erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

**Dagmar Boedicker**

# Leerstelle in der legislativen Praxis

## Plädoyer für eine Überwachungsgesamtrechnung

*Über den Daumen gepeilt sind es 50 bis 80 Gesetze, die es den unterschiedlichsten Sicherheitsbehörden auf mehreren Ebenen gestatten, mich zu überwachen. Nicht nur mich, Sie natürlich auch. Schätzen Sie mal, was alles über Sie gespeichert wird, wenn Sie mit der Bahn von Bremen nach Frankfurt fahren, um dort in ein Flugzeug zu steigen, das Sie nach Rom bringt. Falls Sie aus der EU ausreisen und wieder heimkommen möchten, werden es noch ein paar Dateien und Sicherheitsbehörden mehr. Wie lange wird das eigentlich alles gespeichert? Wer bekommt da was von wem? Kontrolliert jemand, wann es gelöscht wird?*

Vielleicht erwarten Leserinnen und Leser der *FIfF-Kommunikation* gar keine Antwort auf diese Fragen mehr. Ich glaube, das ist ein Fehler! Es ist das eine, realistisch zu sein, und es ist das andere hinzunehmen, dass unsere Grundrechte verfassungswidrig laufend verletzt werden. Menschenwürde setzt nämlich voraus, dass die staatliche Ordnung sich aus unserem Leben weitgehend heraushält, dass es Bereiche gibt, wo Sicherheitsinteressen weniger wichtig sind als unsere Würde.

### Spuren einer Reise

Ich will versuchen, eine Geschäftsreise nach Rom zu beschreiben, die Sie jederzeit unternehmen könnten. Bei dieser Reise verhalten Sie sich ausnahmslos legal. Sie geben keinerlei Anlass für staatliche Eingriffe zur Gefahrenabwehr oder Strafverfolgung:

Die Bremer Straßenbahnen errechnen den für Sie günstigsten Tarif anhand der Route und stellen ihn auf Ihrer Monatskarte in Rechnung. Am Bahnhof übt die Bahn ihr Hausrecht aus und filmt Sie auf Ihrem Weg. Die Bahnfahrkarte haben Sie online gekauft, sie wird von Ihrem Konto abgebucht. Im Zug sitzen Sie an einem Vierertisch und in einer Funkzelle[1] mit einem dunkelhäutigen Herrn. Einem mutmaßlichen Gefährder, wovon Sie natürlich keine Ahnung haben. Während der Fahrt nutzen Sie WIFIonICE für Ihr Pad und einen anderen Telekommunikations-Anbieter für Ihr Smartphone, beide Anbieter speichern mindestens MAC- und IP-Adresse, wahrscheinlicher sind es 29 Verbindungsinformationen pro Verbindung. In Deutschland speichern Telekommunikations-Dienstleister u. a. sämtliche Verkehrsdaten für zehn Wochen. „Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen.“[2]

*Lek, Lawrence (2017): Geomancer. Ausstellung Open Codes. The World as a Field of Data. 2018 im ZKM Karlsruhe*

In Frankfurt werden Sie wieder am Bahnhof gefilmt. Mit dem Ticket haben Sie der Fluglinie allerhand Information geliefert, die diese teilweise gemäß Fluggastdatengesetz[3] für die PNR-Datei übermittelt[4]. Sie speichert aber noch weitere Daten, wozu sie gesetzlich gar nicht verpflichtet ist. Auch am Flughafen Frankfurt werden Sie gefilmt. In der Confiserie kreuzt sich Ihr Weg mit dem einer gerade angekommenen polnischen Staatsbürgerin, Sie stehen beide an derselben Kasse und wechseln einige Worte. Vor dem Geschäft verabschieden Sie sich höflich. Was Sie natürlich nicht wissen können: Die junge Frau hat sich polnischem Recht entzogen, denn sie hat abgetrieben und darauf stehen in Polen drei Jahre Haft.[5] Am Flughafen in Rom werden Sie gefilmt, in der Autovermietung ebenfalls, die Bilder werden aufgezeichnet. Ihr Hotel in Rom hat Ihre Reservierungsdaten an die zentrale Datenbank der Kette geliefert, zu der es gehört. Leider sind die bei einem Hack in falsche Hände geraten.[6] Der WLAN-Anbieter im Hotel speichert natürlich Ihre MAC-Adresse, was sonst noch gespeichert wird, entnehmen Sie bitte den AGBs. Als Sie am nächsten Tag mit Ihrem Mietwagen nach Bologna fahren, passieren Sie auf der Autobahn mehrere Mautstellen, Video-überwacht. Sie treffen sich mit einer Geschäftspartnerin aus Island in einem Restaurant und geraten bei der Rückfahrt auf einer Landstraße in eine Verkehrskontrolle. Die Polizei registriert die Daten von Ihnen und Ihrer Begleiterin. Mit nationalem italienischen Recht kenne ich mich nicht aus, aber EU-Recht gilt auch dort. Und im Schengen-Informations-System SIS sind jedenfalls jetzt alle Ihre Grenzübertritte und die Daten der Verkehrskontrolle vermerkt. Dabei haben Sie noch Glück. Wären Sie keine EU-Bürgerin, stünden Ihnen die Segnungen des Etias bevor:

