



Ludwig Boltzmann Institut für Menschenrechte (BIM)
Ludwig Boltzmann Institute of Human Rights

ao. Univ.Prof. Dr. Hannes Tretter, Universität Wien

„Der digital bewegte Mensch“

Vortrag auf der 38. Europäischen Präsidentenkonferenz
Wiener Advokatengespräche
„Vom Rechtsstaat zum Überwachungsstaat?“
Freitag, 12. Februar 2010, Wien, Palais Ferstel

1. Einleitung

Wie oft hören wir nicht das den Datenschutz verharmlosende Argument „Meine Daten kann doch jedermann haben, denn ich habe nichts zu verbergen !“. Es wird nicht nur von Leuten vorgebracht, die sich mit der Thematik nicht oder kaum auseinandersetzen, sondern auch von Menschen, die sich beruflich mit IT-Technologie, Politik oder Grund- und Menschenrechten befassen oder sich für diese engagieren. Manche haben sogar die Vision einer Welt, in der alle von allen alles wissen können und niemand am anderen etwas auszusetzen hat oder anderen Schaden zufügen will, jeder Mensch also authentisch leben und sich „outen“ kann, ohne fürchten zu müssen, dass das Wissen um sein/ihr Ich, Persönlichkeit, Leben, Gedanken und Eigenschaften ihm oder ihr zu irgendeinem Nachteil gereicht, soweit dabei nicht gegen die allgemein gültigen und akzeptierten Gesetze verstoßen wird. Wir müssten nur darum kämpfen, dass unsere Welt so gesehen besser wird – ein Erziehungsprojekt á la Rousseaus „Emile“, fürwahr.

Ich denke, dass wir in diesem Kreis keine gedanklichen Experimente vollziehen müssen, um zu verdeutlichen, welches Wissen um Sie in Form personenbezogener Daten alleine im Laufe eines normalen Arbeits- oder auch Urlaubstages verarbeitet und gespeichert wird:

Sei es

- im Supermarkt und bei sonstigen Einkäufen, denn Sie bezahlen mit Bankomat-, Kredit- und/oder Kundenkarte;
- beim online-Shopping, denn amazon, ebay & Co wollen Ihr Kaufverhalten für ihre Marketing- und Werbestrategien nutzen;

- bei Ihrem nächsten Bankbesuch, denn Sie haben einige Überweisungen vorzunehmen, u.a. ins Ausland, und eröffnen auch ein Wertpapierdepot;
- bei der Abgabe Ihrer nächsten Steuererklärung;
- bei der Benutzung Ihres Autos, denn Sie haben ein GPS-gesteuertes Sicherheits- und Versicherungssystem oder Sie unterliegen einem Road-pricing;
- beim Abschluss einer Kranken- oder Lebensversicherung oder Pensionsvorsorge, denn Sie geben ehrlich Auskunft über Ihre Krankheiten, Lebens- und Einkommensverhältnisse;
- bei der Nutzung öffentlicher Verkehrsmittel und von Hotels im In- und Ausland, denn Sie haben online gebucht;
- bei Ihrer Arbeit, denn Ihr Arbeitgeber hat mit dem Betriebsrat eine Vereinbarung über die Überwachung der Arbeitnehmer und Arbeitnehmerinnen abgeschlossen;
- bei der RAK und dem Disziplinarrat, denn ein Klient hat sich über Sie beschwert;
- beim Besuch eines Arztes oder Krankenhauses, denn Sie haben eine e-card;
- vielleicht wird in Zukunft sogar bei Geburt eines Menschen dessen DNA erhoben, die Aufschluss über seine Lebenserwartung, seine Anfälligkeit für Krankheiten und seine Leistungsfähigkeit gibt, was für den Abschluss von entsprechenden Versicherungen oder von Arbeitsverhältnissen usw. sicherlich äußerst interessant ist;
- beim Telefonieren und Versenden von e-mails, denn Ihr Provider verzeichnet alle Ihre Verbindungs- und Standortdaten, auch Echelon hat Sie erfasst, weil Sie bei einem Handy-Telefonat die Worte „Islam“, „Koran“ und „Terror“ erwähnten;
- beim Surfen im Internet, denn google & Co wollen beim nächsten Mal die von Ihnen bevorzugten Seiten schon aufbereiten und Ihnen ein ganz persönliches Suchprofil bieten;
- beim Chatten, denn ein Chat-Partner einer Selbsthilfegruppe hat Ihren Dialog online zugänglich gemacht, in dem Sie schwere Vorwürfe gegen bestimmte Personen erheben und eine staatliche Institution stark kritisieren;
- bei You tube, denn irgendjemand, den Sie nicht einmal kennen hat einen Videoclip von Ihrem letzten Urlaubsaufenthalt online gestellt;
- beim Besuch von Orten und Portalen mit Zugangsvoraussetzungen, weil Sie sich registrieren oder identifizieren lassen mussten;
- beim Bloggen, Twittern und bei der Nutzung Ihres Facebook-Account, denn Sie wollen viele Freunde haben oder sich umfassend informieren;
- beim Betreten des öffentlichen Raums, denn Überwachungskameras beobachten und IN-DECT-Polizeidrohnen verfolgen Sie.

