

16

79

JULI 2007

Dokumentation
der Tagung vom
26. März 2007
in Berlin

Bürgerrechtsschutz im digitalen Zeitalter

Impressum

Herausgeberin	Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin www.gruene-bundestag.de
Verantwortlich	Jerzy Montag MdB Rechtspolitischer Sprecher Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin E-Mail: Jerzy.Montag@bundestag.de
Redaktion	Franziska Vilmar, LL.M., wissenschaftliche Mitarbeiterin des rechtspolitischen Sprechers Jerzy Montag MdB
Bezug	Bündnis 90/Die Grünen Bundestagsfraktion Info-Dienst Platz der Republik 1 11011 Berlin Fax: 030 / 227 56566 E-Mail: versand@gruene-bundestag.de
Schutzgebühr	€ 1,--
Redaktionsschluss	Juni 2007

Inhalt

Fachgespräch Bürgerrechtsschutz im digitalen Zeitalter

Programm vom 26.03.2007 3

Begrüßung

Wolfgang Wieland MdB, Sprecher für Innere Sicherheit..... 5

Forum 1:

Was kommt technisch auf uns zu?

Silke Stokar MdB, Sprecherin für Innenpolitik (Moderation) 7

Chaos Computer Club 7

Prof. Dr. Andreas Pfitzmann 10

Dr. Udo Helmbrecht 15

Ulrich Walter..... 19

Fragen und Beiträge aus dem Auditorium 24

Forum 2:

Technische und rechtliche Herausforderungen der Entwicklung

Jerzy Montag MdB, rechtspolitischer Sprecher (Moderation)..... 31

Prof. Dr. Alexander Roßnagel..... 31

Jörg Ziercke 34

Hans Kudlich..... 41

Fragen und Beiträge aus dem Auditorium 47

Zusammenfassendes Schlusswort

Wolfgang Wieland MdB, Sprecher für Innere Sicherheit..... 57

Fachgespräch Bürgerrechtsschutz im digitalen Zeitalter

Programm vom 26.03.2007

12.30 Uhr Imbiss

13.00 Uhr Begrüßung
Wolfgang Wieland MdB, Sprecher für Innere Sicherheit

Forum 1:

Was kommt technisch auf uns zu?

Moderation: Silke Stokar MdB, Sprecherin für Innenpolitik

13.15 Uhr Chaos Computer Club mit einer Vorführung

13.30 Uhr Prof. Dr. Andreas Pfitzmann, Leiter der Datenschutz- und Sicherheitsgruppe an der TU Dresden:
„Qualität und Ausmaß der technischen Entwicklung“

13.45 Uhr Dr. Udo Helmbrecht, Präsident des BSI

14.00 Uhr Ulrich Walter, Direktor von L-1 Identity Solutions AG
„Neuartige polizeiliche Ermittlungsverfahren“

14.15 Uhr Fragen und Beiträge aus dem Auditorium

14.45 Uhr Pause

Forum 2:

Technische und rechtliche Herausforderungen der Entwicklung

Moderation: Jerzy Montag MdB, rechtspolitischer Sprecher

15. 00 Uhr Prof. Dr. Alexander Roßnagel, wissenschaftlicher Direktor des Instituts für europäisches Medienrecht, Saarbrücken, und des Forschungszentrums für Informationstechnik-Gestaltung, Universität Kassel

15.15 Uhr Jörg Ziercke, Präsident des Bundeskriminalamtes

15.30 Uhr Prof. Dr. Hans Kudlich, Juristische Fakultät am Lehrstuhl Strafrecht, Strafprozessrecht und Rechtsphilosophie, Universität Erlangen-Nürnberg

15.45 Uhr Fragen und Beiträge aus dem Auditorium

16.45 Uhr Zusammenfassendes Schlusswort

Wolfgang Wieland MdB, Sprecher für Innere Sicherheit

17.00 Uhr Ende der Veranstaltung

Begrüßung

Wolfgang Wieland MdB, Sprecher für Innere Sicherheit

Meine Damen und Herren, ich darf Sie hier ganz herzlich begrüßen zu unserem Fachgespräch „Bürgerrechtsschutz im digitalen Zeitalter“. Ich freue mich, dass Sie so zahlreich erschienen sind, vielen Dank auch an die Referentinnen und Referenten.

In der TAZ wurde heute gefragt, ob sich hier die größten Hacker der Republik versammeln, der Chaos Computer Club an meiner rechten Seite und Herr Ziercke an meiner linken Seite. Um das klarzustellen, wir machen heute keinen Wettbewerb, wer am cleversten beim Hacking ist.

Natürlich hat uns die Diskussion über Online-Durchsuchungen dazu bewegt, dieses Fachgespräch zu suchen. Es soll ein Fachgespräch sein und keine Podiumsdiskussion werden, wo wir uns verbal die Köpfe einschlagen.

Online-Durchsuchungen, warum? Wir hatten einen Haushaltstitel in dem Programm innere Sicherheit des Bundesministers des Inneren. Es wurde Geld gefordert und auch vom Parlament bewilligt für Ferndurchsuchungen von PCs. Was ist das eigentlich? Die Frage hat uns beschäftigt. Sie wurde jedoch weder konkret gestellt noch konkret beantwortet. Dass das etwas ganz Neues ist und dass das möglicherweise Hacking ist, wussten die Parlamentarier nicht. Die Mehrzahl hat dieses Geld bewilligt. Die Opposition hat weitestgehend, auch aus anderen Gründen, dagegen gestimmt. Nun haben wir einen Haushaltstitel, der zurzeit nicht ausgeschöpft werden kann. Davon gehe ich jetzt mal aus. Denn die rechtliche Grundlage für dieses Hacking, jedenfalls die strafprozessuale, sofern es im Rahmen der Strafverfolgung gemacht wird, besteht nicht.

Wir haben dann mehrfach nachgefragt. Uns erschien es irgendwie merkwürdig. Was wollen die da eigentlich machen? Wollen sie bei einem beschlagnahmten PC ihren Beamten die Reise dorthin ersparen und den PC aus Wiesbaden durchsuchen? So arglos und rechtsstaatlich gepolt war jedenfalls ich. Erst die nächsten Wochen und Monate ergaben dann ein klareres Bild. Es war tatsächlich geplant, mit diesem Geld soll geforscht werden, mit so genannten Trojanern in PC-Systeme einzudringen.

Als ich mich dann im Plenum empörte und sagte, die Bundesregierung kann doch nicht handeln wie ein Chaos Computer Club, beschwerte sich nicht etwa die Bundesregierung, sondern der Chaos Computer Club bei mir. So etwas machten sie nie! Sie hätten eine Ethik, wonach in private PCs nicht rein gegangen werden darf. Wer das nicht will, kann nicht Clubmitglied werden. So habe ich es verstanden.

Deswegen ist eher die Frage: Welche Ethik hat die staatliche Seite oder welche Ethik muss der Gesetzgeber hier als Fundament zugrunde legen? Aber es ist wahrlich nicht die einzige spannende Frage. Es ist für uns der Einstieg gewesen, in zwei Richtungen zu denken. Einmal: Was kommt da eigentlich alles noch auf uns zu? Was kommt gerade auf Personen wie mich zu, die eigentlich schon heilfroh sind, wenn sie eine Sms absenden, die dann auch den Empfänger erreicht, die sich zwar erinnern können, dass sie auch glücklich waren, als es alles dies nicht gab, die aber nun damit leben müssen und heute schon Ratschläge von Datenschutzbeauftragten hören: Bleibe am besten offline, dann hast du diese ganzen Probleme nicht!

Also, was wir gerade mühsam gelernt haben, vernetzt zu sein und jederzeit zugänglich, das soll nun also aus Sicherheitsgründen alles wieder vergessen werden? Ist das die einzige Antwort? Kann man sich vorstellen, dass man hier auch zu Gemeinsamkeiten kommt, möglicherweise von Technikern, die das entwickeln, die das voraussehen, von Bürgerrechtlerinnen und Bürgerrechtlern, von Anwaltsorganisationen und von staatlicher Seite, die, bevor eine Maßnahme mehr oder weniger gut gemacht wird, sich überlegen, welche Auswirkungen diese Maßnahme hat, ob man sie will, ob sie vertretbar oder nicht vertretbar ist?

Abschließend will ich sagen, in der Debatte über die Mautdaten haben das wir mehr oder weniger erfahren. Wir sind ja mitten drin. Wir werden es erfahren müssen, dass auch eine ganz strikte Regelung – ihr dürft diese Mautdaten für nichts anderes benutzen als für die Abrechnung der LKW-Maut, sie dürfen noch nicht einmal beschlagnahmt werden, also, eine absolut strikte Regelung – heute in Frage gestellt wird von beiden Partnern der großen Koalition, von Schäuble als Innenminister und von Dieter Wiefelspütz als innenpolitischer Sprecher. Wiefelspütz erklärt voller Emphase, *diese Regelung ist verfassungswidrig*, die er selber seinerzeit mit geschaffen hat. Und Schäuble sagt sybillinisch, *ich garantiere heute gar nichts mehr, was diesen Bereich angeht. Die technische Entwicklung geht weiter und dann wird auch die Verwertung dieser Daten für Sicherheitszwecke weitergehen*. Wir können also im Grunde nicht mehr den unschuldigen Glauben haben, dass irgendwo eine Datensammlung errichtet wird, die nicht auch irgendwann im Zugriff der Sicherheitsbehörden liegt.

Von daher noch schärfer die Frage gestellt: Was muss privat bleiben? Was ist der geschützte Bereich, den das Bundesverfassungsgericht uns ja bei der Telekommunikation oder bei anderen Fragen ganz nah ans Herz gelegt hat? Wo dürfen Sicherheitsapparate Zugriff nehmen? Wie kann ich Grauzonen verhindern? Und schlicht die neugierige Frage: Was kommt auf uns zu?

Darum wird es im ersten Forum gehen. Es wird auch im zweiten Forum darum gehen, dort dann auch um die Frage der rechtlichen Herausforderungen. Wie kann das Recht uns helfen in der Eingrenzung, in der Beschränkung? Zunächst möchte ich übergeben an meine Kollegin Silke Stokar, die uns durch das erste Forum führen wird.

Forum 1: Was kommt technisch auf uns zu?

Moderation: Silke Stokar MdB, Sprecherin für Innenpolitik

Danke Wolfgang! Ich möchte auch gleich überleiten in das Forum 1, in dem wir erst mal eine Vorführung des Chaos Computer Clubs erleben werden.

Dann folgt ein Vortrag von Herrn Prof. Dr. Andreas Pfitzmann. Ich begrüße Sie hier. Sie sind der Leiter der Datenschutz- und Sicherheitsgruppe an der TU Dresden. Ich habe mir schon Ihren Vortrag in Papierform ansehen können und dabei festgestellt, dass ich ganz viel von dem, was da drauf stand, gar nicht verstehe. Ich hoffe, dass Sie uns hier heute einen Einblick geben können. Wohin geht die technische Entwicklung? Was bedeutet das für die zunehmenden Möglichkeiten der individuellen Überwachung der einzelnen Bürgerinnen und Bürger?

Ich begrüße recht herzlich Herrn Dr. Udo Helmbrecht, Präsident des BSI. Mit dem BSI haben wir hier schon einige Fachanhörungen gemacht zum Thema Biometrie. Ich habe neulich auf einer Anhörung, als es um die Frage von Datenschutzgütesiegeln ging, eine gemeine Frage gestellt: Kann das BSI eigentlich für Datensicherheit noch Gütesiegel vergeben, wenn es gleichzeitig selber damit befasst ist, diese Datensicherheit zu durchbrechen? Das ist eine spannende Frage, die uns von Softwareanwendern und Unternehmen zunehmend gestellt wird. Wie ist eigentlich das Verhältnis auch der Softwareentwicklungsindustrie für Datensicherheit gegenüber der jetzt legalisierten Form, diese Datensicherheit auch zu durchbrechen?

Microsoft hat den Schlüssel für die CIA sowieso im Programm. Wir wollen uns heute näher angucken, wie die Entwicklung hier in Deutschland ist. Ich begrüße zu diesem Punkt auch recht herzlich Herrn Ulrich Walter, Direktor von L-1 Identity Solutions AG. Sie wollen uns etwas erzählen zu neuartigen polizeilichen Ermittlungsverfahren. Das heißt, wir bekommen jetzt gemeinsam einen Einblick darin, was technisch möglich ist und wohin die Entwicklungen gehen. Die Entscheidungen, ob wir das eigentlich alles wollen, oder auch die Entscheidung, ab wann muss Politik nicht nur verstehen, sondern auch klare Grenzen setzen, das werden wir danach diskutieren.

Ich übergebe an den Chaos Computer Club. Wir wollen mal sehen, wie das so mit dem Hacken funktioniert, obwohl wir das ja hier nicht machen.

Chaos Computer Club

Jan Krissler

Schönen guten Morgen! Wie hier schon angesprochen wurde, machen wir so etwas eigentlich nicht. Wir haben im Vorfeld auch mehrere Stunden darüber diskutiert, ob das sinnvoll ist, hier irgendwelche Vorführungen zu machen. Wir sind zu dem Entschluss gekommen, dass es wahrscheinlich schon für die meisten Leute das Problem deutlicher auffassbar wird, wenn man es mal kurz zeigt.

Deswegen haben wir hier auf dem Rechner, der am Beamer hängt, ein Standard Windows XP, wie es noch auf 100.000 Rechnern derzeit im Bundesgebiet unterwegs ist. Die meisten davon sind sicherlich am Netz. Hier haben wir den so genannten Hackrechner, wo

eine Windowsschwachstelle ausgenutzt werden wird, die schon längere Zeit bekannt ist, aber immer noch auf sehr vielen Rechnern funktioniert.

Ich werde das einmal kurz vorführen. Das ist eigentlich nichts Spektakuläres.

Was wir tun: Wir haben jetzt auf den Desktop einen Pfeil hinkopiert, das heißt, wir haben Schreibzugriff. Wir können es ausführen. Wir haben Execute-Zugriff. Wir können lesen. Wir können auf dem Rechner Mails lesen. Wir können uns Fotos angucken. Wir können Daten rauf schieben. Also, es müsste jetzt nicht das schicke Bild vom Bundestrojaner sein, sondern könnte genauso gut – machen wir es plakativ – Kinderpornografie sein, Nazi-propaganda, Terrorismusbombenbauanleitung. Das heißt, mit diesem Bundestrojaner holt man sich im Zweifelsfall Programme auf den Rechner, die man selber nicht kontrollieren kann und die auch ganz gezielt gegen die Person selber benutzt werden können, sei es zur Erpressung oder was auch immer.

Soviel zur Vorführung, ich glaube das veranschaulicht genug.

Constanze Kurz - Chaos Computer Club

Ich hoffe, es ist klar geworden, was wir mit dieser kurzen Präsentation zeigen wollten, nämlich den Kontrollverlust, den der Computerbenutzer mit so einer Schad-Software erleidet, sodass er nicht mehr weiß, wer auf seinen Rechner zugreifen kann und vor allem, welche Programme dort ausgeführt werden.

Wir wollen auch andererseits technisch klarmachen, dass es den ultimativen Trojaner oder ultimative Schad-Software oder Spionage-Software nicht gibt. Denn würde es die geben, hätten wir die schon längst und sie würde eingesetzt werden. Entsprechend muss einem klar sein, dass jede Schad-Software, die Ermittlungsbehörden einsetzen, ihrerseits Schwachstellen hat, z.B. Programmierfehler. Fehler, die diese Software wiederum haben kann und die ein Zweiter, z.B. jemand, der für die Wirtschaft spioniert oder schlicht ein Krimineller ist, ausnutzen kann.

Entsprechend hat dieser so genannte Bundestrojaner immer eine zweite Seite, nämlich die, dass er eine Schwachstelle als Tor auch für andere offen lässt, die vielleicht diese Schwachstelle ausnutzen wollen. Das ist immer eine Gefahr.

Zum Zweiten ist die Gefahr für die Ermittlungsbehörden die, dass dieser Bundestrojaner entdeckt wird. Weil klar ist, dass jede Art von Schad-Software *nach Hause telefoniert*, weil ja Daten, die auf dem aususpionierenden Rechner lagern, wieder dorthin gelangen sollen, wo sie ausgewertet werden können. Entsprechend besteht immer eine Entdeckungsgefahr.

Uns ist jetzt schon vollkommen klar, dass, wenn auch nur einmal so ein Bundestrojaner auf irgendeinem Rechner gefunden wird, sich Wettbewerbe von Hackern bilden werden, die versuchen werden, dieses Schad-Programm zu analysieren. Sie werden auch ganz sicher, Schwachstellen in diesem Programm finden.

Den Missbrauch durch Dritte, der hier angegeben ist, hatte ich schon erwähnt. Es muss natürlich klar sein, dass die Schwachstelle, die benutzt wird, eben auch durch andere benutzt werden kann.

Betonen möchten wir in besonderer Weise, dass der Bundestrojaner nicht nur dafür steht, dass man Daten damit ausspionieren und den Rechner quasi zweckentfremden kann, auch zur akustischen oder visuellen Wohnraumüberwachung, da ja die modernen Rechner wie die, die hier stehen, auch ein Mikrofon und eine Videokamera inklusive haben, sondern dass vor allen Dingen auch eine Manipulation der Daten stattfinden kann, bis dahin, dass

man einfach Daten auf diesem Rechner platziert. All dieses ist mit diesem Programm möglich.

Entsprechend ist auch die Frage, inwiefern ausspionierte Daten überhaupt weiter verwendet werden können, z.B. vor Gericht, weil ja gar nicht klar ist, ob die vielleicht nicht auch manipuliert sind oder erst auf dem Rechner platziert wurden. Es ergibt sich hier auch für denjenigen, der ausspioniert wird, ein hohes Erpressungspotential, weil, man kann sich vorstellen, wenn man plötzlich auf seinem Rechner Bilder platziert bekommt, wie z. B. Kinderpornografie, dann wird man sehr schnell mundtot. Da ist also ein hohes Erpressungspotential.

Wir möchten als Chaos Computer Club hier die Chance nutzen, zu betonen, dass wir den Bundestrojaner in einem etwas größeren Zusammenhang sehen, und zwar in dem Zusammenhang, dass sich eigentlich seit dem 11. September so viele gesetzliche Maßnahmen gegen den Bürger richten, dass er eigentlich schon als Generalverdächtiger gelten kann. Wir haben hier nur einige Beispiele genannt. Es ist insbesondere zu nennen, die schon einleitend durch Sie erwähnte Biometrie in Ausweisdokumenten, wo wir in Kürze sehen werden, dass erwachsene Bundesbürger, die einen Pass beantragen, ihre Fingerabdrücke auf den Meldeämtern abgeben werden. In der Folge werden auch die Personalausweise mit diesen biometrischen Merkmalen ausgerüstet, das heißt, dass also alle erwachsenen Bundesbürger für den Personalausweis ihre Fingerabdrücke abgeben, also, eine biometrische Erfassung der erwachsenen Gesamtbevölkerung.

Zum Zweiten, die auch hier sicherlich schon diskutierte EU-Vorratsdatenspeicherung, wo die Daten der Internetkommunikation, der Telefon- und der Handykommunikation verdachtsunabhängig sechs Monate lang gespeichert werden sollen. Das ist also auch eine Maßnahme, wo im Prinzip alle Bürger, weil jeder mit diesen Mitteln kommuniziert, verdachtsunabhängig ins Ermittlungsraster geraten.