> *„Das Reiseinformations- und -genehmigungssystem Etias dient der Vorkontrolle visafreier Besucher. Betroffene müssen laut Beschluss des EU-Rats über einen Online-Antrag den Behörden Auskünfte zu Identität, Reisedokument, Aufenthaltsort, Kontaktmöglichkeiten, infektiösen Krankheiten und Ausbildung übermitteln. Die Daten werden dann automatisch mit verschiedenen IT-Systemen im Sicherheitsbereich abgeglichen und fünf Jahre auf Vorrat gespeichert.“*[7]

Die Rückreise muss ich wohl nicht mehr beschreiben. Aber ich möchte einige Sicherheitsbehörden aufzählen, die gesetzlich befugt sind, im Verdachtsfall auf die gespeicherten Daten zuzugreifen: Polizei, Landeskriminalamt und Verfassungsschutz in Bremen, Niedersachsen und Hessen, Bundespolizei, Bundeskriminalamt, Zoll, Bundesamt für Verfassungsschutz, Bundes-Netzagentur, Bundesnachrichtendienst (obwohl der eigentlich nur außerhalb Deutschlands ermitteln dürfte), MAD. Zu den italienischen Sicherheitsbehörden kann ich nichts sagen, aber für Deutschland allein sind es 16 während dieser kurzen Reise. Bei jedem Bundesland, das Sie betreten, kommen drei hinzu. Europol ist dabei und von den ausländischen Nachrichtendiensten wie CIA, FSB, MIT, NSA schreibe ich hier nichts, weil es mir um etwas anderes geht.

Die Befugnisse der Sicherheitsbehörden beschränken sich nicht darauf, anderswo gespeicherte Daten abzufragen. Sie dürfen selbst Daten erheben, auch mit *besonderen Mitteln.* Besondere Mittel der Datenerhebung sind beispielsweise längerfristige Observation, der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen, zur Feststellung des Standortes oder der Bewegungen einer Person oder zum Abhören oder zur Aufzeichnung des nichtöffentlich gesprochenen Wortes, verdeckte Ermittler, automatisierte Kennzeichenerkennungssysteme. Diverse Datenerhebungen dürfen durchgeführt werden, selbst wenn Dritte unvermeidbar betroffen werden, beispielsweise Bild- und Tonaufzeichnungen von Drohnen aus.[8]

Telekommunikations-Dienstleister müssen in Deutschland Verkehrsdaten 10 Wochen speichern. Auch darauf dürfen die Behörden zugreifen. Dritte sind betroffen. Wenn die neue Beweismittel-Übergabe-Verordnung (E-Evidence-Verordnung[9]) Wirklichkeit wird, müssen die TK-Anbieter alles herausrücken, was sie über bestimmte Kunden wissen, wenn die Strafverfolgungs-Institutionen eines EU-Mitglieds das fordern. Im Regelfall haben die Anbieter dafür zehn Tage Zeit, in Eilfällen nur sechs Stunden.

> *„Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor.“*[10]

Die deutsche Konferenz der Datenschutzaufsichtsbehörden fordert, den Vorschlag für eine E-Evidence-Verordnung zu stoppen, und ist sich dabei mit dem Europäischen Datenschutzausschuss (früher Artikel-29-Gruppe) einig, der nicht einmal eine Rechtsgrundlage für die Verordnung sieht.[11]

## Unsichtbare Mauern

Europäische Reisefreiheit fühlt sich frei an, keineswegs wie ein Bentham‘sches Panoptikum, in dem Wächter uns beobachten, die wir nicht sehen können. Anders als die Insassen des Panoptikums stoßen wir nie an Mauern, jedenfalls dann nicht, wenn wir westeuropäisch aussehen, uns unauffällig verhalten und keinen Anlass zu Kontrollen geben. Trotzdem werden wir auf Schritt und Tritt überwacht und haben keine Ahnung, wann die virtuellen zu konkreten Mauern versteinern könnten.