Sei es,

- dass staatliche Behörden Interesse an Ihnen und Ihren Daten haben, zB vorgeblich ganz „harmlos“ über Ihren Bildungsweg, oder weil Sie nichtsahnend mit einer Person kommuniziert haben, die im Verdacht strafbarer Handlungen steht, ohne dass Sie jemals etwas darüber erfahren werden;
- vorsorglich werden aber auch auf der Grundlage der Vorratsdatenspeicherungs-Richtlinie der EU alle Ihre Verbindungs- und Standortdaten ohne jeglichen Verdacht für eine bestimmte Zeit gespeichert, denn es könnte ja sein, dass Sie Übles im Schilde führen.
- Auch kann es passieren, dass Behörden Interesse an bestimmten Ihrer personenbezogenen Daten haben, um bestimmte (rechts)politische Ziele verfolgen zu können, zB um den geplanten Nacktscanner auf Flughäfen nur bei denjenigen Personen zum Einsatz zu bringen,

die im Zuge eines „ethnic profiling“ identifiziert wurden, weil bei ihnen eine höhere potentielle Terrorismusgefahr angenommen wird als bei anderen.

- Oder es werden aufgrund bestimmter personenbezogener Daten Personengruppen identifiziert, denen – ohne konkreten Tatverdacht – mehr als anderen zugetraut wird, dass sie terroristische Akte setzen oder organisierte Kriminalität begehen könnten.
- Wenn einmal jemand auf diese Weise identifiziert wurde, erhöht sich damit die Wahrscheinlichkeit, dass weitere Überwachungsmaßnahmen wie etwa Abhörmaßnahmen im privaten Bereich oder online-Durchsuchungen erfolgen.
- Und selbst wenn Sie in einem strafrechtlichen Verfahren freigesprochen wurden, werden die diesbezüglichen Daten zeitlebens aufbewahrt, denn Sie sind ja nun einmal unter Verdacht gestanden, der sich vielleicht irgendwann wieder erhärten oder wiederholen könnte.

Die Reihe ließe sich beinahe beliebig fortsetzen. Die Existenz von Daten schafft rundum Begehrlichkeiten – hier scheint sich das archaische Verhaltensmuster des Jagens und Sammelns widerzuspiegeln, nur wer genügend auf Vorrat hat, der überlebt.