Eine dritte, sehr schwierige Problematik in diesem Zusammenhang sehen wir in der so genannten Personenkenntnis, die jetzt auf mehreren Wegen dem Bürger aufgepfropft wird. Das geschieht einmal durch die biometrischen Merkmale, die ja eindeutige Personenkenntnis sind, weil der Fingerabdruck oder das Gesichtsbild in der digitalen Form eine Personenkenntnis ist, aber zweitens auch über die Planungen, wie sie momentan bereits laufen, über die Finanzämter, wo eine Personenkenntnis vergeben wird, die zwar anders heißt, nämlich Wirtschaftsidentifikationsnummer, die aber praktisch eine Personenkenntnis ist und den einzelnen Bürger auch hier auf eine Nummer reduziert.

Das ist ein Verfahren, von dem wir wissen, dass das Bundesverfassungsgericht dieses als nicht verfassungsgemäß klassifiziert hat, das aber dennoch jetzt gleich auf mehreren Wegen gemacht wird.

Ein letzter Punkt, den wir hier noch in diesem Gesamtszenario eines Kontroll- und Überwachungsstaates ansprechen wollen, ist die immer stärker zentralisierte Datenhaltung. Wir sehen es vor allen Dingen auf der Verwaltungsebene, dass die Daten, wenn auch nur über Indizierung, aber dennoch zusammengelegt werden und vor allem, dass verschiedene Ermittlungsbehörden in den zentralen Lagezentren auf diese Daten zugreifen können. Wir sehen hier eine große Gefahr. Und wir sehen den Staat in der Pflicht, den Bürger und seine Daten zu schützen.

Wir haben auf dem privaten Sektor, wie sicherlich vielen von Ihnen auch bekannt ist, in Bezug auf die Social-Networking-Software einen großen Bereich von privaten Datensammlern, die vor allen Dingen junge Leute und diese, die in den Social-Network-

Plattformen aktiv sind, in Bezug auf ihre Daten tracken, wo alles gesammelt und ausgewertet wird. Der Staat sollte eigentlich hier in der Rolle sein, die Bürger genau zu schützen und sich nicht auch noch als Überwachungs- und Datensammler zu gerieren. Vielen Dank!

Wolfgang Wieland

Eines hatte ich, besonders peinlich bei einer Veranstaltung, die sich so um Datenschutz dreht, vergessen vorab zu sagen: Wir machen Tonbandaufnahmen von den Redebeiträgen hier. Sollte das jemand nicht wollen, gibt es zwei Möglichkeiten, Schweigen oder um Löschung des Beitrages bitten. Wir tun das dann auch sicher und zuverlässig.

Silke Stokar

Wolfgang, bist du dir sicher, dass nicht eventuell Dritte Zugang zu diesen Daten haben und wir eventuell gar nicht löschen können? Diese Frage werden wir uns zunehmend stellen müssen.

Ich bitte nun Herrn Prof. Dr. Pfitzmann seinen Vortrag zu halten, damit wir noch etwas mehr darüber erfahren, was uns an technischer Entwicklung hier erwartet.

Prof. Dr. Andreas Pfitzmann

Leiter der Datenschutz- und Sicherheitsgruppe an der TU Dresden

Ja, herzlichen Dank. Wie kommen Sie zu der Annahme, dass unser Gespräch hier nur einmal aufgenommen wird? Wir haben doch alle ein Mobiltelefon bei uns. Die meisten davon können stundenlang Audio aufnehmen. Ich z. B. habe meinen Mitarbeitern versprochen, dass ich selbstverständlich zumindest meinen Vortrag aufnehmen werde, auf dass die mal hören können, was ich hier so erzähle. Ich glaube, es wird hier mehr aufgenommen, als nur einmal.

Die nächste Frage ist: Sind Sie sicher, dass nur aufgenommen wird? Vielleicht sind wir hier gerade auch auf Sendung! Die meisten Mobiltelefone sind durchaus auch geeignet, Sprache über Entfernungen hinweg zu übertragen. Bitte werden wir mal realistisch mit der Welt, mit der wir es gerade zu tun haben.

Mir wurde ein Thema gestellt, ich habe es mir nicht selbst ausgesucht. Ich werde versuchen, mich daran zu halten. Vielleicht als Vorrede: Alles, was die Kollegen vom Chaos Computer Club über die technischen Möglichkeiten gesagt haben, möchte ich ausdrücklich bestätigen. Diese Möglichkeiten bestehen. Das ist real. Über politische Einschätzungen kann man lange diskutieren. Das müssen wir wahrscheinlich auch. Aber zunächst einmal: Wer die technischen Möglichkeiten und Aussagen bestreitet, der hat entweder keine Ahnung oder er lügt.

Mein Thema: „Qualität und Ausmaß der technischen Entwicklung“: Ich möchte zunächst mit Ihnen kurz durchgehen, was für qualitative Entwicklungen wir die letzten 30 Jahre erlebt haben und was steht uns – die nächsten 15 Jahre kann man in etwa sehen – bevor? Wir werden einen kurzen Exkurs machen, wie es mit den Rohdaten aussieht, was die Hardware so leisten kann. Das ist der Teil der Entwicklung, den man am konkretesten projizieren und benennen kann. Ich werde dann mit Ihnen kurz darüber nachdenken, wie sich Technik entwickelt, wenn man sie sich einfach entwickeln lässt, ungesteuerte Technikentwicklung. Ich werde ein bisschen was erwähnen über diverse Steuerungsversuche, die es gibt. Ich werde mit der Frage schließen: Wenn man versucht Technik zu steuern, in welche Richtung sollte man das denn versuchen zu tun?

Die qualitative Entwicklung sieht so aus, dass das, was ein Rechenzentrum vor 30 Jahren konnte, was ein PC vor 15 oder vor zwölf Jahren konnte, das kann heutzutage ein Smartphone. Wenn wir von hier in die Zukunft gehen: Was heute ein PC kann, das kann ein Smartphone in zehn bis 15 Jahren. Das heißt, die Vorstellungen, Sie könnten Datenverarbeitung in irgendeiner Form kontrollieren, wenn die Daten irgendwo erfassbar waren, erfasst werden konnten, die sind unreal, weil Sie einfach der Rechner nicht mehr Herr werden. Diese Rechner sind vernetzt und können Daten durch die Gegend schieben, wie immer sie wollen.

Das Telefonnetz kennen Sie alle, hundert Jahre Geschichte. Wir haben in Deutschland heftig über ISDN diskutiert. Wir haben weniger heftig über das Internet diskutiert. Was uns bevorsteht unter dem Schlagwort *ubiquitous computing* ist, dass nicht nur speziell gebaute Gegenstände, nämlich Rechner oder Mobiltelefone, Smartphones vernetzt werden, sondern zunehmend unsere Alltagsgegenstände. Was bedeutet, Sie tragen dann Ihr Jackett mit sich herum und das System weiß, wo Ihr Jackett gerade ist. Der Verdacht liegt nahe, wenn es nicht gerade in Ihrem Kleiderschrank ist, dann sind Sie vermutlich in der Nähe.

Fernsehen kennen Sie alle, eine lange Geschichte. Videoüberwachung kennen wir auch alle. Was uns bevorsteht unter dem Schlagwort *Ambient Intelligence*, ist die Vorstellung, dass wir uns in Zukunft in einer Welt bewegen, wo nicht nur unser Aussehen und das, was wir akustisch von uns geben, wahrgenommen wird, sondern auch wie wir atmen, wie wir uns fühlen, um dann unsere Umgebung dazu zu bringen, dass sie sich an unsere Wünsche anpasst.

Die Leute, die diese Systeme entwickeln, machen mitunter technisch tolle Dinge. Aber die meisten Leute aus dem Gebiet, die ich bisher gesprochen habe, haben völlig vergessen, dass es in dieser Welt Konflikte gibt. Sie entwickeln eine Technik, die wunderbar funktionieren würde in einer Welt ohne Konflikte, die aber ein Riesennmissbrauchspotential hat und vermutlich auch kaum Marktchancen in einer Welt mit Konflikten. Bitte an der Stelle über Technikgestaltung nachdenken oder die Konflikte in der Welt eliminieren. Aber das Zweite bedeutet, dann eliminieren Sie Gesellschaft. Sie können Konflikte zwischen Menschen nicht eliminieren.

Wir hatten in der Vergangenheit eine Welt, wo es kaum Identifier gab für Objekte. Irgendwann kamen Barcodes als Typ-Identifier. Sie kennen diese hässlichen Dinge, hauptsächlich von Büchern vermutlich. Wir werden eine Zukunft haben, wo wir Exemplar-Identifier haben. Also, jedes Objekt hat seinen individuellen Identifier. Da steht nicht nur der Typ drin, sondern da steht wirklich die Exemplarnummer drin. Das Ganze wird über Funk auslesbar sein. Ihr Jackett wird selbstverständlich einen RFID-Chip haben. Das könnte der Reinigung sagen, wie das Jackett bitte zu reinigen ist oder auch nicht, aber es könnte selbstverständlich auch Lesegeräten sagen, wo es ist. Wenn Sie Ihr Jackett jetzt nicht in großem Stil mit anderen Leuten tauschen, was natürlich eine Maßnahme wäre, dann sagt dieser Chip auch, wo Sie sich aufhalten. Das gilt in gleicher Weise auch für T-Shirts, nur dass es bei T-Shirts vermutlich fünf Jahre später sein wird, weil die einfach etwas billiger sind als Jacketts. Aber es kommt. Also, es erwischt auch andere Bevölkerungsschichten.

Sie kennen Passbilder. Wir haben seit etwa anderthalb Jahren biometrische Passbilder in der Hinsicht, dass Sie auf ihnen nicht mehr lächeln dürfen, dass das Bild digital gespeichert ist und dann auch über Funk von dem Pass ausgelesen werden kann. Wir werden, wenn es nach dem Innenministerium geht, demnächst auch Fingerabdrücke in Pässen

haben. Das wird drastische Auswirkungen haben, und zwar nicht in erster Linie, weil wir die Fingerabdrücke im Pass haben, sondern weil wir daran gewöhnt werden, an verschiedenen Stellen unseren Fingerabdruck in guter Qualität abzugeben. Was das für organisierte Kriminalität bedeutet, die falsche Spuren legen will, das ist abenteuerlich. Ich weiß nicht, ob irgendjemand im Bundeskriminalamt darüber mal nachgedacht hat und falls er darüber nachgedacht hat, ob seine Bedenken im Innenministerium gehört wurden.

Die Entwicklung im Großen geht letztlich davon aus, dass wir früher einmal in Dörfern oder in kleinen Horden gelebt haben, vermutlich mit wenig Anonymität unter unseren Nachbarn oder Hordenmitbewohnern, hin über eine klassische Stadt, wie Sie es aus vielen klassischen Filmen kennen, wo es doch relativ viel Anonymität gibt, hin zu einem globalen Dorf, wo wir, wenn wir die Technik einfach so entwickeln, wie es jetzt gerade versucht wird, keinerlei Anonymität mehr haben. Die Sicherheitsbehörden werden enorm viel über uns wissen – und wenn wir realistisch sind, dann wird auch die organisierte Kriminalität enorm viel über uns wissen. Denn all diese Schnittstellen, diese Überwachungsmaßnahmen, sind selbstverständlich so, dass sich mit geringer zeitlicher Verzögerung auch die organisierte Kriminalität ihrer zu bedienen weiß. Sei es, die Geschichte ist voll mit Beispielen, dass es auch innerhalb der Polizei- und Sicherheitsbehörden Menschen zweifelhaften Charakters gab, sei es, dass einfach technische Systeme, die so komplex sind, dass sie nicht fehlerfrei administriert werden können, einfach die Lücken haben, sodass der Einstieg dort ist. Das ist erst mal die qualitative Entwicklung.

Quantitativ haben wir eine exponentielle Leistungsentwicklung von Speicherkapazitäten und Kommunikationskapazität. Wir haben eine systemische Entwicklung, die ich vorhin schon skizzierte, also, das Rechenzentrum von vor 30 Jahren, das haben Sie heute in jedem normalen Mobiltelefon. Früher war dann Rechnerbenutzung nach Schulung, heute ab der Schule. Die nächste Generation wird die Sache ab der Geburt benutzen. Es wird hoffentlich leichter, irgendwann kinderleicht und schließlich unbewusst.

Leistungsentwicklung der Speicherkapazität, ich habe das mal im Detail aufgelöst und Ihnen eine schöne Zusammenfassung mitgebracht. Ich bin in das Gebiet Datenschutz gekommen, als wir 1983 geradezu eine Bürgerbewegung gegen die Volkszählung hatten. Die ging nicht ganz spurlos an mir vorbei, weil die Landesbeauftragte für den Datenschutz in Baden-Württemberg damals eine Vorlesung über Datenschutz an der Uni Karlsruhe gehalten hat. Das hat mich in dieses Gebiet gebracht. Und ich habe dann angefangen, so etwa zehn Jahre nach der 1987 dann tatsächlich durchgeführten Volkszählung, Speichermedien in die Luft zu halten. Wie viele braucht man, um alle Daten dieser Volkszählung abzuspeichern? Am Anfang war das noch ein bisschen anstrengend. Da musste man Dinge mit sich herumschleppen. Später waren das dann noch spezielle Speichermedien, die ich hochhalten musste. Ich musste irgendetwas über Lesegeräte beschreiben, die das Publikum nicht kannte.

Heute ist die Volkszählung von 1987 hier drauf und es gibt noch eine Menge Platz für die nächste Volkszählung. Es ist etwas, was Sie alle kennen, was Sie im Media-Markt kaufen für 40,- €. [hält einen USB-Stick in die Luft]

Das heißt, wenn irgendjemand irgendwann mal an diese Daten rankommt – löschen wird er sie nie. Sie werden nicht herausfinden, wo er sie hat. Versuchen Sie mal alleine in diesem Raum festzustellen, wie viele es von diesen Dingen hier gibt. Es wird keine soziale Akzeptanz finden, dass Sie das versuchen festzustellen.

Das heißt also, die Vorstellung, dass Sie Daten, die jemand mal erfasst hat oder auch nur erfassen konnte, wieder aus der Welt schaffen, ist absolut unreal. Es hilft nur vorzubeu-

gen. An der Stelle Gesetze zu machen, die irgendetwas tabuisieren, na ja, das hält fünf Jahre, wenn man Optimist ist, sagt man zehn Jahre. Wer mehr als zehn Jahre sagt, hat irgendetwas verdrängt.

Kommunikation ist wahrscheinlich der Teil in den letzten zehn Jahren, der sich am stärksten entwickelt hat.

Dritter Teil, wenn wir eine ungesteuerte technische Entwicklung zulassen – weitgehend ist sie das – und wenn wir gucken, welchen gesetzgeberischen Trend wir seit dem 11.09.2001 haben, dann arbeitet beides, die ungesteuerte technische Entwicklung wie auch der gesetzgeberische Trend, ganz klar gegen die Autonomie der Bürgerinnen und Bürger. Er arbeitet insbesondere gegen ihre informationelle Autonomie, weil bspw. Speichermedien so billig sind und die Auswertung von Speichermedieninhalten so schnell geht und wenig kontrollierbar ist.

Wo es eine Entwicklung gibt, gibt es natürlich auch eine Gegenbewegung. Es gibt seit 1981 in der Forschung Entwicklungen im Bereich anonyme Kommunikation. Es dauerte etwa ein Jahrzehnt bis man das so gut verstanden hatte, dass man dann sinnvollerweise anfangen konnte, Prototypen zu bauen. Es hat uns wiederum ein Jahrzehnt beschäftigt, bis diese Prototypen so leistungsfähig waren, dass sie inzwischen allgemein nutzbare Dienste erbringen können.

Es wird Sie jetzt nicht überraschen, dass es eine Gegenbewegung zur Gegenbewegung gibt. Das kennen Sie unter dem deutschen Schlagwort Vorratsdatenspeicherung oder dem englischen Begriff Data-Retention.

Einwurf Wolfgang Wieland: Können Sie zu dem Begriff „anonyme Kommunikation“ ein Wort sagen?

Gerne. Das ist sehr gut, dass Sie mich unterbrechen. „Anonyme Kommunikation“ bedeutet, dass wir nicht nur die Option haben, dass die Kommunikationspartner sich nicht gegenseitig identifizieren können. Ich mache mal ein Beispiel. Sie bieten einen Horoskopdienst an. Weder will derjenige, der ihn anbietet, dass Sie wissen, wer er ist, sonst müsste er vielleicht für den Horoskopdienst haften, noch möchten Sie, als derjenige, der den Horoskopdienst abrufen, mit irgendeinem Horoskopdienst in Verbindung gebracht werden – Verdacht auf Aberglauben. Jetzt könnten zwei Leute miteinander Daten austauschen, ohne dass sie sich gegenseitig genau kennen. Sie wissen nur, hier der Horoskopdienst und jemand auf der anderen Seite, der Interesse daran hat. Bloß – und jetzt wird es spannend – ist es keineswegs so, dass notwendigerweise derjenige, der die Kommunikation vermittelt, Telekom, Internetserviceprovider, wer auch immer damit Geld verdient, wissen muss, wer die beiden sind. Wir können heutzutage Kommunikationsnetze so bauen, dass niemand mehr – auch der Netzbetreiber nicht – mitkriegt, wer mit wem kommuniziert. Trotzdem können wir die Sachen so bauen, dass eine Abrechnung erfolgen kann, also, dass man damit auch Geld verdienen kann. Anonyme Kommunikation ist also kein Vorschlag, den Kapitalismus abzuschaffen.

Es gibt also eine Gegenbewegung zur Gegenbewegung. Und es gibt viel Streit darum. Es gibt jetzt nicht nur – da kommen wir wieder zur Gegenbewegung – anonyme Kommunikation, es gibt auch ein so genanntes Identitätsmanagement unter Nutzerkontrolle. Auch da hat die Theorie sehr früh begonnen. Die Prototypen sind etwas jünger. Ziel an der Stelle ist, dass Sie keineswegs alles, was Sie in Ihrem Leben tun, unter Ihrem guten Namen oder irgendeiner Identität tun, die ganz leicht zu Ihrem guten Namen verknüpft werden kann, sondern dass – wenn Sie das wünschen – Sie verschiedene Lebensbereiche

auseinander halten können, sodass nicht leicht verknüpft werden kann, dass sich in verschiedenen Lebensbereichen letztlich dieselbe Person oder unterschiedliche Facetten derselben Person manifestieren. Das kann man bauen. Da gibt es inzwischen auch Prototypen. Und auch an der Stelle gibt es natürlich Gegenbewegungen. Das, was wir jetzt gehört haben, der Bundestrojaner ist so eine Sache. Natürlich werden Sie nicht, weil Sie in Ihrem Leben vielleicht 200 Rollen spielen, 200 PCs benutzen wollen, wobei Sie jeden Ihrer PCs für eine Rolle nehmen. Das könnten wir vielleicht in 30 Jahren diskutieren, wenn die PCs so klein geworden sind, dass wir sie wirklich zu Hunderten kaufen bei ALDI, und zwar ohne es zu merken, aber momentan, für die nächsten 20 Jahre, brauchen wir das noch nicht zu betrachten.