> *„Es steht zu befürchten, dass die weltweite Zunahme der Mauern einen neuen Mauermenschen erzeugt: Dieser Mensch begrüßt die neuen Mauern als Wellenbrecher, mit denen die Stürme der Globalisierung, die Migrationswellen, islamistische Terroristen und kriminelle Banden gestoppt werden. […] Mauern verwandeln Furcht in Zutrauen, Unsicherheit in Sicherheit, Orientierungslosigkeit in Orientierung, Identitätsnot in Identitätsgewissheit. […] Schließlich produzieren die neuen Mauern nicht nur ein Außen, sondern eben auch ein Innen, sie formen das Bild der Ausgesperrten ebenso wie das Selbstbild der Eingesperrten. Sind wir schon eingesperrt?“* [12]

Verdeckte Maßnahmen, bei denen harmlose Menschen wie Sie und ich gern zum *Beifang* werden, haben einen besonderen Pferdefuß. Wir wissen nicht, dass unsere Daten erhoben und gespeichert wurden, dass wir zu den *Dritten* gehören, bei denen das *aus technischen Gründen unvermeidbar ist.* Damit kommen wir gar nicht auf die Idee, Auskunftsrechte in Anspruch zu nehmen,

Löschfristen einzufordern, ganz allgemein den Datenschutzkonformen Umgang mit unseren personenbezogenen Daten zu kontrollieren. Fast alle Gesetze, die zu verdeckter Überwachung ermächtigen, verpflichten die Sicherheitsbehörden deshalb dazu, die Betroffenen zu benachrichtigen. Bisher habe ich allerdings noch niemanden getroffen, die oder der jemals eine solche Benachrichtigung erhalten hätte. Sie vielleicht? Angesichts des Rundum-sorglos-Pakets an polizeilichen und nachrichtendienstlichen Befugnissen stimmt da etwas nicht.

## Rechtsstaat?

Die Befugnisse der Polizeien wurden seit dem 11. September 2001 kontinuierlich ausgebaut, beginnend mit dem Sicherheits-Paket des damaligen Innenministers Otto Schily, spöttisch als *Otto-Katalog* bezeichnet. Dasselbe gilt für die Nachrichtendienste. Regierungen und Parlamente haben Polizeigesetze, Gesetze für die Verfassungsschutz-Ämter, den Zoll usw. gewaltig erweitert und in ganz Deutschland eine Überwachungs-Infrastruktur auf- und ausgebaut, die uns Menschen das Vornehmste verweigert: unsere Würde. Das Gefühl des Überwachtwerdens wächst stetig.

Häufig hat das BVerfG an Polizei- und anderen Gesetzen fehlende Normenklarheit bemängelt. In einem Rechtsstaat sollte es selbstverständlich sein, dass die Staatsdiener ihre Grenzen sehr genau kennen und einhalten. Für die Betroffenen ist es wichtig zu wissen, was sie dürfen und was ihre Obrigkeit darf. Ich bezweifele stark, dass wir oder die Sicherheitsbehörden darüber tatsächlich Bescheid wissen. Niemand, weder Sicherheitsbehörden noch Betroffene, kann sich mehr auskennen, wenn Gesetze zur Definition von Gefahren von einem Gesetz auf ein zweites und von dort auf ein drittes verweisen[13]. Wenn dazu mangelhafte Zweckbindung der personenbezogenen Daten bei ausgedehnten Eingriffsvoraussetzungen kommt, tappen wir im Dunkeln: Darf uns die Polizei bei einer Demonstration fotografieren oder filmen? Was darf sie mit den Bildern und Videos tun? Bleiben wir bei Protesten gegen die *Münchner Sicherheitskonferenz* besser weg? Filmt mich die Drohne? Mit oder ohne Ton? Wann haben Sicherheitsbehörden meinen Standort bei welcher Gelegenheit mit einer Funkzellenabfrage ermittelt? Sind die Verkehrsdaten gespeichert? Wo und wie lange? Haben sie mich bei einer präventiven Rasterfahndung mit im Netz gehabt? Wohin wurde die Information übermittelt? Sollten wir Auskunft verlangen? Bekommen wir die, oder machen wir uns nur erst recht verdächtig? Wurde unser Kennzeichen an einer innereuropäischen Grenze oder auf einer deutschen Autobahn automatisch erkannt? Gespeichert? Genutzt für was? Datenbanken gibt es in jedem Bundesland, jedem europäischen Mitgliedstaat, in Drittstaaten, in denen wir die Speicherung unserer personenbezogenen Daten befürchten müssen.[14]