Natürlich ist nicht jedes Interesse an personenbezogenen Daten abzulehnen, viele sind völlig legitim und ermöglichen dem Staat erst, seinen Aufgaben effizient nachzukommen, oder der Wirtschaft, moderne Dienstleistungen anzubieten, auf die wir auch nicht verzichten wollen und sollen. Aber stellen Sie sich vor, dass alle diese oder bestimmte Daten, die bei staatlichen Behörden und/oder privaten Unternehmen gespeichert sind, in einem Datenverbund zusammengefasst und nach speziellen Kategorien oder Fragestellungen ausgewertet werden. Zwar dürfte das nach den in Europa geltenden datenschutzrechtlichen Bestimmungen nicht oder nur unter bestimmten strengen Voraussetzungen geschehen. Das Problem ist nur, dass wir – die Öffentlichkeit bzw. die Betroffenen – von wahren Datenverwendungen sehr oft überhaupt nichts oder erst zu einem späteren Zeitpunkt, manchmal erst nach journalistischer Aufdeckungsarbeit, etwas erfahren. Die Technik der Datenverarbeitung bleibt für uns weitgehend im Verborgenen, ist oft nur einem elitären Kreis von Wissenden und Eingeweihten vorbehalten. Und die meisten Datenschutzbehörden in den europäischen Staaten sind personell und von ihren Ressourcen her zu schwach ausgestattet, um eine wirksame und vor allem auch präventive Kontrolle auszuüben. Abgesehen von einigen engagierten NGOs und Medien, die sich auch nur langsam Gehör verschaffen können, weiß und interessiert die Öffentlichkeit meistens nicht, wer was wann und zu welchem Zweck gesammelt hat, wo Daten gespeichert, zwischengelagert und versteckt oder weitergeleitet werden, bis sie wie aus dem Nichts ans Tageslicht gelangen. In der Regel ist es dann schon zu spät, ihre illegale oder missbräuchliche Verwendung zu verhindern.

Ich komme zum Ausgangspunkt zurück: Es ist eine Illusion zu glauben, das Wissen um uns, um unsere Persönlichkeit nicht auch zu unserem Nachteil verwendet werden kann. Verletzungen von Grund- und Menschenrechten und missbräuchliche Verwendung von Daten wird es so vermutlich lange geben, solange die Menschheit existiert. Daher kann es nur darum gehen, Wege zu finden, die modernen technologischen Errungenschaften des Informations- und digitalen Zeitalters in einer Art und Weise zu bändigen und zu zähmen, dass wir sie ohne Verlust an elementaren Grundwerten unserer Gesellschaft – wie sie auch in Artikel 2 des neuen EU-Vertrags in der Fassung des Vertrags von Lissabon verankert sind – nämlich des Schutzes der

Grundrechte und der Wahrung der Rechtsstaatlichkeit nutzen können. Oder, mit den Worten des bekannten deutsch-griechischen Datenschutzexperten *Spiros Simitis* in einem Interview in der „Die Zeit“, „sichere Datenwege“ zu finden. Leider sieht die Realität derzeit – trotz mancher Bemühungen auf europäischer und auch auf nationalen Ebenen anders aus.

Daher möchte ich nun näher auf einige zentrale datenschutzrechtliche Herausforderungen der Gegenwart und Zukunft eingehen:

2. Vorratsdatenspeicherung

Die insbesondere von den Innenministern der EU-Mitgliedstaaten als Reaktion auf die Terroranschläge von London und Madrid forcierte und in einer Art „Schnellverfahren“ beschlossene Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die flächendeckende und verdachtsunabhängige Vorratsspeicherung von Daten verfehlt in ihren rechtspolitischen und praktischen Auswirkungen die ursprüngliche Intention der Bekämpfung des Terrorismus und der organisierten Kriminalität, da sie dazu schlechthin ungeeignet sein dürfte. Denn Terroristen und organisierter Kriminalität fällt es leicht, über Verwendung von Wertkarten- oder im (nicht EU-)Ausland angemeldeter Handys sowie außereuropäischer E-Mail-Provider der Vorratsdatenspeicherung zu entgehen. Letztlich trifft die Vorratsdatenspeicherung vorrangig „NormalverbraucherInnen“.