Steuerung in welche Richtung? Erstens bin ich nicht sehr optimistisch, dass man Technik beliebig steuern kann. Es wird sicherlich in dem, wie man Technik steuern kann, gewisse Grenzen geben. Soweit man Technik steuern kann, ist meine Überzeugung: Techniken zur Individualüberwachung, ja. Unter Individualüberwachung verstehe ich, dass jeweils die einzelne Überwachungsmaßnahme spürbare Kosten erzeugt pro Überwachungsvorgang. Denn machen wir uns nichts vor, einen Geheimdienst kontrollieren Sie nur über das Budget. Jede andere Form, einen Geheimdienst kontrollieren zu wollen, ist lachhaft. Man versucht das in Deutschland, was dann die Folge hat, dass wir in Deutschland keine ernsthaften Geheimdienste haben.

Versuchen Sie mal, in Israel den Geheimdienst durch eine parlamentarische Kontrollkommission zu kontrollieren! Ich glaube, die Leute in Israel tun es nicht. Die wissen vermutlich, was ein Geheimdienst ist. Also, es geht nur über das Budget und das heißt, die Kosten müssen anfallen bei der einzelnen Maßnahme.

Die Technik hat an der Stelle unheimlich viel geliefert in den letzten 20, 30 Jahren. Sie wird vermutlich auch für die nächsten 15 Jahre noch einiges verbessern, klassische Dinge: Richtmikrofone, Wanzen. Es gibt Empfangs- und Auswertungsgeräte für elektromagnetische Abstrahlung. Sie wissen, jeder PC, weil da Ströme bewegt werden, sendet Informationen über das aus, was in ihm passiert. Wenn Sie das entsprechend fein mit Antennen auffangen und auswerten, kriegen Sie eine Menge raus. Und das sind Dinge, die sind schwer zu vermeiden, während viele andere Maßnahmen, wie man versuchen will, Kriminelle zu fangen, leicht zu unterlaufen sind.

Dann Individualüberwachung: DNA-Analyse in Einzelfällen, das heißt nicht, wir machen jetzt eine Datenbank der DNA der gesamten Bevölkerung, sondern für ein konkretes Verbrechen mit konkreten DNA-Spuren am Tatort, untersuchen wir die DNA der zehn Verdächtigen und danach löschen wir die Daten.

Wenn Sie unbedingt meinen, dass Sie in Kommunikationsnetzen Daten erheben müssen, dann bitte: das Zwischenspeichern von Kommunikationsdaten im Einzelfall, *quickfreeze* – nicht eine Datenhalde auf Vorrat.

Was ich nicht tun würde, ist, Technik bauen, sodass Sie zur Massenüberwachung geeignet ist. Typischerweise ist alles, was Sie in Infrastrukturen integrieren, zur Massenüberwachung geeignet. Da wird Ihnen natürlich am Anfang jeder Stein und Bein schwören, dass niemand Massenüberwachung in Deutschland durchführen will. Aber wenn Sie sie in die Infrastruktur hineintun, müssen Sie bedenken: es gibt auch fremde Geheimdienste, die vielleicht Interesse daran haben, in Deutschland Massenüberwachung durchzuführen. Die werden sich dieser Infrastruktur auch bedienen.

Also, was würde ich nicht tun? Ich würde keine Schnittstellen zur Fernmeldeüberwachung in die Netze einbauen, die sind schon drin. Das heißt konkret, wir sollten sie nicht ein-, sondern ausbauen. Ich würde zweitens nicht empfehlen, Vorratsdatenspeicherung zu machen.

Mit der letzten Bemerkung gehe ich jetzt als Techniker weit über den Technikbereich hinaus: Wenn man über einen Interessenausgleich zwischen Strafverfolgung einerseits versus *Privacy* andererseits redet, dann sollte man bitte über alle Anwendungen gleichzeitig reden. Man muss eine Optimierung über Anwendungen hinweg machen. Was ich momentan erlebe: Wann immer es eine kleine Gruppe gibt, die damit entweder Geld verdienen kann oder Arbeitsplätze sichern oder schaffen, indem sie sagt, wir hätten gerne noch Überwachungsstrukturen hier und da, dann haben die Leute, wenn sie über einzelne Anwendungen diskutieren, immer einen Anlass und immer ein Beispiel, dass sie sagen, an der Stelle wäre es gut gewesen, wir hätten jetzt noch mehr Überwachung gehabt. Sie verlieren aber an der Stelle völlig aus dem Auge, dass ja auch die technische Entwicklung als Selbstläufer ihnen gewisse Überwachungsmöglichkeiten gibt und dass man viele dieser Anwendungen gemeinsam sehen muss.

Das wäre mein Plädoyer, nicht jedem einzelnen Wunsch auf Sicherung des Arbeitsplatzes bei der Fernmeldeüberwachung zu entsprechen. Dankeschön.

Silke Stokar

Ich bedanke mich auch bei Ihnen. Ich fand das ausgesprochen spannend und gerade auch den Hinweis, dass man alle Maßnahmen insgesamt betrachten muss. Ich glaube, dass wir das schon gar nicht mehr können. Es wäre mal ein ganz spannendes Projekt, beim einzelnen Bürger zu gucken, welche Informationen gibt es an irgendwelchen Stellen über ihn und wer nutzt diese, sowohl staatlich als auch privat.

Ich glaube, nur mit so einem drastischen Bild könnten wir auch wieder ein Bewusstsein dafür wecken, wie weit das Ganze geht. Diese ganzen Techniken, Begriffe und ihre Bedeutungen zu verstehen, sie in der Einzelanwendung zu bewerten, das schafft man im Laufe der Zeit vielleicht im Ansatz. Eine Gesamtbewertung haben wir nicht, sie ist aber dringend erforderlich.

Ich übergebe damit an Herrn Dr. Helmbrecht vom BSI. Sie werden uns jetzt erläutern, wie das BKA das machen will oder auch nicht.

Dr. Udo Helmbrecht

Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Vielen Dank. Im Letzteren muss ich Sie enttäuschen und ich hoffe, dass das nach meinem Vortrag auch deutlich wird.

Den beiden Vorrednerinnen und Vorrednern kann ich technisch nur eingeschränkt zustimmen. Bei meinem Vortrag werden Sie sehen, dass es technisch noch viel weiter geht. Ich habe einen anderen Blick darauf und ziehe eine andere Schlussfolgerung.

Was ich Ihnen hier zeige, ist ein Ausschnitt aus Vorträgen, die ich an vielen anderen Stellen auch halte, wo es im Grundsatz um Sensibilisierung für IT-Sicherheit und den Einsatz von IT-Sicherheitsprodukten geht.

Ich möchte mit dem Thema „Risiken“ beginnen. Die Kriminalität wandert dorthin, wo das Geld verdient wird. Früher wurden Banken überfallen. Heute nennt man das Phishing. Im

Grunde genommen ist das menschlich gesehen das Gleiche. Es wäre sinnlos zu glauben, der Mensch würde sich da verbessern. Der zweite Punkt ist: Staat, Wirtschaft und Wissenschaft müssen sich vor Spionage schützen.

Wenn Sie im Internet unterwegs sind, wenn Sie sich Wareninformationsmeldungen anschauen, dann haben Sie das Bild, was ich da mal zusammengefasst gezeigt habe. Eine Bemerkung, die ich an der Stelle immer mache, ist: Wenn wir heute über islamischen Terrorismus reden, so tragisch das ist, dann sind das Anschläge auf Menschen. Über allem, was wir gehört haben, steht natürlich die Herausforderung an den Staat, sich zu fragen: Was passiert denn, wenn die Terroristen in diesem Umfeld das Internet, diese Mittel, die wir gerade gehört haben, nutzen? Und der Punkt, den ich da auch immer gerne anführe: Die klassische Spionage ist nicht ausgestorben.

Das Problem, mit dem wir konfrontiert sind – und das ist etwas, was Sie hier alle im Raum angeht, wenn wir mit unserem PC im Internet unterwegs sind –, ist, dass wir sind Risiken ausgesetzt sind, dass wir Schadprogramme auf unsere PCs aus unterschiedlichen Richtungen bekommen. Hier ein paar Beispiele aus diesem Jahr.

Das funktioniert so: Sie bekommen eine E-Mail. Sie können sich heute gar nicht sicher sein, ob der Absender der E-Mail gefälscht ist oder nicht. Es gibt das Beispiel, wo das BKA betroffen war. Es gibt gefälschte Rechnungen. Da bekommen Sie sogar perfiderweise eine E-Mail, in der drin steht: Im Anhang haben Sie eine Rechnung, die ist digital signiert. Das heißt, Sie können der vertrauen, aber wenn Sie sie aufmachen, ist es trotzdem eine ausführbare Datei und dann haben Sie irgendein Schadprogramm auf dem Rechner. Es gibt Beispiele von Quelle, Ikea und 1&1. Sie brauchen da nur einen Blick in die Presse zu werfen. Insofern sind das nur wenige Beispiele, mit denen wir konfrontiert sind.

Und – das können Sie auch der Presse entnehmen – gerade aus dem Bereich China gibt es Industriespionage, staatliche Spionage. Wenn Sie sich Statistiken der letzten Jahre anschauen, können Sie sehen, dass genau an dieser Stelle die Kriminalität in Form von Phishing und Hacking zunimmt.

Das ist das, mit dem wir tagtäglich konfrontiert sind. Wenn Sie als sorgfältiger Nutzer im Internet unterwegs sind, dann gibt es ein paar Dinge, auf die ich gleich noch kommen werde, die Sie beachten sollten, um damit vernünftig umzugehen.

Was ist das Neue, mit dem wir uns heute auseinandersetzen müssen? Das eine ist: Spam- und Schadprogramme sind heute ein Geschäftsmodell. Das andere ist: Individuell versandte Trojaner sind heute im Allgemeinen nicht zu entdecken. Was das heißt, will ich Ihnen einmal kurz darstellen.

Die Grafik links oben zeigt, was für Schäden angerichtet werden können und mit welchen Werkzeugen. Ich benutze dieses Bild gerne, weil dort nämlich die Quelle 2004 steht. Da dachte man noch Botnetze gibt es erst 2010. Solche Schäden haben wir schon heute. Und wenn Sie sich das anschauen, heißt das, dass die Effektivität der Schadprogramme zunimmt.

Ich will das an diesem Bild etwas verdeutlichen. Sehen Sie mir ein bisschen nach, wenn da viele Fachbegriffe drin sind, aber ich pflege meine Reden oder Vorträge auf unserer Internetseite zu veröffentlichen, sodass man es nachlesen kann.

Sie kennen Trojanische Pferde, darüber haben wir gerade gesprochen. Wir haben Hacker. Wir haben früher sicherlich den ethischen Hacker gehabt, der gesagt hat: „Toll, ich habe es ins Pentagon geschafft.“ Heute will der Hacker Geld verdienen. Schwachstellen, wenn

Sie heute dort Exploits haben, wenn Sie heute den so genannten Patchday von Microsoft haben, wo Microsoft seine Schwachstellen beheben will, dann kann man als Hacker davon ausgehen, das ist ja gerade gesagt worden, dass nicht jeder seinen Rechner updated, aus Nachlässigkeit oder weil er es nicht kann. Und dann gehen die Hacker hin und gucken nach und sagen dann, wenn da ein Fehler ist, den Microsoft behebt, wo ein Patch ist, da muss doch eine Schwachstelle sein. Also, schau ich doch mal nach, was das für eine Schwachstelle ist. Und mit dem so genannten Reverse Engineering finde ich die Schwachstelle und mache dann gleich ein Programm daraus und greife damit an. Und ich bin sicher, dass ich diese Schwachstelle ausnutzen kann, weil nicht alle Privatleute ihren PC upgedated haben.

Das andere sind die so genannten Botnetze. Botnetz kommt von Robot, das sind ferngesteuerte Netze, die nach dem Prinzip funktionieren, dass irgendwo auf der Welt ein Hacker sitzt, jetzt ein böser Hacker – nicht vom Chaos Computer Club – der über das World Wide Web Schadprogramme verschickt. Das sind Spam- und Schadprogramme, also Massenmails, die die Programme infizieren. Dann kann man diese Programme ferngesteuert übernehmen. Man kann dort andere Schadprogramme starten und wieder irgendwo einen Angriff starten, ob das nun Erpressungsversuche sind, Datendiebstahl oder sonstiges ist.

Wir haben hier Größenordnungen von gekaperten Rechnern von 10.000 und mehr. Sie können solche Botnetze im Internet jetzt schon kaufen. Sie können solche Botnetze mieten. Sie können sagen: „*Ich möchte mal jemanden angreifen.*“ In diesem Zusammenhang haben Sie dann natürlich die Schwierigkeit, dass Sie heute weltweit gar nicht wissen, wo dieser Hacker sitzt.

Sie kennen den klassischen Breitenangriff, bei dem mit vielen Massenmails, Spammails, Werbemails oder anderen, so genannten internationalen Serverattacken, Server oder andere Infrastrukturen attackiert wurden. Wir haben die kritischen Infrastrukturen mit ferngesteuerten Zugriffsmöglichkeiten in der Industrie, wo Sie heute die Gefahr haben, dass Kontrollsteuerungen in Industrieanlagen am Internet angeschlossen sind. Es gibt Beispiele aus den USA, wo die Staudammsteuerung für den Wasserstandpegel am Internet angeschlossen ist, sodass man es fernsteuern kann.

Wenn Sie heute – und das ist, was es uns als BSI natürlich schwierig macht, was wir als Abwehrmaßnahmen machen können – ganz dezidiert einen Trojaner schicken, erkennt das heute kein Virenschutzprogramm. Virenschutzprogramme und Firewalls gehen davon aus, dass es Signaturen und Erkennungsmuster gibt. Sobald sie erkannt sind, kann man die publik machen. Die funktionieren im Allgemeinen so, dass es viele gleichartige Muster gibt.

Wenn jetzt also jemand oder ich Ihnen eine E-Mail schicke und sage, im Attachment finden Sie meine Präsentation, dann glauben Sie, dass die Mail von mir ist. Die Mail kann gefälscht sein. Die Anlage ist keine Power-Point-Datei, sondern ein ausführbares Programm. Da haben Sie keine Chance, weil Sie dann gar nicht merken, dass Sie erwischt worden sind.

Insofern ist das jetzt ein düsteres Bild. Die Herausforderung für uns an der Stelle ist, dass wir uns mit dieser technischen Entwicklung auseinandersetzen müssen. Ich persönlich bin der Meinung, dass diese technische Entwicklung nicht aufzuhalten ist, weil sie global stattfindet. Wie können wir uns dagegen schützen? Denn hundertprozentige Sicherheit gibt es nicht, auch nicht im täglichen Leben. Aber wir wollen das IT-Sicherheitsniveau erhöhen.

Das ist der Punkt. An der Stelle noch einmal eine Folie über die Schäden, mit denen sich das BSI beschäftigt. Virus, Trojaner, Phishing hatte ich erwähnt. *Voice over IP*, d.h. Telefonie über das Internet, beginnt sich durchzusetzen. Auch dort werden wir demnächst Schäden haben.

Das BSI-Profil: Wir sind der IT-Sicherheitsdienstleister des Bundes und wir sind für die IT-Sicherheit in Deutschland verantwortlich. Das heißt, wir versuchen alles Mögliche zu tun, was im Bereich der Internetsicherheit in diesem Fall möglich ist. Wir wollen uns daran messen lassen, dass wir sagen, wir tun das Beste, was technisch möglich ist. Wir arbeiten für die Bundesverwaltung, kooperieren mit der Wirtschaft und mit der Wissenschaft und investieren von unseren 64 Millionen Euro Jahresbudget eine ganze Menge in Produkte und Projekte, um die IT-Sicherheit zu verbessern.

Ich will das kurz an diesem Beispiel verdeutlichen. Das BSI deckt das Spektrum von der Beratung für die Bundesverwaltung bis hin zur Produktentwicklung ab. Wenn Sie die Beispiele Galileo, den BOS-Digitalfunk oder hoheitliche Dokumente nehmen, dann ist es heute in vielen Projekten so, dass wir für die Kryptographie und Zertifizierung verantwortlich sind. Wir diskutieren nicht im politischen Raum. Dafür sind Sie als Politiker zuständig. Aber wir sind dann diejenigen – wenn politisch entschieden ist „Das wollen wir machen.“ (z.B. die Fingerabdrücke) – die dann sagen, wie man das nach dem Stand der Technik sicher machen kann.

Wir entwickeln mit der Industrie zusammen Produkte, links oben in dem Bild z.B. ein ISDN-Verschlüsselungsgerät, wo Sie Ende-zu-Ende-Verschlüsselung im Internet einsetzen. Das sind Produkte, die sowohl im hoheitlichen Bereich, im Staat, eingesetzt werden, wie auch von der Firma secunet im industriellen Bereich angeboten werden.

Das heißt also, an den Stellen, wo Sie mit so genannten digitalen Signaturen und Verschlüsselungen arbeiten, wo Sie Punkt-zu-Punkt-Verbindungen, also vertrauenswürdige Verbindungen, aufbauen, gibt es ein Höchstmaß an Sicherheit, was man gewährleisten kann. Wenn wir hier z.B. in der Bundesverwaltung kommunizieren, machen wir das über das Regierungsnetz. Dort sind dann eben Sprache und Daten verschlüsselt.

Eine Nebenbemerkung: Wenn man heute Signaturen nutzen würde, um E-Mails zu signieren, und das wirklich flächendeckend nutzen würde, dann wäre das vergleichbar mit Einschreiben bei der Post. Dann wüsste man, dass der Absender zumindest ein Zertifikat hat. Und ich könnte das in der großen weiten Welt dessen, was ich an Spam und anderen ungewollten Werbemails bekomme, auseinander sortieren.

Was wir auch zusammen mit den Prüfstellen in der Bundesrepublik tun, ist, Produkte zu zertifizieren. Das heißt, dort werden Produkte nach gewissen Richtlinien, so genannten Protection Profiles, untersucht, um dann festzustellen, ob diese gewisse IT-Sicherheitsstandards erfüllen.

Wir bieten auf unseren Homepages weitere Dienstleistungen an. Wir haben das BSI Bundportal (www.bsi.bund.de), wo für den Profi viele Informationen zu finden sind. Wir haben das Bürgerportal (www.bsi-fuer-buerger.de). An der Stelle kann man sich informieren: Was ist Spam? Was ist ein Dialer? Was ist ein Virus? Und wir bieten seit etwa einem Jahr einen Bürgerservice an. Das ist ein Warn- und Informationsdienst. Dort kann man sich Abonnements definieren, wo man dann für seinen PC, seine Infrastruktur, Informationen bekommt (www.buerger-cert.de).

Ich wollte mit dem Vortrag hier einerseits zeigen, dass es Gefahren im Internet gibt, dass es, genau wie in der alten Welt, ein Hase-und-Igel-Spiel zwischen Hackern und dem BSI

ist, und dass wir uns darauf einstellen müssen. Es gibt Kriminalität im Internet und Herr Ziercke kann uns noch mehr im Detail dazu sagen. Wir an dieser Stelle sind die Behörde, die präventiv zum Schutz der staatlichen Souveränität, zum Schutz unsere Industrie und unserer Bürger tätig ist.