Bei der Quellen-TKÜ oder Online-Durchsuchung werden massenhaft höchst persönliche Daten ausgeleitet. Gehören wir zu den unbeteiligten Dritten und wurden wir jemals darüber informiert? Haben die verdeckten Maßnahmen jemals zu einem Ergebnis geführt? Hat eine Sicherheitsbehörde eine Gefahr damit abgewehrt oder eine Person einer schweren Straftat überführt? Diesen Nachweis bleiben uns Exekutive und Legislative bisher schuldig. Außerdem zeigt sich, dass Beschäftigte des BKA eine eigenwillige Definition davon haben können, was zum Kernbereich privater Lebensgestaltung gehört, oder nach ihrer Auffassung eben nicht.[15]

Spätestens 2010 hätte etwas geschehen müssen. Es hatte mehrere Verfassungsbeschwerden gegen die Vorratsdatenspeicherung gegeben und in ihrer Entscheidung aus dem Jahr 2010 haben die Richterinnen und Richter dem Gesetzgeber eine Überwachungsgesamtrechnung[16] auferlegt. Sie haben klargestellt, dass neue Überwachungsmaßnahmen und Eingriffe in das Grundrecht auf informationelle Selbstbestimmung immer im Kontext bereits bestehender Instrumente geprüft werden müssen. Im Dezember 2016 hat es auch der Europäische Gerichtshof (EuGH) auf Grundlage der europäischen Grundrechte-Charta untersagt, Telekommunikationsanbieter ganz allgemein zur Speicherung persönlicher Nutzerdaten zu verpflichten.[17] Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) schützt geschäftliche wie private Kommunikation und der Europäische Gerichtshof für Menschenrechte (EGMR) verlangt Mindestsicherungen bei der Informationssammlung und -speicherung durch einen Geheimdienst.[18] Wenn nämlich „Daten aus Kommunikationsverläufen behördlich aufgezeichnet und verwertet werden", entsteht

> *„ein Klima, in dem die Menschen sich bei der Äußerung der eigenen Meinung ebenso wie beim Konsum von Informationen zur Bildung einer eigenen Meinung selbst bei völlig legalen Inhalten immer häufiger selbst beschränken, um mögliche nachteilige Folgen zu vermeiden. Diese Selbstbeschränkung bei der Ausübung der durch Artikel 10 EMRK garantierten Meinungs- und Informationsfreiheit wird auch als „chilling effect" bezeichnet."*[19]

## Unsere Forderungen

Mit dem BVerfG sind wir überzeugt, dass „die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“[20]. 2006 hat es in seinem Urteil zur Rasterfahndung[21] eine Abwägung verlangt zwischen der Eingriffsschwere, den verfolgten Schutzzielen und der gesellschaftlichen Relevanz dieser Maßnahme wegen ihrer Streubreite und der möglichen Einschüchterung ganzer Bevölkerungsgruppen. Wenn die Instrumente zur Kontrolle vorhanden sind, können sie gegen uns verwendet werden, das haben Gestapo, SD und Stasi gezeigt.

- Deshalb fordern wir eine Überwachungsgesamtrechnung: Wir fordern den Nachweis des Gesetzgebers, dass weitere Überwachungsbefugnisse erforderlich sind, und dass sie dem Verfassungsgerichts-Urteil entsprechen! Der Nachweis kann durch unabhängige Forschungseinrichtungen oder die zuständigen Datenschutzbeauftragten erbracht werden, die mit den dafür erforderlichen Ressourcen auszustatten sind.

- Wir fordern, dass Überwachungsmaßnahmen gestrichen werden, wenn sich ihre Notwendigkeit und Verhältnismäßigkeit nicht belegen lässt!

- Wir fordern eine Evaluierung der großen staatlichen Datensammlungen, ob sie durch anlassbezogenere Datenverarbeitung ersetzt werden müssen!

- Wir fordern eine unabhängige Instanz, die prüft, ob die Sicherheitsbehörden bei ihren Überwachungsmaßnahmen verhältnismäßig und damit verfassungsgemäß vorgehen!

- Wir fordern den Nachweis der Sicherheitsbehörden, dass sie alle Betroffenen tatsächlich über alle Überwachungsmaßnahmen aufgeklärt haben! Der Nachweis kann durch die zuständigen Datenschutzbeauftragten erbracht werden, die mit den dafür erforderlichen Ressourcen auszustatten sind.

Diese Forderungen richten wir an die Gesetzgeber auf Landes-, Bundes- und europäischer Ebene. Es ist ihre verfassungsrechtliche Pflicht sie zu erfüllen!