Nach wie vor steht daher die Frage im Raum (die zuletzt auch von der neuen Kommissarin für Justiz, Grundrechte und Bürgerschaft, *Viviane Reding*, in ihrer Anhörung vor dem Europäischen Parlament gestellt wurde), ob die Richtlinie *per se* mit den grund- und datenschutzrechtlichen Anforderungen in Einklang steht. Zu bezweifeln ist allerdings auch, ob die grundrechtlichen Konsequenzen für den Einzelnen, aber auch die Auswirkungen auf die Gesellschaft insgesamt, in einem angemessenen Verhältnis zu den Interessen stehen, die mit dem genannten Zweck verfolgt werden.

Der Grundsatz, dass gegen eine bestimmte Person ausschließlich bei Vorliegen von konkreten Verdachtsmomenten Ermittlungs- bzw. Verfolgungsmaßnahmen gesetzt werden sollen, zieht sich einem roten Faden gleich durch wohl alle europäischen Rechtsordnungen. Die flächendeckende und verdachtsunabhängige Vorratsdatenspeicherung aber stellt diesbezüglich einen Paradigmenwechsel dar, der aus grundrechtlicher Sicht nicht vertretbar ist. Denn selbst wenn das Speichern von Verkehrs- und Standortdaten auf den ersten Blick harmlos erscheinen mag, offenbart sich doch bei genauerem Hinsehen, dass die Vorratspeicherung in die Grundrechte auf Datenschutz und auf Achtung des Privatlebens nicht unwesentlich eingreift: Aufgrund der gewonnenen Verkehrs- und Standortdaten können indirekt soziale Netzwerke bis in Details ebenso nachvollzogen, wie mehr oder weniger genaue Bewegungsprofile erstellt werden. Schließlich können Verkehrsdaten auch Rückschlüsse über sensible Inhalte einer Kommunikation ermöglichen (laufende Anrufe bei der AIDS-Hilfe, regelmäßiger Email-Verkehr mit einer politischen Partei). Zu bedenken ist auch (und dies ist für Rechtsanwälte von besonderem Interesse), dass im Fall einer konkreten Datenanwendung durch Strafverfolgungsbehörden nicht nur in die Rechtssphäre eines möglichen Straftäters oder dessen Komplizen eingegriffen wird, sondern auch in die Rechtssphäre derjenigen Personen, die mit den Adressaten

der Maßnahme über Telekommunikationseinrichtungen nur zufällig oder eben beruflich in Verbindung standen oder stehen.

Das Vorhandensein solcher Daten weckt aber auch Begehrlichkeiten, diese für andere Zwecke als zur Bekämpfung „schwerer Straftaten“ (wie dies die Richtlinie vorsieht) zu nutzen: etwa zur Verfolgung von Urheberrechtskriminalität (illegale Downloads) oder in Zivilrechtsstreitigkeiten (zB Scheidungsprozessen). Wenn wir aber damit rechnen müssen, dass alle diese Daten erfasst und gespeichert und von Behörden für verschiedenste Zwecke verwendet werden können, schafft dies eine bedrückende Atmosphäre, die mit einem freiheitlich organisierten Rechtsstaat nichts mehr zu tun hat. Es wäre damit ein System geschaffen, das im Sinne der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ein System der Überwachung zum Schutz der Sicherheit des Staates und der Gesellschaft kreiert, das Demokratie und Rechtsstaatlichkeit aushöhlt und umgeht, die es vorgibt schützen zu wollen.