Abschließend möchte ich das mit einem Vergleich. Sie haben das Thema Vertrauen angesprochen. Wenn Sie mit dem Arzt reden, dann muss der Arzt auch wissen, wie man mit Viren umgeht, um am Ende einen Impfstoff zu entwickeln und einzusetzen. Aber Sie vertrauen dem Arzt auch, dass er Ihnen hilft. In diesem Sinne sind wir die Behörde, der Sie vertrauen können. Wir sind gerne bereit uns so transparent aufzustellen, wie Sie das wünschen.

Dankeschön.

Silke Stokar

Ich danke auch und möchte gleich überleiten zu Herrn Walter. Neue polizeiliche Ermittlungsmethoden, das ist natürlich auch ein ganz spannendes Thema. Ich habe da gleich mal eine Frage, die mir von der Grünen Jugend vor dem G8 Gipfel gestellt wurde. Ist es möglich in einem größeren Raum alle Handys tot zu schalten? Ich habe geantwortet, ich glaube schon, dass sie das können, aber da die Polizei kein BOS-Digitalfunk hat, braucht sie selber Handys, also, wird sie nicht alle tot schalten. Vielleicht können Sie uns einen Einblick geben über das, was möglich ist. Und auf was müssen wir uns auf der anderen Seite aus dem Bereich Datenschutz und Steuerung dieser Technik einstellen?

Ulrich Walter

Direktor von L1 Identity Solutions AG

Vielen Dank für die nette Eingangsfrage, die ich definitiv jetzt nicht beantworten werde im Sinne der Firma o. ä., sondern da würde ich dann im Zweifelsfalle Herrn Ziercke dazu fragen wollen und ihm die fachliche Beurteilung überlassen.

Ich kann das höchstens so beantworten: Wir haben dazu alle viele Kinofilme gesehen. Da wurden auch mit großem Gelächter und großer Freunde von vielen gesehen, wie mit einem relativ speziellen elektrischen Instrument sämtliche elektronische Systeme in einem kleineren Raum tot geschaltet wurden, nicht nur die Handys. Da denken wir z. B. an „Ocean's Eleven“.

Wenn ich hier als Vertreter eines Wirtschaftsunternehmens spreche und Ihnen vielleicht ein paar Informationen vermitteln kann und darf, so bedeutet das letztlich in der Tat, dass wir versuchen, mit modernen Technologien, wie sie z.B. in der Polizeiarbeit eingesetzt werden, Geld zu verdienen. Ich bitte Sie diese Tatsache vorweg zu entschuldigen. Andererseits hoffe ich, Ihnen vielleicht ein wenig die Angst nehmen zu können, was tatsächlich Theorie und in der Theorie denkbar ist, was aber wirklich in der Praxis heute geleistet und getan werden kann.

Eines sollte ich vorweg noch sagen, da den meisten wahrscheinlich der Name L-1 und Identity Solutions noch nicht so bekannt ist. Wir sind hauptsächlich ein Hersteller von Lösungen, die sich mit dem Thema Biometrie beschäftigen. Deswegen sehen Sie auch hier schon auf der Folie die Themen Iris, Finger und Gesicht, aber auch insbesondere Biometrie in Verbindung mit hoheitlichen Dokumenten bzw. deren Kontrolle. Ich werde Ihnen aber auch ein bisschen was dazu sagen können, was unter Einsatz von Teilen der Biometrie in der heutigen Polizeiarbeit möglich ist, das allerdings nicht nur mit dem Fo-

cus auf Deutschland, sondern, da wir insbesondere international tätig sind, mit einem etwas weiteren Blickwinkel. Das soll heißen, nicht alles, was Sie heute hier sehen werden, werden Sie heute oder morgen in Deutschland so finden, sondern was letztendlich auch denkbar ist und auch im Ausland vielfach schon getan wird, dort allerdings nicht unter dem Aspekt, den wir jetzt hier sehr, sehr stark gesehen haben, der Überwachung o. ä.. Letztlich kann Biometrie eben auch zum Nutzen der jeweiligen Bürger sein und damit das Leben auch erleichtern. Diesen Aspekt werde ich versuchen, Ihnen etwas näher zu bringen.

Wenn wir so viel über Biometrie sprechen, möchte ich Ihnen auch natürlich etwas zum Thema polizeiliche Ermittlungsarbeit generell sagen, wo wir letztendlich im engen Kontakt einerseits mit Behörden wie dem BKA in Deutschland, aber auch anderen Sicherheitsinstitutionen international, sind, aber letztlich genauso mit dem BSI. Die schauen wiederum darauf, dass diese Technologien, die sie von uns dann als Reaktion, auf politische Vorgaben zum Teil, erhalten – ich meine, der 11. September war hier eine politische Vorgabe, nicht nur in Deutschland, sondern international – wie man darauf reagieren kann.

Die Anforderungen heute für die Polizeiarbeit wechseln so rapide konträr zu dem, was wir noch vor wenigen Jahren gesehen haben. Wir haben das Internet. Es ist zur Genüge beleuchtet worden. Ich muss da jetzt nicht mehr so viel sagen. Ich möchte allerdings vom Chaos Computer Club einen Aspekt aufgreifen, der sich mit dem Thema der pornografischen Materialien z. B. beschäftigt. Auch hier werde ich Ihnen zeigen, was man da heute schon machen kann. Das ist leider noch nicht ganz ausgereift, um das zu unterbinden. Ich denke, da sind wir, ich unterstelle das, uns alle hier im Raum einig, dass man dagegen sehr wohl etwas tun sollte und dass hier nicht in die Persönlichkeitsrechte oder andere Schutzbedürfnisse des Einzelnen eingegriffen wird.

Zum anderen, sind die neuen Kommunikationsstrukturen natürlich für die Polizei- und Ermittlungsarbeit sehr, sehr wichtig und vor allem auch die Datenquellen. Das heißt, es reicht eben heute nicht mehr, ein Telefon, ein Handy zu überwachen. Sie müssen eben noch ganz andere Dinge bewältigen. Wie man das leisten kann, ist auch nicht immer ganz einfach. Damit ergibt sich die Möglichkeit einer Massenüberwachung, wie wir sie vorhin von Herrn Pfitzmann gehört haben, die aber auch nur im Einzelfall möglich ist, um eine einzelne Person zu überwachen.

In diesem Zusammenhang sind insbesondere die Anforderungen da an die Selektion der millionenfachen Information auf ihre Relevanz. Und es geht darum, wie ich das mit herkömmlichen Verfahren und Strukturen insbesondere in der Polizeiarbeit tue, die sich – das gilt nicht nur für Behörden und Polizei – sondern auch für Privatwirtschaftsunternehmen, ja auch nicht von heute auf morgen verändern. Die Beamten, die z.B. heute eine Ermittlung im Internet betreiben, werden noch nicht deswegen morgen sofort bereit sein, die neuesten Technologien, wie wir sie jetzt gerade hier gehört haben, dann einzusetzen, geschweige denn so einzusetzen, dass daraus eine Bedrohung oder eine Gefahr für den einzelnen Bürger entstehen würde.

Ich habe kurz Internetsuchmaschinen skizziert. Es gibt natürlich auch eine Bildanalyse im Netz. Wie kann ich mir z. B. anhand von Gesichtsinformationen im Netz Daten besorgen? Dann möchte ich Ihnen allerdings auch eine Datenbank gestützte biometrische Personenüberprüfung im mobilen wie auch stationären Einsatz etwas erläutern. Zu einem Schwerpunkt wird Herr Ziercke vielleicht noch etwas sagen, zu dem abgeschlossenen Versuch, wie er in Mainz gerade im Hauptbahnhof erfolgt ist. Dazu gibt es die nächsten Tage

eine Presseveröffentlichung. Am Schluss möchte ich Ihnen noch einmal die Vernetzung und Kombination in einzelnen Datenbankanalyse-Systemen zeigen.

Was sehen Sie hier? Sie sehen eine nur sehr schematische Darstellung von verschiedensten Bildmaterialien, wie wir sie im Internet und in anderen Medien heutzutage immer wieder finden. Wo es eben sehr schwierig ist, letztlich dann nachzuvollziehen, wer betreibt denn hier was und mit welchem Hintergrund. Eventuell verletzt das bestehende Gesetze bzw. schutzwürdige Bedürfnisse anderer. Hier kann ich Ihnen nur mitgeben, dass es bereits erste Forschungsprojekte, die speziell mit den Universitäten betrieben werden, in Deutschland gibt, aber auch international, wo man versucht anhand solcher Bildmaterialien, die eben dann durch Suchmaschinen überprüft werden, und zwar anonym zunächst mal, um festzustellen, wie alt ist denn z. B. eine Person auf einem jeweiligen Bild.

Das heißt, man versucht anhand des Gesichtes, nicht das Alter auf den Monat genau, sondern ein ungefähres Altersraster zu bilden. Das passiert in einer Massenanalyse, wo man dann sehr schnell sagen kann „*Oh, hoppla, hier treffe ich aber auf Bilder von definitiv unter 10-Jährigen.*“ Wenn ich dann dazu noch einen Text in der jeweiligen Seite oder Informationsquelle finde, sei es eine Email oder Ähnliches, dann kann ich auch noch sagen, hier könnte es sich eventuell eben um Kinderpornografie handeln. Auch dann gibt es natürlich den Beamten, der dann dahinter sitzen kann, der sich das genauer ansehen muss. Hier gibt es die Biometrie im weitesten Sinne bei einer Überprüfung.

Ich möchte noch einmal drei Elemente herausstellen: Wir haben zum einen die Biometrie beim Thema der ganzen hoheitlichen Dokumente, die Reisepässe wurden angesprochen. Ich möchte hier allerdings sagen, ich denke nicht, dass hier ein Generalverdacht gegen den Bürger erhoben wird, sondern es soll das Gegenteil in der Zukunft und auf lange Sicht erreicht werden, nämlich dass das einzelne Ausweisdokument des Bürgers ihm ja auch den Schutz bietet, dass es eben nicht ohne Weiteres von einem anderen verwendet werden kann. Alleine das Speichern von Bildern im Chip stellt ja keine zusätzliche Biometrie dar, die wir, die Schuldigen, die wir hier sitzen, neu eingeführt hätten oder der Gesetzgeber uns vorgegeben hat, sondern es ist ja letztlich nur das Digitale, dass wir eben auch jetzt im Chip haben in der digitalen Form.

Die Finger, natürlich, das ist eine neue Form. Aber auch hier muss man sehr genau die Pressemitteilungen lesen und auch die Wünsche, die aus dem Bundestag kamen, was hier gemacht werden soll. Es soll jetzt nicht eine Analyse eines jeden einzelnen Bürgers bei der Aufnahme von Biometriedaten erfolgen, die dann zu einer Massenspeicherung führen, sondern es soll dann, wenn an der Grenze, wie auch schon heute, ein Verdacht besteht, eine zusätzliche Möglichkeit geschaffen werden, das zu überprüfen.

Natürlich, ich möchte es nicht abstreiten, ist ein Missbrauch rein theoretisch immer möglich. Da vertrauen wir auch auf Sie z.B., dass Sie sagen, Herr Montag, Sie löschen auch die Daten, die wir hier heute aufnehmen. Insofern vertrauen wir Ihnen da auch. Skepsis ist natürlich immer angebracht, ganz klar.

Wir haben sicherlich die Fingerabdruckdateien in Europa, was z.B. Asylbewerber angeht, was aber auch zukünftig die Visaantragsteller angeht und Ähnliches mehr, allerdings hier eben auch nicht eine Speicherung mit der Verbindung, dass das jetzt ein kriminelles Element wäre, sondern letztlich immer als Gegenprüfung. Wer ist denn die Person, die hier nach Europa kommen möchte?

In der Kriminalistik ist auch schon klar geworden, wir dürfen eines nicht vergessen: Es gibt in der Zukunft die Herausforderung nicht mehr nur zu sagen, „*Gut, ich überprüfe jetzt einen Pass oder ein ähnliches Dokument wie ein Personalausweis.*“ Sondern ich verwende natürlich dann auch nach Möglichkeit eine Biometrie, wie einen Fingerabdruck oder ein Gesicht oder eine Iris vielleicht in der Zukunft mal, um die Identität festzustellen. Glauben Sie es oder nicht, in 50-60 % aller polizeilichen Überprüfungsfälle hat die Person gar keinen Ausweis bei sich, warum auch immer. Dann sind Sie heute auf Daten angewiesen, die sehr rudimentär bzw. sehr verteilt liegen. In der Zukunft kann man dann zumindest den Negativfall ausschließen, um den geht es ja hier, dass eventuell der Ulrich Walter, der sich Ihnen hier präsentiert, unter dem Namen Andreas Meier einer der meistgesuchten Schwerverbrecher ist.

Zum Thema Überwachung und Screening zeige ich Ihnen auch gleich noch was. Ich möchte hier gar nicht groß auf Geräte o.ä. eingehen. Ich möchte Ihnen einfach nur zeigen, dass diese Dinge, mit denen wir so etwas aufnehmen können, immer kompakter werden und dass das letztlich auch zum Vorteil der privaten Nutzung sein kann. Was Sie hier beispielsweise in der Mitte sehen, ist ein Fingerabdrucksensor, wie er z.B. auch dem Zugangsschutz zu PCs oder ähnlichen IT-Systemen dienen kann, also, auch hier mal wieder der positive Aspekt der Biometrie.

Eines muss ich zum Thema der Einzel- bzw. Massenüberwachung noch einmal sagen: Was passiert denn in vielen Fällen in der Zukunft an der Grenze durch die Polizeibeamten? Im Prinzip passiert zunächst mal eine 1:1-Überprüfung, die Verifikation, *entspricht ein Gesicht dem anderen oder nicht?* Oder entspricht ein Fingerabdruck dem anderen? Das heißt, hier wiederum Daten, die letztendlich lokal im Dokument auch gespeichert sind, wo man aber dem jeweiligen Beamten eine Unterstützung an die Hand gibt.

In dem Moment, wo Sie eine Datenbank haben, sei sie lokal oder verteilt abgelegt, kann ich dann natürlich eben auch feststellen, ob diese Person hier an erster Stelle letztlich identisch mit einer anderen Person ist, die ich unter einem anderen Namen, darum geht es hier hauptsächlich, eventuell schon kenne und die auf meiner Fahndungsliste liegt. Hier erst komme ich in den Bereich der Massenverdächtigungen bzw. der Massenüberwachung hinein. Das sollte man in der Diskussion immer ganz klar differenzieren.

Jetzt möchte ich Ihnen ganz kurz einmal so ein System zeigen, wie Sie es beispielsweise an Bahnhöfen wie in Mainz gesehen haben, wie es aber auch in Stadien oder Flughäfen und – da beziehe ich mich nicht auf Deutschland, sondern ganz explizit auf das europäische Ausland – international zum Einsatz kommt, um Ihnen einfach mal zu zeigen, wie solche Systeme aussehen. Das Video, was Sie gleich sehen, ist schon ein wenig älter. Das hat nichts mit dem Produkt zu tun, sondern es soll Ihnen einfach mal zeigen, wie Gesichter gefunden werden können bzw. wann auch nur Gesichter gefunden werden können. Da greift dann auch schon eines der Probleme ein, die wir heute ganz klar erkennen müssen. Wir können Gesichtserkennung und damit Videoüberwachung nur dann machen, wenn wir wirklich relativ frontale Aufnahmen der Gesichter haben und solche, auf denen das Gesicht relativ klar zu erkennen ist. Das heißt, wir haben eben nach wie vor – übrigens wenn ich sage *wir*, dann meine ich die Technologielieferanten – Probleme in dem Moment, wo Gesichter gesenkt sind, wo Sie dunkle Sonnenbrillen tragen usw. Wenn man an den Schutz denkt, kann sich das, das war ja bei dem Trojaner auch so, sicherlich sehr schnell verbreiten und die Leute können sich überlegen, wie sie sich auf der Straße bewegen.

Allerdings, wenn man gestern *Planetopia* gesehen hat, dann hat man sicherlich auch die Weiterentwicklung gesehen, wie es in Zukunft dann mit dem Thema 3D-Gesichtserkennung vielleicht einmal aussehen könnte. Ich würde allerdings sagen, das war doch noch relativ bis sehr weit utopisch. Aber auch hier müssen wir sicherlich sehen, wie die Technologie weiter fortschreitet und auch unter welchem Kostenaufwand das Ganze dann möglich wäre.

Zum Schluss möchte ich Ihnen noch zeigen, wie man auch die Privatsphäre schützen kann. Das ist eines unserer ganz wesentlichen Interessen hier. Das bieten wir und das fordern wir auch ganz aktiv. Dass wir nämlich z.B. in Videoaufnahmen, wie sie mit guten Digitalkameras heute sehr gut möglich sind auf großer Entfernung, die Gesichter, die gefunden werden – so wie Sie es gerade eben gesehen haben in dem Bild – nicht kenntlich sind, sondern nur dann kenntlich werden, wenn eine Person wirklich z.B. in einer Datenbank gesucht ist. Wenn Sie jetzt mal verfolgen, dann sehen Sie links den ungefilterten Videoteil und rechts werden die Gesichter anonymisiert, das heißt, solange jemand nicht wirklich irgendwo gesucht wird oder in der Datenbank hinterlegt ist, wird er auch anonymisiert abgespeichert. Das ist wirklich bereits heute in der Kameratechnologie machbar. Hier gehen wir erst gar nicht rein und würden das irgendwo speichern, sondern nur in dem Fall, wo eben wirklich bereits ein Anhaltspunkt vorliegt.

Zum Schluss ein kleiner Ausblick: Diese Themen Biometrie, Vernetzung von Telekommunikationsdaten, Speicherung, Vorratsspeicherung und all das kann man natürlich in Ermittlungssystemen verwenden. Die bayrische Polizei ist hier ein Vorreiter in der Einführung eines solchen Systems namens ERIS Case, wo Sie tatsächlich Netzwerkdigramme und Ähnliches schaffen können. Aber auch hier muss man ganz klar fragen: Wo wird es denn wirklich eingesetzt und in welchen Fällen?

Ich kann Ihnen sagen, es wird sehr, sehr begrenzt eingesetzt und auf ganz, ganz wenigen Rechnern, vor allem aber auch immer durch geschulte Beamte, die entsprechend qualifiziert sein müssen, um überhaupt mit so einem Tool umgehen zu können. Das ist nichts, was der Polizist im kleinen Ort verwenden würde, sondern das sind zentrale Systeme, wie sie wirklich nur in einzelnen Fällen zum Einsatz kämen.

Silke Stokar

Dank an Sie. Eine Bemerkung möchte ich machen. Die Sicherheitstechnik *made in Germany*, die global durchaus wettbewerbsfähig ist, wird ja nicht nur in Deutschland angeboten. Hier stellt sich für mich die Frage der Ethik und sogar die Frage, ob man nicht ähnlich wie im Bereich der Rüstungskontrolle hier über ganz andere Dinge nachdenken muss. Innerhalb der EU werden ja andere Dinge ausprobiert. Der Mainzer Bahnhof ist das eine. Der Flughafen in Ungarn zeigte ja schon einmal die Möglichkeiten der Totalüberwachung von Fluggästen mit Aushändigung des Tickets. Sie wurden durch den Duty Free Shop zum Klo begleitet. Ihnen wurde dann auch gesagt: „Jetzt müssen Sie aber zum Flieger, sonst startet der nicht pünktlich.“ Die Möglichkeiten der vernetzten Anwendung werden nicht in Deutschland gezeigt. Die Technik wird aber hier entwickelt. Ganz schwierig wird es natürlich, wenn solche Techniken weiterverkauft werden in Staaten, wie Weißrussland oder andere, die deutsche Sicherheitstechnik nutzen, um Minderheiten und die Opposition in Diktaturen zu überwachen. Das ist eine Dimension einer Diskussion, die wir hier bisher noch viel zu wenig führen, die aber sicherlich geführt werden muss.