## Anmerkungen

1 *https://media.ccc.de/v/35c3-9972-funkzellenabfrage_die_alltagliche_rasterfahndung_unserer_handydaten (Stand Januar 2019)*

2 *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7. November 2018 zur E-Evidence-Verordnung, S. 2*

3 *Gesetz zur Umsetzung der Richtlinie (EU) 2016/681*

4 *Die Daten (Anschlussflüge, Flugscheindaten, Zahlungsinformationen, Vielfliegereinträge, Gepäckangaben, Informationen über Mitreisende etc.) aus den nationalen PNR-Dateien werden im Advance Passenger Information System (APIS) zusammengeführt. „Der Europäische Datenschutzbeauftragte geht von mehr als 300 Millionen betroffenen nicht-verdächtigen Fluggästen aus, die von der PNR-RL betroffen sind, European Data Protection Supervisor, Opinion 15/2015, 7.“ Tschohl, Christoph et al: HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze, Version 1.2. S. 94. https://epicenter.works/document/706 (Stand Oktober 2018)*

5 *Nach der Europäischen Herausgabeverordnung (E-Evidence, siehe Endnote 9) kann Polen die über diese Dame gespeicherten Daten von italienischen Dienstleistungs-Anbietern fordern, unabhängig davon, ob eine Abtreibung in Italien strafbar ist. Kriterium ist die Freiheitsstrafe von drei Jahren.*

6 *Die Marriot-Kette musste zugeben, dass ihr im November 2018 ca. 500 Millionen Kundendaten inkl. Geburtsdatum, Kreditkartennummer usw. gestohlen wurden. Die Täter hatten sich Zugang zur Reservierungsdatenbank der Marriot-Tochterfirma Starwood verschafft und offenbar schon seit 2014 Zugriff auf das System. http://www.lirobit.de/sicherheitsvorfaelle-hackerangriffe-chronologischer-ueberblick/ (Stand 28. Januar 2019)*

7 *Krempl S (2018) Big Brother Europa. EU plant biometrische Superdatenbank. https://www.heise.de/select/ct/2018/18/1535696151919730; Krempl S (2018) ESTA für Europa: EU-Vorkontrolle visafreier Reisender soll 2021 starten. https://www.heise.de/newsticker/meldung/ESTA-fuer-Europa-EU-Vorkontrolle-visafreier-Reisender-soll-2021-starten-4156695.html (Stand 28. Januarv2019)*

8 *Die hier genannten Befugnisse stammen aus dem Bayerischen Polizeiaufgaben-Gesetz, Art. 33 und 47, sie finden sich auch in anderen Polizeigesetzen.*

9 *Die Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final) sieht vor, dass die Strafverfolgungsbehörden der EU-Mitgliedstaaten die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten. Das Recht des Staates, in dem die Daten gespeichert sind, soll von den Anbietern der Dienstleistungen grob geprüft werden, nicht etwa von staatlichen Rechtsinstanzen. Die Verordnung kann nur noch im Trilog gestoppt werden.*

10 *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Münster, 7. November 2018*

11 *Europäischer Datenschutzausschuss: Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters. https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de (Stand 30.1.19)*

12 *Körner T (2019) Von Mauern und Menschen. Deutschlandfunk, 13. Januar 2019, 9.30 Uhr*

13 *Unterrichtung durch die Bundesregierung. Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes. https://dip21.bundestag.de/dip21/btd/18/130/1813031.pdf, S. 33 (Stand 28. Januar 2019)*

14 *Seit 2006 gibt es beispielsweise das Gemeinsame-Dateien-Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder.*

15 *Unterrichtung durch die Bundesregierung. Evaluationsbericht zu den §§ 4a, 20j, 20k des Bundeskriminalamtgesetzes. dip21.bundestag.de/dip21/btd/18/130/1813031.pdf, S. 45 (Stand 28. Januar 2019)*

16 *Rossnagel A (2010) in: Neue Juristische Wochenschrift 18/2010, Seite 1238*

17 *Rechtssachen C-203/15 und C-698/15*

18 *Tschohl C et al (2018) HEAT – Handbuch zur Evaluation der Anti-Terror-Gesetze, Version 1.2. S. 134f. https://epicenter.works/document/706. (Stand Oktober 2018)*

19 *Tschohl C et al (2018) a.a.O. S. 136*

20 *BVerfG, Urteil vom 2.3.2010, NJW 81 (2010), 833, 839*

21 *BVerfG, B. v. 04.04.2006, 1 BvR 518/02*