Nicht von ungefähr brauen sich daher am europäischen Dach für alle Sicherheitsfanatiker und Sicherheitsdienstleister staatlicher und privater Couleur dunkle Wolken zusammen, die freilich viele Fragen offen lassen, ob und wie sie sich entladen werden:

- So ist beim deutschen Bundesverfassungsgericht derzeit eine Beschwerde von ca. 35.000 Personen (!) anhängig, die sich gegen das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ wendet, in der unter anderem auch ein Verstoß der Richtlinie gegen das Recht auf informationelle Selbstbestimmung des Grundgesetzes und das Recht auf Datenschutz iSd Artikel 8 EMRK geltend gemacht wird. Der Antrag hatte vorläufig teilweise Erfolg und führte zur Erlassung einer einstweiligen Anordnung, mit der die Anwendung einiger der angefochtenen gesetzlicher Bestimmungen bis zur Entscheidung über die Verfassungsbeschwerde außer Kraft gesetzt wurden. Denkbar ist, dass das BVerfG zur Klärung dieser Frage ein Vorabentscheidungsverfahren vor dem EuGH anstrengt, in der Sache selbst entscheidet und/oder im Fall der Abweisung der Beschwerde die Angelegenheit von den nicht erfolgreichen BeschwerdeführerInnen dem EGMR vorgelegt wird.
- Kürzlich hat das rumänische Verfassungsgericht das nationale Gesetz, mit dem die Richtlinie umgesetzt wurde, wegen Verletzung der Rechte auf Datenschutz und Privatsphäre aufgehoben, was zu einem Vertragsverletzungsverfahren vor dem EuGH führen könnte, je nachdem wie der rumänische Gesetzgeber weiter verfährt.
- Und in Österreich liegt zwar seit Kurzem ein Entwurf zu einer entsprechenden Novelle des Telekommunikationsgesetzes vor, mit der die Richtlinie umgesetzt werden soll, Justiz- und Innenministerium wollen aber nicht nur den strengen grundrechtlichen Vorgaben des Entwurfs nicht oder nicht in allen Punkten folgen, sondern auf Vorrat gespeicherte Daten auch zur Verfolgung von Straftaten unterhalb der Kategorie „schwerer Straftaten“ nutzen. Da eine Einigung zwischen den Koalitionspartnern derzeit nicht in Sicht ist, zeichnet sich eine weitere „Verweigerung“ Österreichs ab, die zu einer Verurteilung Österreichs wegen Nichtumsetzung der Richtlinie führen könnte.

3. Überwachungsmaßnahmen und Datenverwendungen durch Sicherheitsbehörden und Geheimdienste für präventive Zwecke

Wesentlich aufgrund undurchsichtiger gesetzlicher Grundlagen, zweifelhafter Motive, mangelnder Kontrolle sowie fehlenden oder unzulänglichen Rechtsschutzes geraten vermehrt Überwachungsmaßnahmen und Datenverwendungen durch Sicherheitsbehörden und Geheimdienste in ein schiefes Licht:

3.1. Das SWIFT-Abkommen

Gestern hat das Europäische Parlament dem interimistischen SWIFT-Abkommen mit den USA nach heftigem politischem Tauziehen wegen unzureichendem Datenschutz seine Zustimmung verweigert. Der Finanzdienstleister SWIFT mit Sitz in Belgien managt die Transaktionen von über 8.000 Banken in mehr als 200 Ländern bei etwa 15 Millionen Transfers täglich, auf deren Daten US-Fahnder jahrelang zur Bekämpfung von Terrorfinanzierung und Geldwäsche ungehindert permanenten und pauschalen Zugriff zu Zwecken des „Data-mining“ hatten. Zwar erhielt SWIFT von den US-Behörden in der Folge auf der Grundlage eines Abkommens den „Safe Harbor“-Status, was bedeutet, dass das Unternehmen in den USA nach Maßgaben des EU-Datenschutzrechts behandelt wurde. Nach Auslaufen des Vertrags Ende Dezember hätte am 1. Februar 2010 das – nunmehr geplatze – Interimsabkommen in Kraft treten und bis 31. Oktober 2010 gültig sein sollen. Eine Sicherheitslücke besteht nach vorliegenden Informationen dennoch nicht, da die Fahnder – allerdings nur auf Einzelfälle bezogen – auf Amtshilfeabkommen zurückgreifen können. Der Abschluss eines neuen Abkommens steht nun in den Sternen, könnte aber auf Druck der USA im Laufe des Jahres zustande kommen. Die u.a. zuständige Innenkommissarin *Cecilia Malmström* hofft in einer ersten Reaktion auf ein neues Abkommen „mit ambitionierten Sicherheitsstandards für die Privatsphäre und den Datenschutz“. Kürzlich hat jedoch das deutsche Bundeskriminalamt dem Nachrichtenmagazin „Der Spiegel“ zufolge die Weitergabe von Bankdaten an die USA kritisiert. Die Ermittlungsbehörde hält den Datentransfer im Zuge des SWIFT-Abkommens bei der Bekämpfung des internationalen Terrorismus für nutzlos. In einem internen Vermerk des Bundeskriminalamts heißt es laut dem Bericht, dass die aus fachlicher Sicht zu erwartenden Erkenntnisse aus einem systematischen und umfangreichen Abgleich der SWIFT-Daten zumindest für den Bereich der Finanzierung des Terrorismus „aus hiesiger Sicht nicht den mit der Datenrecherche verbundenen erheblichen materiellen und personellen Aufwand rechtfertigen“.