Meine Damen und Herren, Sie haben jetzt die Möglichkeit, Fragen zu stellen oder eine Stellungnahme abzugeben.

Fragen und Beiträge aus dem Auditorium

Christian Rath – TAZ

Ich habe zwei Fragen. Die erste geht an den Chaos Computer Club: Jenseits der Überwachungsfrage habt ihr ja auch das Thema aufgeworfen, dass Dinge reingeschmuggelt werden können in den Computer, die da vorher nicht drin sind. Das ist ja noch einmal ein separates Problem. Was ist jetzt hier die neue Qualität gegenüber einer normalen Hausdurchsuchung, wo ja auch ein Polizist meinen Schrank anguckt und dort mit Handschuhen z. B. eine Waffe unter die Socken schieben könnte? Das ist ja bisher möglich, kommt relativ selten vor, die Frage ist: Ist die Polizei automatisch moralisch schlechter, nur weil sie jetzt mit Computern arbeitet?

Die zweite Frage geht an Herrn Helmbrecht: Sie haben ja nun beide Seiten im Blick, so die Überwachungsseite, aber auch die Vielfalt der neuen Kommunikationsmöglichkeiten. Herr Ziercke hat im Interview gesagt: „Wir holen ja nur auf.“ Die Verbrecher nutzen die neuen Kommunikationsmöglichkeiten und wir versuchen hinterherzukommen. Würden Sie jetzt, wenn man das auf die letzten 50 Jahre betrachtet, sagen, dass die Freiheitsmöglichkeiten oder die Überwachungsmöglichkeiten gestiegen sind für die Gesellschaft?

Ricardo Christof Remmert-Fontes – AK Vorratsdatenspeicherung

Meine Frage ist eher erstmal eine ethische Frage. Ich höre immer wieder hoheitliche ID, zentrale Datenbanken, Personenkennziffer, Vorratsdatenspeicherung. Es gibt in der Geschichte einfach Beispiele von Datenmissbrauch. Es gibt eine ganz einfache klare Intention des Grundgesetzes, nämlich Datenvermeidung und auch der Wille dazu formuliert im Grundgesetz und in anderen Gesetzgebungen, möglichst wenig Daten zu speichern und möglichst wenig Daten zentral zu speichern. Das ist ganz wichtig für unsere Konstitution, für unsere Verfassung. Dazu würde ich gerne noch mal etwas hören von den Referenten, Herrn Helmbrecht und von Herrn Walter als Technologievertreter. Danke.

Constanze Kurz – Chaos Computer Club

Wodurch unterscheidet sich die Online-Durchsuchung von der normalen Hausdurchsuchung?

Der Name suggeriert hier möglicherweise einen Zusammenhang, de facto besteht aber keiner. Die Online-Durchsuchung ist im Gegensatz zur Hausdurchsuchung eine verdeckte Ermittlungsmethode. Entsprechend erfahren Sie als Computernutzer natürlich nicht, dass Sie ausspioniert wurden. Im Vergleich dazu findet die Hausdurchsuchung nur unter Zeugen statt. In der Regel klingelt der Ermittlungsbeamte an der Tür. Man lässt ihn ein. Man kann sich einen Zeugen holen und selbstverständlich wird die Hausdurchsuchung auch protokolliert und das Protokoll bekommt derjenige, dessen Haus durchsucht wird, auch ausgehändigt.

Ganz anders die Online-Durchsuchung. Sie ist aber auch nicht nur verdeckt, sondern auch eine dauerhafte Maßnahme, weil das Spähprogramm selbstverständlich nicht für eine Stunde auf dem Rechner installiert wird, sondern als dauerhafte Maßnahme weiter genutzt werden kann. Es ist also eine verdeckte, heimliche und dauerhafte Maßnahme. Das sind die größten Unterschiede zur Hausdurchsuchung. Nur der Name ist hier ähnlich, vom Verfahren her besteht eigentlich kein Zusammenhang.

Einwurf Herr Rath: Die Frage war eine andere – das Missbrauchspotenzial. Natürlich kann ich dabeistehen, aber wenn da vier Polizisten in meiner Wohnung sind, würde es ein gewiefter Polizist sehr wohl schaffen, mir eine Waffe unter die Socken zu stecken.

Ich weiß nicht, ob Sie schon mal bei einer Hausdurchsuchung dabei waren. In der Regel ist es so, dass die ausführenden Beamten tatsächlich nur die Sachen, die sie beschlagnahmen wollen, beschlagnahmen und das notieren. Ein gewisses Missbrauchspotenzial gibt es natürlich schon. Die Beamten, die ich bisher bei Hausdurchsuchungen getroffen habe, hätten nicht mal gewusst, wie sie den Computer anmachen. Sie geben ihn nur zur weiteren Analyse ab.

Das Missbrauchspotenzial ist bei einer Online-Durchsuchung ein ganz anderes, weil selbstverständlich diejenigen, die einen individualisierten Trojaner auf einem auszuspiönierenden Rechner installieren, ein weit höheres Fachwissen haben.

Außerdem gibt es, wenn es die Polizisten vor Ort machen, die direkte Gefahr der Aufdeckung, dass diese Personen strafrechtliche Konsequenzen befürchten müssen. Wohingegen es, wenn es online passiert, sehr schwierig wird nachzuweisen sein, welche Person das gewesen ist, die dort eventuell Beweismaterial auf dem Rechner platziert hat.

Wolfgang Wieland

Ich habe noch eine Anschlussfrage an Christian Rath. Wenn es so relativ einfach ist...

(Gelächter)

... Ich knüpfe an eine Frage an und frage natürlich auch die ehrenwerten Mitglieder des Chaos-Computerclubs, von mir aus frage ich auch dich, Jerzy, als Rechtsexperten: Wenn es so einfach ist, mit Trojanern alles auf Rechner zu bekommen, welchen Beweiswert hat es dann überhaupt noch, dass ich Kinderpornographie auf meinem Rechner habe, wenn der sonst woher gekommen sein kann?

Also braucht es nicht nur den bösen Polizisten, sondern kann es auch sonst jemand sein, der mir Übel will und mir das auf die Festplatte verpflanzt?

Jörg Ziercke

Zur Klarstellung: Es hat bisher noch keine Online-Durchsuchung des BKA oder der Polizei in Deutschland gegeben. Es gibt auch keine Rechtsgrundlage. Eine Rechtsgrundlage muss natürlich so beschaffen sein, dass ein Ermittlungsrichter die Maßnahme beschließt. In diesem Beschluss wird auch der Zeitraum festgelegt. Eine Maßnahme auf Dauer kann es aus Verhältnismäßigkeitsgründen nicht geben.

Im Übrigen zum Manipulationsvorwurf: Etwa bei Gefahr im Verzug – das haben Sie sicher schon mal gehört – muss gem. § 105 StPO niemand zwingend dabei sein, wenn Sie die Wohnung durchsuchen. Insofern bestünde bei jeder Hausdurchsuchung theoretisch die Möglichkeit, jemandem etwas unterzuschieben, wie das hier gesagt wurde. Ich kenne aus meiner 40-jährigen Praxis keinen solchen Fall in Deutschland, um es ganz klar zu sagen. In Amerika hat es das erste Verfahren gegeben, wo ein Anwalt behauptet hat, man habe seinem Mandanten – das war ein US-Offizier – kinderpornographisches Material auf den Computer manipuliert. Man hat dann tatsächlich die Manipulation datentechnisch nachweisen können.

Einwurf Herr Krissler: Dann haben sie sich blöd angestellt.

Udo Helmbrecht

Ich kann das nicht im Hinblick auf mehr Freiheit oder mehr Überwachung beantworten, ich kann es nur hinsichtlich der verfügbaren Technologien beantworten. Das ist das, was dieses Schaubild mit der Grafik auch zeigte. Wir erleben einfach, dass mit der fortschreitenden Technik diese Technik auch in diesem Umfeld von Schadprogrammen missbraucht wird. Was vor zehn Jahren an Viren und Würmern auf Disketten war, kommt heute per E-

Mail. Insofern ist es eine Technologisierung dessen, was wir erleben. Das ist das, was ich auch ausdrücke, dass – sobald man mit diesen Dingen wie Spam Geld verdienen kann – damit auch diese Spams missbraucht werden, um Schadprogramme zu verschicken und sozusagen die Technik die treibende Kraft an der Stelle ist. Unsere Herausforderung ist, dem immer entgegenzuhalten und neue Abwehrmechanismen zu entwickeln.

Das andere war die Frage nach der Ethik. So weit will ich da gar nicht gehen, ich will nur die Motivation darstellen, warum – jetzt kommen Pass und Personalausweis – das getan wird und worin auch sicherlich die Herausforderung liegt.

Wenn Sie sich den Pass oder den Personalausweis nehmen, dann hat er über seine Entwicklung immer ein höheres Sicherheitsniveau erlangt. Wenn Sie Ihren Personalausweis heute anschauen, werden Sie unterschiedliche Personalausweise haben, weil je nach dem da schon gewisse Sicherheitsmerkmale drin sind. Wenn Sie sich Geldscheine anschauen, haben die auch immer weitere Sicherheitsmerkmale.

Der Punkt, wo die Diskussion einsetzt, ist, dass wir heute sagen: Zur Erhöhung des Sicherheitsniveaus setzen wir RFID-Chips ein und speichern gewisse Daten da drauf. Mit dieser neuen technischen Qualität diskutieren wir auch darüber, wie wir das dann an der Stelle sicher machen. Aber für uns als BSI ist die Herausforderung: Mit dieser technischen Entwicklung und neuen Sicherheitsmerkmalen, die zusätzlich in diese Dokumente hineinkommen, wollen wir auch die Sicherheit im Sinne von IT-Sicherheitsmerkmalen mit hineinbringen.

Ulrich Walter

Ich greife die Frage nach der Massendatenspeicherung, Vorratsdatenspeicherung aus der ethischen bzw. aus der Systemfrage heraus auf. Ich ziehe mich ein bisschen aus der Schlinge, weil wir letztlich nicht darüber entscheiden, was, wie, wann, wo gespeichert wird.

Einwurf Herr Krissler: Das hat IBM auch nicht vor 60 Jahren.

Gut, ob wir jetzt eine Karriere wie IBM machen, lassen wir dahingestellt. Ich kann es nur insoweit beantworten, dass das eine politische Vorgabe bzw. eine Vorgabe durch die jeweiligen Behörden ist. Wir als Unternehmen und Technologielieferanten und -hersteller, gehen in unseren Systemen natürlich so weit, dass wir sehen, je weniger Daten, desto besser, weil wir dann natürlich zum einen auch schneller Ergebnisse liefern können. Da ist die Rechenleistung in vielen Fällen heute noch begrenzt, das ist ganz klar. Zum anderen schaffen und bieten wir aber auch gewisse Filtermöglichkeiten an, die eben genau das verhindern, dass von jedem die Daten gespeichert werden – wenn, dann schon anonymisiert. All das ist machbar und eine Option, aber über den Einsatz können wir in dem Sinne wirklich nicht entscheiden.

Silke Stokar

Ich stelle noch eine Frage zu RFID: Mich hat eine Meldung elektrisiert, dass das kanadische Parlament zur Zeit einen Gesetzentwurf – Verbot von RFID-Chips in Identifikationskarten – berät, weil sie sich als unsicher herausgestellt haben und weil in den USA die Bewertung des ersten Versuches mit den zwei flach aufgelegten Fingerabdrücken zu einem verheerenden Ergebnis kommt. Die USA entscheiden für ihre Bürgerinnen und Bürger, auf gar keinen Fall solche Dokumente einzuführen, weil das – für mich war es auch ein neuer Begriff – Thema *Identitätsdiebstahl* eine immer größere Bedeutung gewinnt. Es gibt Zahlen: 6 Mrd. Dollar Schäden durch Identitätsdiebstahl, auch durch die sehr unterschiedliche Verwendung verschiedener Fingerabdruckscanner. Das heißt, je öfter ich in

unterschiedlichen Bereichen meinen Fingerabdruck irgendwo hingeb, desto schneller wird er ausgelesen, kopiert, geklont, was auch immer. Auf jeden Fall scheint das ja mittlerweile dort, wo das eingesetzt wird, schon ein Riesenproblem zu sein.

Warum führen wir einen Ausweis ein, um in die USA zu reisen, während die USA selber erklärt, das Ding ist so unsicher, dass wir es unseren Bürgerinnen und Bürgern nicht zuzumuten wollen? Das ist für mich völlig unverständlich, ein völliger Widerspruch.

Grietje Bettin

Zwei Fragen: Herr Prof. Pfitzmann, Sie hatten ja diese provokative These vorgetragen, dass wir die Überwachungsschnittstellen am besten wieder ausbauen sollen. Das finde ich natürlich sehr reizvoll, aber ich teile doch eher die Einschätzung, dass eine globale technische Entwicklung durch nationale Regelungen nicht aufzuhalten ist. Ich glaube, dass wir uns hier in einer Art des technischen Wettrüstens befinden, die globale Antworten braucht. Als nationaler Gesetzgeber sind wir da immer ein bisschen in der Bredouille, wenn wir sagen: „*Informationelle Selbstbestimmung ist für uns ein hohes Gut.*“ Wie lösen Sie dieses Spannungsfeld mit Ihrer These auf?

Die zweite Frage an Herrn Helmbrecht zum Stichwort digitale Signatur: Sie hatten das in einem Nebensatz angedeutet, dass das durchaus Schutz bieten kann.

Nun ist die Durchsetzung, was den Verbraucher angeht, relativ schwierig. Was können wir hier tun, um die Bereitschaft der Verbraucher zu erhöhen, sich diesem Thema anzuschließen. Wir kriegen tausend Bürgerbriefe „*Spam und alles ist ganz schrecklich.*“ Das wäre ja eine Möglichkeit, die aber natürlich ein bisschen schwieriger ist, als uns einfach mal kurz eine Mail zu schicken.

Jerzy Montag

Eine kurze Bemerkung und eine technische Nachfrage in der gleichen Richtung wie die Kollegin Stokar sie auch schon gemacht hat.

Das Verfälschen und das Unterschieben von Beweismitteln ist uns natürlich seit Jahrzehnten bekannt. Es ist strukturell überhaupt nichts Neues. Eine neue Struktur könnte sich allerhöchstens aus der technischen Perfektion ergeben. Natürlich sind einzelne Polizeibeamte gegenüber so einem Verdacht auch nicht sakrosankt. Auch wenn ich natürlich zugebe, dass das absolute Ausnahmefälle sind, es ist alles denkbar. Deswegen muss man sich schon darüber Gedanken machen, ob diese neue technische Möglichkeit der technischen Perfektion uns nicht zu noch mehr Vorsicht anleiten sollte.

Meine Frage an Sie, Herr Walter: Wenn ich also jetzt einen Reisepass oder Personalausweis habe, wo mein Fingerabdruck in einer digitalen Form gespeichert ist und ich damit in jedes beliebige Land der Welt reisen kann, einige davon ohne rechtsstaatliche Strukturen und mit durchaus struktureller Kriminalität und Korruption versehen, dann besteht doch die ganz reelle Gefahr, dass bereits bei der Vorlage des Reisepasses an der Grenze dieser Fingerabdruck in digitaler Form abgelesen wird und dann genau zu dem benutzt wird, was Sie uns als *individuelle Sicherheit* dargeboten haben, dass nämlich dann mit diesem Abdruck, genau mit dem Print das gemacht werden kann, mit meinen Daten, mit meinen Konten, mit meinem Computer, was verhindert werden soll.

Was ist technisch von Ihrer Firma angeboten, dass eine solche Ablesung unterbunden wird?

Herr Jünemann – Deutscher Richterbund

Meine Frage geht in eine ähnliche Richtung an Herrn Prof. Pfitzmann:

Welche Sicherheiten, welche technischen Beweismittel gibt es dafür, dass ich sicher sein kann, welche Person ein technisches Gerät benutzt hat – egal, ob es ein Handy, ein Computer oder sonst irgendetwas ist? Ich weiß ja üblicherweise nur, dass dieses technische Gerät irgendwelche Signale ausgesandt oder transportiert hat, kenne aber den eigentlichen Benutzer dieses Gerätes nicht.

Wie stellt man das eindeutig und bitte auch gerichtsfest fest? Danke.

Herr Schallaböck – Landeszentrum für Datenschutz, Kiel

Meine Frage richtet sich auch an Herrn Helmbrecht. Ich bin gerade etwas hellhörig geworden. Sie sagten, die biometrischen Ausweise dienen dem Sicherheitsgewinn. Wir haben zwei Kernkomponenten darin. Das eine ist die Biometrie, das andere ist der RFID-Chip.

Ich frage mich jedes Mal, was eigentlich der Sicherheitsgewinn ist. Wenn ich mit der Biometrie anfangen, dann habe ich doch zusätzlich zur normalen Identifizierung anhand des Fotos, das darauf abgedruckt ist, noch ein weiteres Merkmal, z.B. den Fingerabdruck. Das heißt, es ist ein Gewinn an zusätzlichem Sicherheitsrisiko. Ich komme jetzt auch durch die Grenze, wenn ich den Computer damit überliste, dass er glaubt, *das sei der Fingerabdruck*, während ich vorher nur die Möglichkeit hatte, den Grenzbeamten mit dem Foto zu überlisten. Ich muss immer diese zwei Strukturen ausbilden. Nur allein über den biometrischen Fingerabdruck können wir nicht gehen, weil wir wissen, dass die Technologie nicht gut genug dazu ist. Und dass es eine Menge Leute gibt, die diese Sicherheitsmerkmale nicht aufweisen, weil z.B. die Hände kaputt sind oder weil sie blind sind. Das heißt, wir müssen sowieso immer noch eine Sicherheitslücke der normalen Identifikation offen lassen.

Das zweite Element des biometrischen Ausweises ist der RFID-Chip, dessen wesentliche Eigenschaft es ist, dass er eine Funktechnologie hat. Was ist jetzt der Sicherheitsgewinn, wenn wir Daten über Funk übertragen, anstatt sie direkt abzulesen? Da können dann doch Dritte intervenieren, d.h. den Funk abhören. Das scheint mir also auch ein Verlust von Sicherheit zu sein.

Ruth Weinzierl – Deutsches Institut für Menschenrechte

Heute wurde im Rahmen der Vorträge darauf hingewiesen, dass man überprüfen müsste, wie die Kumulation verschiedener Datenerhebungsnetzwerke – eine Forderung, die auch das Bundesverfassungsgericht an den Gesetzgeber gestellt hat – nämlich die Kumulation der verschiedenen Eingriffsmöglichkeiten zu beobachten und ggf. die Gesetzgebung nachzubessern, wenn die Eingriffsintensität zu hoch wird – daher auch eine gewisse Evaluierungspflicht an bestimmten Punkten.

