.

Geht es dagegen um Strafverfolgung, sollte es sich von vornherein verbieten, Beweise zu erheben, bei denen nicht gesichert ist, dass sie am Ende unverfälscht beim Strafgericht ankommen.[20] Und es sollte auch nicht vergessen werden, dass z.B. aus einer auf einer Festplatte vorhandenen Datei oder der Identifizierung einer IP-Adresse eines PC´s, ebenso wie aus einer für ein bestimmtes Handy gespeicherten Funkzelle immer nur der Schluss zu ziehen ist, dass das betreffende *Gerät* die Datei erstellt hat oder sich auf einer Website „eingeloggt" hat, oder zum Telefonieren benutzt wurde. Von welcher Person, ist damit ebenso wenig festgestellt wie ausgeschlossen werden kann, dass durch den Online-Zugriff selbst die Datenlage im ausgespähten Rechner zum Nachteil des Beschuldigten verändert wurde.

5. Abschließende Betrachtungen

Wir sollten uns beim Umgang mit den elektronischen Medien bewusst sein, dass die Verlockungen einer unbegrenzten Nutzung aller technischen Möglichkeiten zwar groß, aber die Gefahren auch nicht gering zu schätzen sind. Obwohl das Informationszeitalter erst „in den Kinderschuhen" - oder sollte man besser sagen: schon „in den Flegeljahren" - steckt, existieren bereits gigantische Datenmengen über uns alle, die wir nicht (mehr) zu überblicken in der Lage sind, geschweige denn zu steuern und zu beherrschen. Und es werden stündlich mehr. Das „Internet vergisst" nicht, und mit ihm viele jemals mit ihm verbunden gewesene Rechner auch nicht. Wenn uns nicht ein kontrollierter Umgang mit dem „Netz" gelingt, und dazu gehört auch und ganz elementar die Besinnung des Staates auf individuelle Freiheitsrechte seiner

[20] Auf den Unterschied im Beweiswert bei präventiven Maßnahmen im Vergleich zu den höheren Anforderungen in einem Strafverfahren weist das Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung (Fn. 10) ausdrücklich hin, vgl. Rn. 223 des Urteils; instruktiv zu den Fehlerquellen auch: Alexandra Harrison, Rise of the machines: The growing importance of computer forensics in criminal cases, Journal of European Criminal Law, 2008, 39 ff.

Bürgerinnen und Bürger, dann schreiten wir geradewegs in die nächste Epoche, die dann aber als das „Gläserne-“ oder das „Überwachungs-Zeitalter“ in die Geschichte eingehen wird. Das können wir nicht wollen. Es muss so auch nicht sein. Wir haben es in der Hand.