3.2. Stockholmer Programm und INDECT-Projekt

Das kürzlich beschlossene Stockholmer Programm des Rats der EU „An open and secure Europe serving and protecting the citizens“ für die Jahre 2010-2015, das die Union als „Raum der Freiheit, der Sicherheit und des Rechts“ weiter stärken soll, enthält einigen datenschutzrechtlichen Sprengstoff. Zwar wird an zahlreichen Stellen des Programms auf die Bedeutung des Datenschutzes verwiesen und seine Einhaltung eingemahnt, zugleich wird jedoch bei näherer Analyse der Schwerpunkt des Programms deutlich, der auf den Bereichen innere und öffentliche Sicherheit, Management von Migration und Grenzen, der Bekämpfung der organisierten Kriminalität sowie dem Drogenhandel und der Bekämpfung des Terrorismus liegt. Zur

Umsetzung dieser Vorhaben sind eine Reihe von Datenbanken und -systemen geplant, nicht nur ein „European Information Exchange Model“ und eine „EU Information Management Strategy“, sondern auch ein „European Criminal Records Information System (ECRIS)“, ein „Police Records Index System (EPRIS)“, eine Datenbank über „Travelling Violent Offenders“ und ein Register über Drittstaatsangehörige, die in der EU verurteilt wurden. Im Rahmen der Europäischen Agentur für die operative Zusammenarbeit an den Außengrenzen (FRONTEX) soll das Grenzkontrollsystem EUROSUR geschaffen werden. Vielleicht klingt all das noch nicht so dramatisch, denn es ist ein legitimes Anliegen der Politik und sogar auch eine grundrechtliche Verpflichtung der Staaten und der EU, sich um die Sicherheit ihrer Bürger und Bürgerinnen zu sorgen und adäquate Maßnahmen zu treffen. Nur darf dies nicht um den Preis der Würde, der Freiheit, der Selbstbestimmung des Menschen, der Rechtsstaatlichkeit und einer angstfreien demokratischen Gesellschaft geschehen.

Diese fundamentalen Werte scheinen jedoch bedroht, wenn wir beispielsweise einen Blick auf das von der Europäischen Kommission finanzierte Forschungsprojekt INDECT werfen, das in einen Kontext mit den Ambitionen des Stockholmer Programms gestellt werden kann. INDECT soll Wege und die Technik (er)finden, Informationen aus dem Internet, aus Datenbanken, von Überwachungskameras und von sogar von unbemannten „Polizeidrohnen“ europaweit zu einem automatischen Bevölkerungsscanner verknüpfen. Mit dem Ziel der Erhöhung der Sicherheit sollen Menschen und Fahrzeuge überwacht, ihre Bewegung im öffentlichen Raum observiert und das www durchforstet werden. Suchmaschinen zur schnellen Ermittlung von Personen und Dokumenten und Programme, die ständig und automatisch öffentliche Quellen wie Websites, Foren, User-Gruppen, File-Server, P2P-Netzwerke und individuelle Computersysteme durchsuchen. Das Projekt soll erforschen, wie sich im Netz mit automatisierten Suchroutinen „Gewalt“, „Bedrohungen“ und „abnormales Verhalten“ finden lassen. Jüngsten Informationen zufolge ist auch ein System zur Rundumüberwachung in Städten geplant, das militärischen Kommandostrukturen zur vernetzten Kriegsführung nachgebildet ist und der Bekämpfung künftiger Aufstände im urbanen Raum dienen soll.