Mich würde interessieren, inwieweit dies bedacht wird und wie sich die Kumulation verschiedener Überwachungsmöglichkeiten auf den Einzelnen auswirkt. Vielleicht gibt es hierzu auch Ideen vom Chaos-Computer-Club.

Jörg Ziercke

Ich beantworte die Frage zur Kumulation, die eben gestellt worden ist. Man muss sich das so vorstellen, dass die Polizei einen Instrumentenkasten benötigt, um in den verschiedensten Fragen der Schwerestrafkriminalität situationsabhängig das richtige Instrument einsetzen zu können. Beispielsweise unterscheiden sich im Bereich des Terrorismus Al-Kaida-Strukturen von ggf. organisationsungebundenen Suizidattentätern oder von fanati-

sierten Einzeltätern oder von Homegrown-Terroristen. Und ergänzend zur OK-Kriminalität: Im Bereich Waffen hat man ein anderes phänomenologisches Spektrum als beim Menschenhandel, bei der Schleusungskriminalität oder sonst wo.

Ich will es mal mit einem Arzt vergleichen. Ein Neurochirurg kann nicht mit den Instrumenten des Orthopäden operieren. Oder der Augenarzt kann Ihnen nicht mit den Apparaturen des Zahnarztes helfen. Ähnlich ist es bei der Gefahrenabwehr und Strafverfolgung im Grunde auch. Sie müssen für den konkreten, in seiner Ausgestaltung jeweils spezifischen Fall ein konkretes Eingriffsinstrumentarium haben, unabhängig davon, wie oft Sie es tatsächlich anwenden. Nur es muss im Einzelfall bei schwerster Kriminalität erfolgreich sein können. Mir sind keine Fälle bekannt, wo in dem Maße kumulativ parallel Maßnahmen eingesetzt wurden, ohne dass die einzelne Maßnahme geprüft wurde, die weniger eingriffsschwer war. Selbstverständlich kann es vorkommen, dass mehrere Instrumente in einem Fall eingesetzt werden, aber der Regelfall ist das nicht. Dies gebietet der Grundsatz der Verhältnismäßigkeit; im Übrigen war diese Thematik bereits Gegenstand einer bundesverfassungsgerichtlichen Entscheidung, die die polizeiliche Praxis in dem konkreten Fall für verfassungsrechtlich unbedenklich befunden hat.

Ulrich Walter

Zu der Frage von Herrn Montag. Herr Montag, Sie hatten Bedenken, dass repressive Staaten, z.B. die sog. Schurkenstaaten die Technologie in den neuen Pässen missbrauchen könnten. Ganz ausschließen lässt sich ein Missbrauch gegenwärtig sicherlich nie. Andererseits trägt das Zusammenspiel von Biometrie und RFID-Chip schon jetzt und langfristig auch die Entwicklung des sog. „lebendigen Fingerabdrucks“ zu einem erheblichen Sicherheitsgewinn bei. Den „lebendigen Fingerabdruck“ haben wir aber gewiss erst in fünf Jahren.

Dr. Udo Helmbrecht

An mich ist die Frage nach den Digitalen Signaturen gestellt worden. Das ist wie das „Henne-und-Ei“-Prinzip. Oft ist es den Bürgern nichts wert, sich ein Gerät für die digitale Signatur zu kaufen. Zeitgleich bedauern sie, dass es nicht genügend Sicherheit im Netz gibt. Die Frage stellt sich: Wieviel ist man bereit, für Sicherheit zu bezahlen? Stichwort „Online-Banking mit TAN anstatt mit Digitaler Signatur und Kartenlesegerät“. Viele Gebrauchsmöglichkeiten sind da schlicht bequemer für den Verbraucher, auch wenn sie mit einem Sicherheitsverlust einhergehen.

Andreas Pfitzmann

Kriminelle mögen kriminell sein, aber die sind nicht dümmer als wir. Viele davon sind vielleicht sogar hochintelligent. Kriminelle passen sich viel mehr an und schauen, wie sie sich verhalten sollen und was die Polizei machen kann. Das aber tut der brave Bürger nicht. Kriminelle können hingegen den meisten Maßnahmen ausweichen. Selbst wenn wir die Vorratsdatenspeicherung in der EU für ewige Zeiten machen würden – ohne Weltstaat bringt das nichts. Kriminelle kommunizieren dann trotzdem um Europa herum. Man wird mit solchen Maßnahmen nur brave Bürger und dumme Kriminelle finden.

Stellen Sie sich vor, wir haben Häuser, die so unsicher sind, dass sie nach Rückkehr nicht feststellen können, ob sie jetzt einmal, zweimal oder gleich dreimal besucht wurden. Nehmen wir an, da gibt es Schränke drin, die durchsucht werden. Stellen Sie sich eine Welt vor, wo Sachen in diese Schränke in diesen Häusern hineingetan und herausgenommen werden können und Sie können nicht feststellen, wo was ist. In so einer Welt würden man andere Häuser bauen, wo man transparent feststellen kann, ob da jemand drin war oder nicht. Es ist eine völlig falsche Diskussion, diese Diskussion über den Bundes-

trojaner. Man braucht stattdessen eine Diskussion über minimale Standards bei der IT-Sicherheit.

Ich habe keine Angst vor dem BKA oder deutschen Geheimdiensten. Die sind nicht besonders gefährlich. Da gibt es viel gefährlichere Geheimdienste im Ausland. Aber wenn wir Infrastrukturen schaffen, die es anderen möglichst einfach macht, dann ist es ein Problem.

Ich danke ja der Bundesrepublik und dem BSI, die sich Mühe geben, dass die RFID-Pässe so sicher wie möglich realisiert werden und die sich viel mehr darum kümmern, als andere auf der ganzen Welt. Aber das ist nicht das Problem. Das eigentliche Problem ist, dass Bürger daran gewöhnt werden, ihren Fingerabdruck ständig abzugeben.

Wir brauchen endlich sichere Rechner. Also nicht „Microsoft Windows Irgendwas“, eine Wohnung wo jeder rein kann, wann und wie er will.

Herr Jünemann, die Gestaltungsdiskussion über die Techniknutzung führt aus meiner Sicht in die falsche Richtung. In weniger demokratischen Staaten werden die Fingerabdrücke von braven Deutschen ohne Probleme dann an der Grenze hinterlassen.

Forum 2: Technische und rechtliche Herausforderungen der Entwicklung

Moderation: Jerzy Montag MdB, rechtspolitischer Sprecher

Ich begrüße Sie nach der Pause ganz herzlich zum zweiten Teil unserer Veranstaltung. Wie uns mehr als deutlich vor Augen geführt wurde: Die Entwicklung auf der technischen Seite wird nicht mehr aufzuhalten sein. Von Herrn Walter weiß ich jetzt, dass man bei der Videoüberwachung das Einscannen der Gesichter dadurch verhindern kann, dass man sich verschleiern, das Gesicht senken oder gebückt läuft. Wir wollen aber nicht in einer Gesellschaft leben, in der wir gebückt herumlaufen müssen.

Es stellt sich also die Frage, welche rechtlichen Vorgaben wir haben und welche rechtlichen Antworten wir auf die skizzierte Entwicklung der Technik geben können. Deshalb übergebe ich das Wort jetzt an Herrn Professor Roßnagel, der uns zu den verfassungsrechtlichen Vorgaben vorträgt.

Prof. Dr. Alexander Roßnagel

wissenschaftlicher Direktor des Instituts für europäisches Medienrecht, Saarbrücken, und des Forschungszentrums für Informationstechnik-Gestaltung, Universität Kassel

Ja, vielen Dank. Ich werde Ihnen meinen Vortrag anhand von Folien verdeutlichen. Er trägt den Titel der Veranstaltung: „Bürgerrechte im Digitalen Zeitalter – technische und rechtliche Herausforderungen“. Aus Sicht der Verfassung ist das Thema der Bürgerrechte ein doppelbödiges und spannungsgeladenes Thema.

Einerseits geht es um den Schutz des Bürgers durch den Staat. Dieser ist verfassungsrechtlich zum Schutz aller Grundrechte verpflichtet. Er muss sich im Rahmen der Strafverfolgung und bei der Gewährleistung innerer Sicherheit für den Schutz der Grundrechte einsetzen. Selbstverständlich verbleibt ihm für die Erfüllung dieser Schutzpflicht ein gewisser Spielraum, innerhalb dessen er auch andere verfassungsrechtliche Aufgaben zu berücksichtigen hat. Die Grenze ist allerdings stets das Untermaßverbot. Er darf die Grundrechte nicht faktisch schutzlos stellen.

Andrerseits geht es um den Schutz des Bürgers vor dem Staat. Die Abwehrfunktion gegen die Macht des Staates ist die älteste und wichtigste Funktion aller Grundrechte. Verfassungsrechtlicher Ausgangspunkt ist der Vorrang für die Freiheit vor einem Eingriff. Eingriffe in Grundrechte bedürfen daher der Rechtfertigung. Die Begrenzung staatlicher Macht zugunsten der Freiheit ist die vornehmste Aufgabe von Grundrechten und Rechtsstaat.

Beide Aufgaben des Staates, Schutz der Grundrechte und Freiheit zur Grundrechtsausübung zu gewährleisten, können in Konflikt geraten. Daher kann die Freiheitsausübung beschränkt werden, wenn dies zum Schutz der Grundrechte anderer erforderlich und verhältnismäßig ist, und müssen die Schutzmaßnahmen zugunsten von Grundrechten berücksichtigen, dass sie möglichst nicht oder allenfalls im unabdingbaren Umfang in Freiheitsrechte eingreifen. Im Ergebnis und dem Wesen und Sinn der Grundrechte entspre-

chend geht der Schutz des Bürgers vor dem Staat dem Schutz des Bürgers durch den Staat regelmäßig vor.

Nun komme ich – wie Sie auf der Folie sehen – zu den drei Dilemmata des Bürgerrechtsschutzes vor dem Hintergrund der technischen Entwicklung:

Das erste Dilemma betrifft die Dringlichkeit des Konkreten und Aktuellen. Konkrete und aktuelle Bedürfnisse werden unmittelbar erfahren und verdrängen auf Grund dieser Eigenschaften leicht andere vernünftige Erwägungen. Abstrakte, zukünftige oder langfristige Überlegungen finden in der praktischen Gestaltung des Bürgerrechtsschutzes keinen Eingang. Stattdessen wird auf Tagespolitik reagiert. Kumulative, synergistische oder latente Risiken werden nicht mitbedacht. Ein schönes Beispiel dazu – wir hatten es heute schon – sind die Mautdaten. Sie waren allein für den Zweck des Zahlungssystems der Maut gedacht. Nun wird darüber diskutiert, die vorhandenen Daten oder auch das vorhandene System zur Datenerfassung anderweitig – zu Zwecken der Strafverfolgung – einzusetzen.

Wie begegnen wir rechtlich diesem Dilemma? Notwendig ist vor allem, dass wir das Wissen über langfristige, synergistische und latente Risiken sowohl in die Forschungspolitik und die Technikentwicklung als auch in den Gesetzgebungsprozess einbringen. Der Gesetzgeber muss die beiden großen Prinzipien des Datenschutzes – Zweckbindung und Datensparsamkeit – immer wieder verankern und durch die Gestaltung der Systeme zu gewährleisten. Man muss versuchen, rechtsstaatliche Prinzipien so gut es geht langfristig zu sichern. Nur dann hat man eine Chance, dass die dann eine Hilfestellung bieten, wenn man im Konflikt mit konkreten aktuellen Bedürfnissen diese längerfristigen abstrakten Risiken vermeiden will.

Das zweite Dilemma ist die selbständige Ausweitung der Befugnisse durch die Fortentwicklung der Technik. Abstraktgehaltene Eingriffsbefugnisse erweitern sich von selbst zum einen dadurch, dass die technischen Überwachungsmöglichkeiten zunehmen, zum anderen aber auch dadurch, dass die technischen Anwendungen immer mehr Lebensbereiche und diese immer intensiver erfassen. So war ursprünglich die Telekommunikationsüberwachung nur auf die Erfassung der Sprachkommunikation und die Telefonnummern beschränkt. Inzwischen können etwa bei der Internetkommunikation unterschiedliche Dienste, einzelne Suchschritte und die Orte der Kommunikation erfasst werden. Zugleich hat sich die Kommunikation auf viele weitere Felder des sozialen Lebens ausgeweitet.

Ich denke, man kann sich da etwas dadurch behelfen, dass man die Befugnisse nicht technikneutral, sondern technikbezogen formuliert. Dies entspricht nicht dem modernen Trend der Technikregulierung, das ist mir vollkommen klar. Aber es entspricht dem vom Bundesverfassungsgericht eingeforderten Bestimmtheitsgrundsatz, der ermöglichen soll, dass die staatlichen Behörden in der Ausübung ihrer Tätigkeit konkret kontrolliert werden können sollen. Und es ermöglicht bei einem Fortschreiten der Technik immer wieder eine politische Entscheidung, ob man diese weitere Ausweitung des Überwachungsbereichs noch haben will oder nicht. Es findet dann zumindest kein rechtlich unterstützender Automatismus von Befugnisausweitungen durch die Technik statt, sondern diese Befugnisausweitung findet durch die Politik statt. Da gibt es dann jemanden, der dafür verantwortlich ist, der das verhindert oder befürwortet. Es findet aber nicht einfach so statt, nur weil neue technische Maßnahmen eingeführt werden.

Das dritte Dilemma betrifft die Falle des technischen Fortschritts, die darin besteht, dass jede neue technische Anwendung im Regelfall zugleich das Überwachungspotenzial erhöht. Zunehmender Nutzen und steigende Bequemlichkeit durch neue Informations- und Kommunikationstechnik bedeutet immer auch weiter Ausbau der technischen Überwa-

chungsinfrastruktur. Daher muss man versuchen, das Nutzpotenzial vom Überwachungspotenzial der Technik zu entkoppeln. Das geht nur dadurch, dass man entsprechende Technik entwickelt oder die Technik entsprechend gestaltet, so dass mehr Datenschutz, mehr Vertraulichkeit und mehr Identitätsmanagement ermöglicht wird. Da gibt es Möglichkeiten. Ich überlasse es aber den Technikern, diese im Detail zu beschreiben. Man kann das, man braucht dafür aber entsprechende Technikforschung und -gestaltung. Insofern ist Rechtspolitik an der Stelle absolut eng mit Forschungspolitik gekoppelt.

Wenn man sich jetzt überleget, wie man die technische Entwicklung mit dem Schutz der Bürgerrechte und dem Thema, das wir heute haben – mit Strafverfolgung und Ermittlungsmaßnahmen – in Einklang bringen kann, dann kann man an die abstrakten Ausführungen, die ich bei meiner ersten Folie gemacht habe, anknüpfen. Die Grundrechte und die Verfassung fordern Freiheit für den Normalfall und erlauben deren Einschränkung nur als Ausnahmefall. Wenn man das zur Grundlage nimmt, dann kann man sich für die technische Entwicklung am Normalfall orientieren. Das heißt, die Technik soll in ihrer Architektur und in ihrer Infrastruktur so aussehen, wie es notwendig ist, um die gewünschten sozialen Funktionen zu erbringen. Das heißt, in der Telekommunikation müssen die Daten verarbeitet werden, die für Telekommunikation notwendig sind. Und wenn sie für Telekommunikation nicht oder nicht mehr notwendig sind, sollte man sie auch löschen. Insofern ist also den Ausbau der technischen Infrastruktur am Normalfall, am Alltag und nicht am seltenen Extremfall der Überwachung zu orientieren.

Dagegen spricht jetzt die Regelung der Richtlinie der Europäischen Gemeinschaft zur Vorratsdatenspeicherung, weil man da den Extremfall, dass auf diese Daten irgendwann mal zur Lösung eines kriminalistischen Problems zurückgegriffen werden soll, zur Grundlage für den alltäglichen Umgang mit diesen Daten macht. Man speichert also von allen Personen alle Verkehrsdaten – immer und nicht dann, wenn sie für spezielle Überwachungsmaßnahmen notwendig sind.

Umgekehrt – wenn man Überwachungsmaßnahmen nur für den Ausnahmefall zulassen will – muss man dann aber für diesen Ausnahmefall effektive Maßnahmen finden, die es ermöglichen, punktuell, aktuell gegen konkrete Personen vorzugehen, die man im konkreten Verdacht hat, eine Straftat begangen zu haben oder zu begehen. Das Entscheidende ist, dass man durch so ein Verständnis von technischer Entwicklung und Überwachungsmaßnahmen eine massentaugliche Überwachungsinfrastruktur vermeiden können sollte. So kann man eine auf konkret Betroffene bezogene Überwachungsmaßnahme erlauben und technisch ermöglichen, die dann auch viel, viel besser nachprüfbar ist.

Wenn man sich dann überlegt, wie diese punktuelle konkrete Überwachung durchgeführt werden kann, dann kann man in der Rechtsprechung des Bundesverfassungsgerichts in den letzten fünf Jahren ganz umfangreich fündig werden, weil sehr viele dieser modernen Überwachungsmaßnahmen jetzt beim Bundesverfassungsgericht einer verfassungsrechtlichen Probe unterzogen wurden.

Das Bundesverfassungsgericht hat eine Reihe von wichtigen Aspekten für seine Entscheidungen herangezogen, die im Rahmen der Prüfung des Verhältnismäßigkeitsprinzips von Bedeutung sind. Diese betreffen weniger die Eignung, auch weniger die Erforderlichkeit, sondern vor allem die objektive Zumutbarkeit einer Überwachungsmaßnahme. Diese Aspekte kann man aus den zehn, zwölf einschlägigen Entscheidungen des Bundesverfassungsgerichts zusammentragen und verallgemeinern:

Entscheidend ist zum einen die Schwere des Eingriffs. Die ist gegenüber der Schwere des bedrohten Rechtsgutes abzuwägen. Oft war die Zahl der betroffenen Grundrechtsträger

entscheidend. Das Bundesverfassungsgerichts spricht von der Streubreite des Eingriffs. Entscheidend war auch, ob die Betroffenen Anlass für die Überwachung gegeben haben oder ohne jeden Anlass zum Objekt von Überwachung werden, und ob sie in einer Situation überwacht werden, in der sie eigentlich Vertrauen darauf entwickeln dürfen, dass sie sich zurückziehen können. Entscheidend ist auch, ob der Eingriff offen oder heimlich stattfindet und wie aussagekräftig die Überwachungsergebnisse sind, also die Daten, die dabei gewonnen werden. Es geht also immer darum, wie intensiv ein Eingriff in den entsprechenden Lebensbereichen ist. Durch all das – und wenn es kumuliert stattfindet, umso mehr – kann sich die Schwere des Eingriffs jeweils erhöhen.

Das Bundesverfassungsgericht hat eine Reihe von Eingriffsvoraussetzungen formuliert. Zum einen wurde immer wieder die mangelnde Bestimmtheit der Eingriffsermächtigung gerügt. In diesen Fällen war es unklar, gegen wen in welcher Situation bis zu welchem Grad jeweils der Eingriff stattfinden darf. Ganz wichtig war auch immer, dass ein Verdacht vorliegen muss und dass dessen Wahrscheinlichkeit ein bestimmtes Maß erreichen muss. Das Maß muss immer höher sein, je schwerer der Eingriff ist.