3.3. *Rechtsschutz*

Ein – alleine an der Rechtsprechung des EGMR gemessenes und in vielen nationalen Rechtsordnungen auftretendes – Problem stellen geheime Überwachungsmaßnahmen und Datenverwendungen ohne ausreichend wirksamen Rechtsschutz dar. Selbst das bloße Bestehen von Gesetzen, die ein System der geheimen Überwachung der Kommunikation erlauben, bringt für alle Personen, auf die sie Anwendung finden können, die Gefahr einer Überwachung mit sich. Der Gerichtshof fordert wegen des Fehlens öffentlicher Kontrolle und der dadurch verbundenen Gefahr des Machtmissbrauchs in solchen Fällen daher adäquate und effektive Rechtsschutzgarantien. Damit stellt sich die Frage, ob Formen des kommissarischen oder parlamentarischen Rechtsschutzes – wie in vielen Rechtsordnungen, auch in der österreichischen, vorgesehen – ausreichend sind. Nach der Rechtsprechung des EGMR bewirkt es eine Verletzung des Artikels 8 EMRK, wenn die Kontrolle nicht durch eine ausreichend unabhängige und qualifizierte Instanz erfolgt, die die Einhaltung des Rechtsstaatsprinzips garantiert. Zudem muss die zur geheimen Überwachung zuständige Behörde an eine unabhängige Einrich-

tung oder die Öffentlichkeit über die gesamte Verwendung des Systems oder die in Einzelfällen angewandten Maßnahmen berichten.

Schließlich verlangt der EGMR – gestützt auf das Recht auf eine wirksame Beschwerde vor einer nationalen Instanz gemäß Artikel 13 EMRK – bei geheimen Überwachungsmaßnahmen eine nachträgliche Information der betroffenen Person, sobald dies ohne Gefährdung oder nach Beendigung des Überwachungszwecks erfolgen kann, damit diese unter Einräumung eines subjektiven Beschwerderechts in einem rechtsstaatlichen Verfahren die (Grund-)Rechtmäßigkeit der Maßnahme von einer unabhängigen Instanz überprüfen lassen kann. Der Rechtsschutz muss nicht zwingend ein gerichtlicher, wohl aber ein unabhängiger und unparteiischer sein.

Dramatisch bemerkbar macht sich in vielen EU-Mitgliedstaaten das Fehlen mit einem umfassenden Mandat und ausreichenden finanziellen und personellen Mitteln ausgestatteter Datenschutzbehörden. Das derzeitige, im Wesentlichen „klassische“ Instrumentarium des Datenschutzes ist den aktuellen und künftigen Bedrohungsszenarien nicht mehr gewachsen. Neben datenhungrigen Geheimdiensten und Sicherheitsbehörden ist es auch die Wirtschaft, die zunehmend zu einer Gefahr für uns alle wird. Mehr als alle Behörden zusammen wissen vermutlich die Daten-Giganten Google, Amazon, ebay & Co. zusammen mit Banken, Finanzdienstleistern, Versicherungen, Krankenanstalten, Konsumgüterkonzernen usw. mehr über uns und unsere Vorlieben, Meinungen, Vorzüge, Schwächen, Gesundheit, Sexualität, Vermögen usw. Bescheid als uns lieb ist und sein kann. Nicht auszudenken, wenn am sich neuerdings abzeichnenden lukrativen Markt gestohlener Daten entsprechende staatliche Nachfragen ungeniert entstehen.