Für den Eingriff hat das Bundesverfassungsgericht im Wesentlichen zwei Grenzen genannt. Das eine ist: Es darf nicht zu einer Rundumüberwachung kommen! Zweitens darf der Eingriff nicht in den Kernbereich privater Lebensgestaltung führen. Das hat dann dazu geführt, dass das Bundesverfassungsgericht für alle rechtlichen Regelungen immer nachfragt, ob diese auch Sicherungsmaßnahmen vorsehen, um diese Eingriffsgrenzen einzuhalten, und entsprechende Schutzmaßnahmen gegen unverhältnismäßige Nutzung dieser Eingriffsbefugnisse fordern. Als solche Sicherungsmaßnahmen sieht das Bundesverfassungsgericht an, dass der Eingriff von einem Richter angeordnet sein muss, dass er dokumentiert und nachträglich kontrolliert wird, dass es möglich sein muss, den Eingriff abubrechen, wenn man merkt, dass man in den Kernbereich privater Lebensgestaltung eingreift, und dass möglicherweise nach Ende des Eingriffs der Betroffene informiert wird.

Wenn diese Anforderungen erfüllt sind, hat das Bundesverfassungsgericht auch immer Überwachungsmaßnahmen akzeptiert und für verfassungsgemäß erklärt, aber in letzter Zeit relativ konsequent diese Anforderungen durchgeprüft. An denen müsste man auch das eine oder andere, worüber schon diskutiert wurde, messen. Ich vermute schon, dass da nicht alles Bestand haben wird.

Vielen Dank.

Jerzy Montag

Recht herzlichen Dank. Herr Ziercke, wir haben zwei Sachen gehört: Erstens bedürfen Eingriffe, die Sie sich wünschen, einer Legitimation bedürfen. Und zweitens, wenn wir als Gesetzgeber -gesetzlich Regelungen schaffen sollen, dann müssen diese Regelungen technikbezogen sein. Da liegt – jedenfalls für uns – noch unglaublich viel im Dunkelfeld. Ich hoffe, dass Sie uns jetzt Einiges ins Hellfeld bringen können.

Jörg Ziercke

Präsident des Bundeskriminalamtes

Ob ich das wirklich kann, werden Sie am Ende meines Vortrags feststellen. Ein Problem habe ich natürlich bei einer öffentlichen Debatte über ein Thema, in dem es um verdeckte Maßnahmen geht. Sie werden Verständnis dafür haben, dass ich bestimmte Fälle ver-

fremden muss. Ich könnte in nichtöffentlicher Sitzung auch mit Billigung des Generalbundesanwalts weitergehende Details präsentieren.

Zunächst möchte ich mich bei meinem Nachbarn bedanken. Sie haben mit einem Zitat eines bekannten Verfassungsrechtlers begonnen, als es um die Frage ging: Freiheit vor dem Staat und Freiheit durch den Staat. Bisher war in dieser Runde überwiegend von der Freiheit vor dem Staat die Rede, auch bei vielen Redebeiträgen. Ich denke, da liegt genau das Dilemma. Mit diesen beiden Sätzen wird genau das Spannungsfeld beschrieben, auch sehr schön bei dem Mautgesetz – Herr Wieland, Sie haben das Beispiel selbst angesprochen. Die Mautdaten können Sie verwenden, um eine Ordnungswidrigkeit zu verfolgen, weil derjenige, der möglicherweise seine Maut nicht bezahlt hat, zur Rechenschaft gezogen werden soll. Aber in dem konkreten Fall, in dem es um Mord- bzw. Totschlag auf einem Parkplatz der Autobahn ging, sollte man die Mautdaten nicht heranziehen dürfen. Da entsteht genau das Dilemma, das Sie hier beschrieben haben.

Mir will nicht in den Kopf, warum das nicht möglich sein soll. Hier ist das Problem begründet, dass man bestimmte Prinzipien immer wunderbar abstrakt diskutieren kann, aber keine Problemlösung im konkreten Fall erzielt. Ich präsentiere Ihnen gleich Fälle, wo sich jeder fragen muss: Wollen wir das als Staat? Ist das unsere Freiheit? Brauchen wir hier nicht Sicherheit, um diese Freiheit auch zu schützen – immer in rechtlich begrenztem Umfang natürlich. Ich unterschreibe all die Dinge, die Sie hier eben dargestellt haben, zum Schluss auch, was einen Richtervorbehalt und eine Dokumentationspflicht angeht. Ich gehe sogar noch weiter, was ich auch gleich noch mal deutlich zum Ausdruck bringen will.

Ich möchte zunächst mal die kriminalistische und phänomenologische Seite aufzeigen, die Rolle des Internets, dessen Bedeutung als Tatmittel heute für die Kriminalitätsbekämpfung.

Eine besonders vielfältige Rolle hat das Internet als Tatmittel im Bereich des islamistischen Terrorismus. Das haben die Anschläge in Bali, Casablanca, Istanbul, Madrid, Amsterdam und London gezeigt. Das trifft auch auf die beiden Studenten zu, die im vergangenen Jahr in Deutschland Anschläge in Regionalzügen versucht haben. Begünstigt durch islamistische Propaganda und das Internet ist der virtuelle Dschihad aus Sicht von Al-Kaida im Grunde weltweit realisiert. Das soll zur Selbstradikalisierung, zur Rekrutierung von jungen, sehr jungen Menschen führen, die sich dieser Ideologie und dieser Form des Terrors anschließen.

Auch bei der Tatplanung spielt das Internet eine wichtige Rolle. Dort kann man sich nicht nur die zu attackierenden Zielobjekte anschauen, sondern man hat unerschöpfliche Möglichkeiten, was die Anleitung zum Bau unkonventioneller Sprengvorrichtungen und von Bomben angeht. Für den islamistischen Dschihad ist es ein Leichtes, sich diese auch herunterzuladen. Diese Entwicklungen sind natürlich Aspekte, die uns interessieren, nicht nur für die Strafverfolgung als Beweismittel, sondern auch im Rahmen der Gefahrenabwehr.

Die zweite Gruppe, das ist von Herrn Helmbrecht schon angesprochen worden, ist die Organisierte Kriminalität. Was wir erleben, ist eine steigende Entwicklung im Bereich der angezeigten Kriminalität, also des Hellfeldes. Im Bereich der Informations- und Kommunikationskriminalität hatten wir 2004 62.000 Straftaten, ein Jahr später eine Verdoppelung auf 120.000. Ich verrate hier nicht viel, wenn ich sage, wir haben weitere Steigerungsraten in 2006, also eine exponentielle Entwicklung in diesem Bereich insgesamt. Im Jahr 2005 hatten wir in Deutschland über 3.000 so genannte „Phishing-Fälle“. Für 2006

zeichnet sich ein ähnlich hohes Niveau ab. Da geht es im Grunde um Identitätsdiebstahl. Im Dezember 2006 wurden weltweit 28.000 Webseiten festgestellt, die im Zusammenhang mit Phishing standen. Wir stellen fest, es gibt immer mehr organisierte Täterstrukturen in diesem Bereich. Sie können sich im WWW die notwendigen Programme und Tools kaufen. Sie schicken Ihre Spammails über Botnetze, um Leute zu gewinnen, die als Financial-Agents dann ihr Konto zur Verfügung stellen. Aber auch das brauchen Sie heute alles gar nicht mehr. Der neueste Trick ist der: Sie annoncieren den Verkauf eines Gebrauchtwagens. Ein vermeintlicher Kunde aus dem Ausland bietet Ihnen statt der 7.000 Euro auf einmal 7.800 Euro und sagt, die Zahlung erfolge sofort, solle aber über einen Verwandten in Deutschland abgewickelt werden. Das passiert auch am nächsten Tag. Einen halben Tag später kommt jedoch der Anruf, man möge den Kauf bitte aus verschiedensten Gründen rückgängig machen, sie könnten aber 400 bis 500 Euro für eigene Aufwendungen zurück behalten. Man überweist das Geld ins Ausland z.B. über Western Union. Nur einen Tag später kommt die Bank und belastet Sie mit den 7.800 Euro. Was war passiert? Sie sind unfreiwillig zum Financial Agent im Rahmen eines Phishing-Verfahrens geworden. Sie haben ihre Überweisung von einem gehishten Konto bekommen. Das ist eine grassierende Entwicklung, für die ich Ihnen eine Vielzahl von anderen Beispielen nennen könnte.

So können Sie, wenn Sie morgen in einem Hotel sind und die Rechnung mit Ihrer EC-Karte begleichen wollen, nicht sicher sein, dass technisch irgendetwas eingebaut wurde, dass diese Daten irgendwohin in diese Welt überträgt, z.B. nach China, nach Südkorea, in die Ukraine. Dort werden dann so genannte „white plastics“ hergestellt. Bevor Sie das Hotel verlassen haben, ist man schon dabei, Ihr Konto abzuräumen.

Wir haben von 2004 bis 2005 1,2 Mio. Bankkunden weltweit registriert, die Phishing-Opfer geworden sind. Ich frage mich daher, ob das Vertrauen in das Internet in der Zukunft nicht Schaden nehmen muss, wenn man solchen organisierten Strukturen nicht das Handwerk legen kann. Botnetze mit 100.000 infizierten und damit fremdgesteuerten PCs werden künftig keine Seltenheit mehr sein. Wir haben Beispiele mit 140.000 PCs, wo diese mittels eines Trojaners gekapert und dann dazu benutzt werden, Spammails mit Trojanern zu verschicken, um die Privat-PCs von anderen Leuten zu infizieren. Mittels des Trojaners werden online-Bank-Geschäfte betrügerisch manipuliert. Der Online-banking-Kunde ist der Auffassung, mit der Bank ein Bankgeschäft abzuwickeln, tatsächlich greift der Trojaner die Daten ab, und übermittelt zu Lasten des Kontos des Kunden Gelder an die Betrügerkonten.

Botnetze sind wie gesagt keine Seltenheit mehr. Das ist für mich die Kriminalitätsform der Zukunft. Was man mit Botnetzen tatsächlich machen kann, wie man Spams verschickt, wie man Unternehmen, ja die Infrastruktur von Staaten mittels DDoS-Attacken lahm legen kann, ich glaube, das brauche ich hier nicht weiter darstellen.

Der dritte Bereich: Ich zitiere hier eine Meldung, in der es um sexuellen Missbrauch von Kindern und Kinderpornographie geht. Ich muss Ihnen das antun, um nicht Gefahr zu laufen, dass Sie alle sagen: „*Terrorismus, das sind alles Totschlagsargumente.*“ Die Kriminalitätswirklichkeit ist breiter. Wir haben in Deutschland 6,3 Mio. Straftaten in der Polizeilichen Kriminalstatistik registriert – und das ist nur das Hellfeld. Ein erklecklicher Teil davon ist Schwer-kriminalität. Man muss sich bei den Dilemmata, die hier aufgezeigt worden sind, entscheiden. Wie will der Staat darauf reagieren?

Ich zitiere eine dpa-Meldung vom 23. März 2007 von der NGOs „Innocence in danger“: Die 13-jährige Anna sitzt vor ihrem Computer. Wie viele Kinder und Jugendliche chattet

sie gern. Schnell kommt sie mit einem Unbekannten ins Gespräch. Anfangs geht es um Hobbys und Interessen, dann um ihr Aussehen. Schließlich fragt er sie, ob sie sich vor einer Webkamera ausziehen oder sich mit ihm treffen möchte. So oder ähnlich beginnen viele Fälle von sexuellem Missbrauch von Kindern und Jugendlichen.

Früher war es aufwendig Bilder zu entwickeln. Heute genügen wenige Mausklicks; Web- und Handykameras haben zu einer Bilderflut geführt. Nach Schätzungen kursieren im World Wide Web sieben Millionen Bilder missbrauchter Kinder. In Chats können Kontakte anonym und schnell geknüpft werden. Die Hemmschwelle ist niedrig. 90% der 12- bis 19-Jährigen nutzen laut der Studie „Jugendinformation Multimedia“ von 2006 das Internet. Ein Handy besitzen nahezu alle. Sieben Prozent von ihnen wurden bereits per Mobiltelefon mit Pornovideos konfrontiert. „Die Bilder bleiben“, so eine Ärztin in diesem Artikel, „den Kindern im Gedächtnis“. Ihrer Meinung nach hat sich „ein weltweites Netz zum Austausch von pornographischem Material gebildet. Täter fühlen sich nicht mehr alleine“.

Ich kann diese Entwicklung auch für Deutschland nur bestätigen. Wir haben seit Jahren eine konstant steigende Zahl bei Kinderpornographie. Kinderpornographie ist – ich habe es gerade an dem Beispiel deutlich gemacht – die schlimmste Form der Kindesmisshandlung. Im Jahr 2005 wurden 8.200 Fälle des Verbreitens und des Besitzes von Kinderpornographie mit 6.400 Tatverdächtigen registriert und damit ein Anstieg von über 13%. Das Fallaufkommen des sexuellen Missbrauchs insgesamt bewegt sich zwischen 14.000 und 16.000 Fällen jährlich.

Neben dem überwiegend kostenlosen traditionellen Austausch von Kinderpornographie im Internet beobachten wir seit Jahren einen steigenden Markt kommerzieller Webseiten. Die festgestellten Zugriffe inkriminierter Dateien belaufen sich im Einzelnen auf mehrere Hunderttausend. Gerade erst wurde vor 14 Tagen in Baden-Württemberg ein Fall aufgedeckt. Es ging um 138.000 Zugriffe auf 4.600 inkriminierte Dateien. Ein solcher Verbreitungsgrad war vorher ohne Internet nicht möglich. Soll man diesen Entwicklungen tatenlos zuschauen? Oder soll man, wenn man die Chance hat, auch versuchen, an die Leute heranzukommen? Das sind die Fragen, die wir uns alle natürlich stellen müssen.

Was bedeuten nun diese kriminologischen Entwicklungen für die Strafverfolgung und die Gefahrenabwehr der Sicherheitsbehörden?

Die Kommunikation, das ist hier sehr deutlich geworden, hat sich in den letzten Jahren in den virtuellen Raum verlagert – in Chatrooms oder Internetforen. Daraus ergibt sich die Notwendigkeit, diese Veränderungen der Kommunikation und Interaktion in der Gesellschaft auch bei den Ermittlungsmethoden nachzuvollziehen. Der neue virtuelle Raum schafft auch ein Erfordernis für eine neuartige Formen der Informationsbeschaffung. Sonst müssen Sie konsequenterweise sagen: „Das Internet ist ein rechtsfreier Raum.“

Neue technologische Entwicklungen eröffnen die Möglichkeit, dass ein Kommunikationsvorgang anonym und weitgehend verschleiert erfolgen kann. So werden Nachrichten als Bilder getarnt oder in diesen verborgen versandt. Diese Entwicklung muss im strafrechtlichen Ermittlungsverfahren nach meiner Überzeugung nachvollzogen werden. Andernfalls würde der verfassungsrechtliche Wert einer wirksamen Strafrechtspflege versagen.

Es geht daher für die Ermittlungsbehörden im Hinblick auf den durch das Internet ausgelösten digitalen Quantensprung darum, die technologische Entwicklung – ich greife diese Dinge besonders heraus – zur Bekämpfung von Terrorismus, Organisierter Kriminalität, Kindesmisshandlung, Computer- und Internetkriminalität und auch Rechtsextremismus in

Deutschland nachzuvollziehen. Das Bundesverfassungsgericht hat mehrfach betont, dass ein unabweisbares Bedürfnis für eine wirksame Strafverfolgung besteht.

Bevor ich einige konkrete Fallbeispiele der Praxis schildere, noch folgende Vorbemerkung, damit da auch kein Zweifel besteht, wie ich eine solche technologische Anpassung des Ermittlungsinstrumentariums unter Berücksichtigung verfassungsrechtlicher Grenzen vorstelle.

Erstens ist eine Online-Durchsuchung sehr aufwendig und nur in schwerwiegenden Fällen verhältnismäßig. Zweitens ist und wird Online-Durchsuchung keine polizeiliche Standardmaßnahme sein können. Drittens ist der verdeckte Charakter dieser Maßnahme kriminalistisch entscheidend. Offene Maßnahmen, z.B. die Beschlagnahme des Computers, warnen Mittäter – gerade bei Organisierter Kriminalität oder Terrorismus ist das einleuchtend – oder bringen wegen der Verschlüsselung der Daten auf der Festplatte oder wegen der Verschlüsselten externen Auslagerung von Daten ins World Wide Web als Speicherplatz keinen Erfolg. Sie müssen die Schlüssel haben, um z.B. an die gespeicherten Inhalte auf der Festplatte heranzukommen.

So muss man z.B. zum Nachweis des Tatvorwurfs der Bildung einer terroristischer Vereinigung gem. §§ 129 a und b StGB die Beteiligung von mindestens drei Personen nachweisen. Wird daher ein Beteiligter durch offene Maßnahmen ermittlungstaktisch zur Unzeit aufgedeckt, ist der Ermittlungserfolg aufgrund der damit erfolgten Warnung gefährdet. Ich unterstelle, das ist einleuchtend. Anonymisierung und Verschlüsselung sind die entscheidenden Verhinderungsfaktoren zur Bekämpfung dieser Art schwerster Kriminalität im Internet. Ein flächendeckender Einsatz einer Online-Durchsuchung – das zeigen meine Bemerkungen auch schon – im Sinne einer Schleppnetzfangung im Internet ist polizeilich nicht vorstellbar und nicht praktikabel. Um das klar zu sagen: Was ich hier gehört habe, welche Daten angeblich alle gesammelt werden sollen, das ist schlicht Unfug. Das kann die Polizei mit ihren Ressourcen überhaupt nicht und will es auch gar nicht. Ich sage auch ganz klar: In einem solchen Staat möchte ich persönlich auch nicht leben.

Zum Schutz des Kernbereichs des Persönlichkeitsrechts der Betroffenen können z.B. je nach dem Einzelfall bestimmte Schlüsselbegriffe als Suchbegriffe verwendet werden. Unerslässliche Voraussetzung für einen solchen Eingriff ist eine gesetzliche Grundlage mit Richtervorbehalt und die Beschränkung auf bestimmte Katalogstraftaten. Einige davon habe ich eben genannt. Nur nach richterlicher Zustimmung und nur, wenn auch der Schutz des Kernbereichs der Persönlichkeit gewahrt bleibt, ist eine solche Maßnahme nach meiner Überzeugung zulässig, aber sie ist dann auch zulässig. Der Staatsanwalt und der Ermittlungsrichter kontrollieren die Polizei, der Datenschützer überwacht das Verfahren. Vielleicht müssten die Datenschutzbehörden mehr Personal haben, um dieser Kontrollfunktion effektiv nachkommen zu können. Ich lade den Bundesdatenschützer immer wieder ins Bundeskriminalamt ein. Er sagt mir häufig: „Ich kann nicht kommen, ich habe nicht genug Personal“. Alle Dateien, alle Akten stehen einer solchen Kontrolle offen. Von daher: Alles, was hier gesagt wird, wie z.B.: „Das BKA sammelt DNA-Daten“ - wir sammeln im Übrigen nicht DNA-Material, sondern nur alphanumerische Daten – und wir würden alle möglichen Vorratsdatenspeicher, wie z.B. bei der Diskussion über Mindestspeicherungsfristen von Telekommunikationsverbindungsdaten, im BKA vorhalten, ist Unsinn. In diesem Fall geht es um die Provider, die solche Daten unabhängig von einem Verdacht speichern sollen. Der Zugriff auf diese Daten erfolgt im Rahmen eines konkreten Ermittlungsverfahrens.