Unternehmen sperren sich aber auch gegen Kontrollen, beschwichtigen uns mit dem Argument, „sozial verantwortlich“ zu handeln, auch wenn der UN-Global Compact über CSR eine gute Sache ist und CSR beginnt, sich auch des Datenschutzes anzunehmen. Das aber ist nicht genug. Wir brauchen starke, personell und technisch umfassend ausgestattete unabhängige Datenschutzbehörden, die über die Ressourcen und die Kompetenz verfügen, nicht nur Datenschutzregister zu verwalten, sondern auch auf eigene Initiative mit technisch hervorragend ausgebildetem Personal zumindest stichprobenartig Kontrollen durchführen und entsprechende Sanktionen verhängen oder einleiten zu können. Derzeit führt die EU Agentur für Grundrechte mit Sitz in Wien eine rechtsvergleichende Studie über die in den EU-Mitgliedstaaten bestehenden Datenschutzsysteme im Hinblick auf deren Kompetenzen und Effizienz durch. Auf das Ergebnis dürfen wir gespannt sein.

4. Fazit

Wir sollten die Warnrufe nicht überhören. Warnrufe, die im deutschsprachigen Raum neben zahlreichen engagierten NGOs zuletzt etwa von *Wolfgang Sofsky* („Verteidigung des Privaten“), *Ilija Trojanow* und *Juli Zeh* („Angriff auf die Freiheit – Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte“) sowie *Gerhart Baum* („Rettet die Grundrechte ! – Bürgerfreiheit contra Sicherheitswahn“) trefflich formuliert wurden. Schleichend, ja klammheimlich laufen wir auf einem Paradigmenwechsel zu, der nicht nur unsere Freiheit, unsere Grund- und Menschenrechte und den Rechtsstaat unterminiert, sondern dem demokra-

tischen Gemeinwesen und seinem Selbstverständnis tiefen Schaden zufügt. Der Mensch läuft Gefahr, nicht mehr sich selbstbestimmt durch Raum und Zeit zu bewegen, sondern in vorgegebenen Bahnen und unter Beobachtung *bewegt zu werden*. In Bahnen, die von Geheimdiensten, elitären Bürokratien definiert, von manchen Medien befördert und von Sicherheitsdienstleistern und Konzernen zur Nutzung angeboten und versilbert werden. Ausbrechen kann, überspitzt formuliert, zum „Freiwild“ geworden eine Art „bürgerlichen Tod“ bedeuten.

Letztlich aber hängt es auch entscheidend von uns selbst ab, ob wir uns verführen und verblenden lassen, *wie* wir selbst mit der digitalen Welt umgehen und uns in ihr bewegen. Zweifellos findet – insbesondere in der jüngeren Generation – eine Verschiebung des Privaten hin zum Öffentlichen statt, wenn wir den unbekümmerten Umgang der Jugend mit den Kommunikationsmitteln betrachten, die das Netz bietet. Besteht hier aber etwa auch eine Chance der zivilen Gesellschaften, mit Hilfe ein- und derselben Technik deren Missbrauch zu bekämpfen ? Die (noch bestehende) Freiheit der globalen Kommunikation zu nutzen, diese und damit die eigene Freiheit zu verteidigen ?

Sehr wesentlich wird es auch darauf ankommen, ob es gelingt, mit engagierter und profunder grundrechtlicher Argumentation alle diejenigen zu unterstützen, die um ihre und solidarisch um die Freiheit der demokratischen Gesellschaft kämpfen, und vor den europäischen Höchstgerichten das Recht auf Datenschutz und Achtung der Privatsphäre, der „Privatheit“, und rechtsstaatliche Garantien durchzusetzen. Den Anwaltschaften kommt hier naturgemäß eine besondere Bedeutung zu.