Ich gehe noch einen Schritt weiter. Der Quellcode dieser Software, die wir für eine Online-Durchsuchung benötigen, kann meines Erachtens beim Ermittlungsrichter für eine spätere Untersuchung hinterlegt werden, damit man genau nachvollziehen kann, was gemacht wurde. Das setzt allerdings auch voraus – ich trete der Justiz hier nicht zu nahe –, dass sich auch die Justiz in diesem Bereich fachlich fortentwickeln muss. Ich denke, das ist auch eine Selbstverständlichkeit. Ergänzend sei klargestellt: Eine Online-Durchsuchung darf immer nur erfolgen, wenn sich andere, weniger eingriffsintensive Maßnahmen als ungeeignet erweisen, auch hier greift das Subsidiaritätsprinzip.

Die Softwaretools, die wir einsetzen wollen, sind keine Schadsoftware, und müssen auch keine Schwachstellen von Programmen ausnutzen. Diese Tools haben eine Doppelkomponente, d.h. unter anderem eine Steuerungskomponente, die es uns erlaubt, diese Software wieder abzuschalten, oder sie aufzurufen und genau zu steuern. Das ist ganz konkret möglich, auch wenn der Computer-Chaos-Club möglicherweise den Kopf schüttelt. Da können Sie sich gerne mit meinen Experten drüber unterhalten.

Diese Tools dienen nicht dazu, die gesamte Festplatte zu kopieren. Sie sollen für bestimmte Zeiten im Hinblick auf bestimmte Dateien eingesetzt werden. Denn auch der richterliche Beschluss hat, wie bei der Telekommunikationsüberwachung, immer ein Zeitfenster. Drei Monate beträgt dieser im Moment kraft Gesetz. Die Telekommunikationsüberwachung, die wir in Deutschland durchführen, wird in 65% der Fälle bereits nach anderthalb Monaten abgebrochen. Auch diese Tatsache belegt, dass polizeilicherseits gar keine Absicht besteht, Daten über die Maßen hinaus irgendwie abzugreifen und zu sichern. Zu diesem Komplex gibt es auch Untersuchungen des Max-Planck-Instituts dazu. Diese zeigte u.a. das Problem auf, dass Benachrichtigungspflichten, nicht eingehalten worden sind. Gleichwohl steht für mich außer Frage, dass solche Pflichten kraft Gesetzes zu statuieren sind.

Mit der Steuerungssoftware ist es möglich, nur bestimmte, identifizierte Dateien zu übertragen. Die Online-Übertragung einer ganzen Festplatte – im Regelfall demnächst bis zu 300 Gigabyte – ist technisch nicht möglich. Das sagen Ihnen alle Experten. Die spezielle Software zur Online-Durchsuchung, die für jeden Einzelfall spezifisch programmiert werden muss, wird nicht auf Dauer auf dem Computer belassen. Sie muss – auch das ist vielleicht neu – ein Datum zur Selbstaflösung haben. Auch dies muss der Richter dann verfügen. Auch so etwas ist durch eine Steuerungssoftware technisch möglich.

Einer Erkennung durch Antivirensoftware wird durch eine prinzipiell geringe Verbreitung sowie durch technische Schutzmaßnahmen entgegengewirkt. Die Software enthält keine eigene Verbreitungsroutine und wird nur nach intensiver Vorbereitung bezogen auf den Einzelfall jeweils spezifisch eingebracht. Das bedeutet zunächst eine Umfeldanalyse des Betroffenen. Wir müssen genau wissen, mit wem wir es zu tun haben, deshalb ist diese Maßnahme auch nur im Einzelfall einsetzbar, also nach eindeutiger Identifikation des Zielsystems. Eine Unterstützung durch das BSI und den Kollegen Helmbrecht ist nicht erforderlich. Ich habe auch keine Probleme mit dem, was das BSI als Warnung vor Schadsoftware herausgibt. Das BKA wird keine Schadsoftware in Umlauf bringen, um das ganz konkret zu sagen.

Ich komme nun zu konkreten Fällen und weise darauf hin, dass ich sie teilweise, was die Daten angeht, verfremdet habe.

In einem bereits laufenden Verfahren gegen eine Gruppierung mit terroristischem Hintergrund bekommt das BKA aus einer Telefonüberwachung mit, dass in der Zeit vor unserer Maßnahme tatrelevante Daten, z.B. Sprengvorrichtungen, Informationen zu potenziellen

Sicherheitseinrichtungen etc. ausgetauscht worden sind. Sofern der Rechner lokalisiert werden kann, könnten wir derzeit nur offen durchsuchen. Damit hätten wir zwar Zugriff auf die Daten – sofern sie nicht verschlüsselt sind, muss ich hinzufügen – aber das Netzwerk wäre gewarnt. Die Online-Durchsuchung würde uns in die Lage versetzen, die Relevanz der gespeicherten Daten zu prüfen, ohne die gesamte Maßnahme quasi offen legen zu müssen.

Zweiter Fall: Wir erlangen Hinweise über einen Personenkreis, der sich im Internet zu einem Verbrechen verabredet – z.B. die Anwerbung für ein Selbstmordattentat oder das Vorbereiten einer Bekennung. Wie auch im ersten Fall bleibt uns derzeit nur die Möglichkeit offener Maßnahmen, verbunden mit der Gewissheit, dass die Täter dadurch frühzeitig gewarnt werden. Andere verdeckte Maßnahmen, z.B. Telefonüberwachung, bringen uns in dem Fall nicht weiter, weil die Täter ihr Vorhaben nicht am Telefon besprechen oder aber weil sie bestimmte Dokumente gar nicht per Email übermitteln, sondern sie nur auf ihren Rechnern gespeichert haben. Mit dem Mittel der Online-Durchsuchung wären wir in der Lage nach Kontaktlisten, gespeicherten Mails, Planungsdokumenten zu suchen, um so den Kreis der beteiligten Personen als auch deren Absichten zu erhellen.

Kinderpornographie: Betreiber von pädophilen Internetforen gehen vermehrt dazu über, ihre Foren extrem abzuschotten und besser zu verschlüsseln. Videofilme und Bilder in Form von Dateien werden sequenziert und verschlüsselt auf Datenträger abgelegt und das Bord ausgetauscht. Eine Entschlüsselung ist ohne Kooperation des Urhebers durch Nennung des Passworts zurzeit nicht möglich. Ohne die Erkennung, Zusammensetzung und Auswertung des Materials ist jedoch die Identifizierung der Herstellung dieser Bilder, der Missbraucher, und damit auch die Beweisführung nicht möglich. Nur wenn wir online auf den Computer dieser Kriminellen zugreifen können, haben wir eine realistische Chance, vor der Verschlüsselung bzw. nach der Entschlüsselung an Beweismittel und verdeckt an Zugangsdaten für Foren zu gelangen, die weitere Ermittlungsmaßnahmen, Identifizierung pornographischer Tauschringe im Internet ermöglichen. In diesem Zusammenhang darf ich auch auf den Aspekt des Opferschutzes hinweisen, d.h. auf das Beenden des fortgesetzten Missbrauchs kleinster Kinder.

In einem anderen Fall geht es um einen fremden Geheimdienst. Es geht um Konstruktionszeichnungen. Auch da sind wir mit den Ermittlungen beauftragt, wo es um Rückschlüsse auf bestimmte Schlüsseltechnologien geht. Hier kann ich jetzt nicht konkreter werden, in Rede steht der Verdacht des Landesverrates und der geheimdienstliche Agententätigkeit. Der Verdächtige – das wissen wir – hat diese Daten in elektronischer Form auf seinem Computer. Auch hier geht es um die Netzwerke, die wiederum hinter dem Täter stehen.

Ein weiterer Fall: Die mit Hilfe der bisher zur Verfügung stehenden Instrumente durchgeführten Ermittlungen haben in diesem Fall – da geht es um eine Anschlagplanung – ergeben, dass eine gewisse Gruppe von Personen feststellbar war, nicht aber deren Kontakte untereinander. Das heißt, die Telefonüberwachung hat nur Erkenntnisse darüber ergeben, mit wem der Beschuldigte kommuniziert und wann diese stattfindet, aber nicht den Inhalt des Mailverkehrs, weil dieser verschlüsselt gesendet wird. Aus dieser Fallkonstellation ergab sich, dass eine klassische Telekommunikationsüberwachung nicht ausreicht, wenn zum einen die E-Mails schon vor Beginn der TK-Überwachungsmaßnahme versandt worden sind und außerdem der Emailverkehr verschlüsselt ablaufen soll. Aber es ging um eine konkrete Anschlagplanung.

Ein anderer Fall: Hier wird ein Beschuldigter verdächtigt, Spendengeldtransfers für eine terroristische Vereinigung vorgenommen zu haben. Er kommuniziert bewusst verschlüsselt und verwendet für Telefongespräche ein kostenloses Internettelefonieprogramm – ich muss Ihnen nicht nennen, welches das ist – das die Gespräche vor Übergabe an das Netz natürlich verschlüsselt, sehr gut verschlüsselt sogar, wie wir wissen. Ferner verwendet der Beschuldigte E-Mailadressen zur Nachrichtenübermittlung und kommuniziert sehr wahrscheinlich im so genannten Entwurfsmodus. Entwurfsmodus heißt, die Emails wurden geschrieben, als Entwurf gespeichert, aber nicht versandt. Vielmehr hatte der Empfänger der Nachricht ebenfalls die Zugriffsdaten für den E-Mail-Account und rief das entsprechende Konto auf, um den Mailentwurf zu lesen und auf diesem wiederum im Entwurfstext zu antworten, ohne das Dokument abzusenden – interessante Variante, nicht? Die Übermittlung der Textbeiträge erfolgt verschlüsselt. Die richterlich angeordnete Überwachung der von dem Beschuldigten genutzten DSL-Leitung führt ins Leere, da weder Telefongespräche noch E-Mailnachrichten entschlüsselt werden können. Das ist ein konkreter Fall, wo es um Terrorismus geht.

Zum Schluss noch einen so genannten weiteren Phishing-Fall: Auch hier erfolgt die Phishing-Attacke durch massenhaft versandte E-Mails, die den Eindruck erwecken von einer bestimmten Bank zu kommen. Die Betroffenen werden über eine angebliche bankinterne Sicherheitsüberprüfung – das kennen wir ja – zur Versendung ihrer persönlichen Bankdaten aufgefordert. Das ist der klassische Fall. Zur Versendung der Phishing-Mails hatten die Täter ein so genanntes Botnetz eingerichtet mit Zehntausenden von gekaperten Bots weltweit von Deutschland aus, um auf diese Art und Weise an die Bankkonten der Bürger ranzukommen. Wenn wir das verhindern, finde ich, ist das ein Zugewinn an Freiheit und an Sicherheit.

Die Kontrolle über die einzelnen Rechner wurde durch heimliche Installation bestimmter Schadprogramme usw. hergestellt. Die einzelnen Netzwerkrechner dienten auch als Proxy-Server zur Anonymisierung der IP-Adressendaten des aktiven Rechners.

Ich habe noch zwei weitere Fälle, aber die kann ich nur in nichtöffentlicher Sitzung und nur mit Zustimmung des Generalbundesanwalts hier vortragen. Da geht es um Unterstützung und Rekrutierung für den internationalen Dschihad.

Dankeschön.

Jerzy Montag

Danke, Herr Ziercke. Herr Prof. Kudlich, wir würden von Ihnen jetzt gerne hören, ob all das, was gewünscht wird, auch unter strafprozessualen und verfassungsrechtlichen Gesichtspunkten machbar und sinnvoll ist.

Hans Kudlich

Juristische Fakultät am Lehrstuhl Strafrecht, Strafprozessrecht und Rechtsphilosophie, Universität Erlangen-Nürnberg

Meine Damen und Herren, ich bin in der etwas zwiespältigen Situation, hier als Letzter zu sprechen. Denn einerseits wird in dieser Präsentation kein einziges Stichwort auftauchen, zu dem nicht schon irgendetwas gesagt worden ist. Andererseits gibt mir das vielleicht dann auch die Freiheit, nicht alle Punkte noch einmal erörtern zu müssen, sondern selektiv auf einige Dinge hinzuweisen, die mir unter den hier angesprochenen Punkten strafprozessual und verfassungsrechtlich wichtig erscheinen. Vielleicht kann ich dabei auch

kurze Einwürfe zu Dingen machen, an die ich eigentlich gar nicht gedacht hatte, als ich die Präsentation ausgearbeitet habe, die sich aber hier aus der bisherigen Veranstaltung ergeben haben.

Es würde sicherlich bedeuten, Eulen nach Athen zu tragen, wenn ich jetzt noch mal ausführlich auf Rechenleistungen und Transferkapazitäten einginge oder darauf, dass die zunehmende Digitalisierung und das Voranschreiten der Informations- und Kommunikationstechnologie ein Phänomen ist, das wir überall beobachten können. Ich möchte vielleicht nur ein bisschen greifbarer machen, was es für uns alle, für den Bürger im Alltag bedeutet.

Im Grunde hat die gesamte Vorbereitung zu dieser Veranstaltung – jedenfalls für mich – per Email stattgefunden. Ich habe keinen Brief bekommen. Ich habe nicht mal analog telefoniert, sondern ich habe nur Emails bekommen. Der Emailverkehr bestimmt bei vielen von Ihnen sicherlich diesen Alltag. Wenn ich mir dann überlege, dass diese Daten irgendwo bei mir zu Hause auf dem Rechner gespeichert werden und im Ordner daneben vielleicht die Daten für meine Steuererklärung und im nächsten Ordner die Daten für die Krankenversicherung sind, dann gibt jeder von uns gibt sehr viel an persönlichen Informationen in diesen Bereichen preis.

Nun darf man die Augen nicht davor verschließen, dass die Gefahr illegaler Nutzung von solchen Daten, von solchen Informationssystemen und auch die Gefahr der Angriffe darauf natürlich besteht. Die Angriffe auf Informationssysteme sind ja gegenwärtig auch ein Thema im Bundestag – Herr Montag und ich haben uns letzten Mittwoch im Rechtsausschuss gesehen, wo es um ein Gesetz zur Bekämpfung der Computerkriminalität ging. Hinzu kommt die Schiene des Einsatzes des Internets als Tatmittel. Die neuesten Zahlen, die ich in der PKS für das Jahr 2005 gefunden habe, sagen, dass zwar „nur“ in 2,3 % der Straftaten das Tatmittel das Internet war. Aber man kann sich leicht vorstellen, dass es eine Reihe von Straftaten gibt, bei denen das Internet als Tatmittel per se ausscheidet bzw. keine große Rolle spielt. Also, Mord, Totschlag, die meisten Diebstahlsvarianten, Straßenverkehrsdelikte – das sind ja die Delikte, die den Großteil der PKS ausmachen. Das zeigt uns umgekehrt, dass wir eben in den Bereichen, wo eine Tatbegehung über das Netz an sich vorstellbar ist, durchaus einen großen Anteil haben. Und in dem schon mehrfach angesprochenen Feld Kinderpornographie ist dort für über 60 % der Fälle als Tatmittel das Internet ausgewiesen. Wenn ich Herrn Ziercke da richtig verstanden habe, müssen wir hier wohl eher mit einer steigenden Tendenz rechnen.

Aus diesem Grunde möchte auch ich mich dazu bekennen, dass *natürlich* ein Erfordernis für hinreichende Ermittlungsbefugnisse für die Sicherheitsbehörden und die Strafverfolgungsbehörden besteht. Ich würde durchaus auch unterstreichen wollen, dass sich Bürgerschutz oder Schutz der Bürgerrechte natürlich nicht nur um den Schutz der Bürger *vor* dem Staat dreht, sondern auch um den Schutz der Bürger *durch* den Staat. Das ist keine Frage. Aber wir müssen uns eben bewusst sein, dass wir – wenn wir solche Maßnahmen schaffen – ernstzunehmenden Gefahren für die bürgerlichen Rechte, für die Grundrechte gegenüber stehen. Das bedeutet nicht, dass diese Maßnahmen von vornherein ausgeschlossen sein müssen, sondern dass wir sie eben mit Augenmaß konstruieren und mit Augenmaß anwenden müssen.

Woher kommt es, dass gerade in diesem Bereich oder gerade bei Ermittlungsbefugnissen, die den Online-Bereich betreffen, die Grundrechte in besonderem Maße gefährdet sind? Es ist ja nicht die schlichte Tatsache, dass hier die traditionell schriftliche Kommunikati-

on und Inhalte auf irgendwelchen Schmierzetteln, die in Pappkartons liegen usw., im Wesentlichen durch elektronische Speicher und Kommunikation abgelöst worden ist.

Vielmehr geht es zunächst um die erzielbare und zumindest theoretisch speicherbare, verarbeitbare Datenmenge. Vielleicht in diesem Kontext eine kurze Bemerkung zu dem, was Herr Ziercke gesagt hatte, auch mit Blick auf das, was im Vortrag des Chaos-Computerclub genannt worden war, Stichwort „*Online-Durchsuchung*“ und die zeitliche Komponente: Selbst wenn wir eine Begrenzung auf drei Monate hätten, selbst wenn das wie bei der TKÜ im Schnitt nur 1,5 Monate dauern würde, hätten wir natürlich trotzdem von der zeitlichen Komponente her etwas ganz anderes als die klassische Durchsuchung nach § 102 StPO, die sozusagen nur eine Momentaufnahme abbildet. Ich glaube, das war auch mit Ihrem Hinweis gemeint. Nicht dass Sie hätten anbringen wollen, dass sich das über Jahre hinweg entwickelt, sondern dass es eben so ist, wie wenn der Durchsuchende, der in diesem unsicheren Windowshaus ist, hier zwei Monate sitzt und mir zuguckt. Das ist was anderes, als wenn er eben ganz kurz kommt.

Hinzu kommt der oftmals verdeckte Eingriffscharakter, der hier ebenfalls schon verschiedentlich angesprochen wurde. Das betrifft nicht nur die Online-Durchsuchung, sondern das betrifft auch Dinge wie etwa Ortung des Aufenthaltsortes bei Mobiltelefonen. Wir haben hier im strafprozessualen Bereich Ermittlungsmaßnahmen, die nicht offen stattfinden. Wir kennen dieses Phänomen zwar auch sonst in der StPO, etwa in § 100 a ff. StPO die Überwachung der Telekommunikation und in § 110 a ff. StPO den Einsatz der verdeckten Ermittler. Aber das sind eben doch Ausnahmen, die jeweils im Einzelfall genau abgewogen sein wollen. Schon die Zählung – 100 a ff., 110 a ff. StPO – zeigt: das sind alles Dinge, die nachträglich in die StPO aufgenommen worden sind. Deswegen kann man wohl mit Fug und Recht behaupten, dem ursprünglichen System, der ursprünglichen Vorstellung von strafprozessualen Ermittlungen sind eigentlich diese verdeckten Ermittlungsmethoden fremd. Das heißt nicht, dass man nicht auf geänderte Umstände reagieren müsste; aber man muss sich eben dieser Fremdheit bewusst sein.

Ich habe heute auf der Zugfahrt zufällig in der Zeitschrift „Kriminalistik“ einen längeren Aufsatz eines Kriminalober- oder -hauptkommissars a.D. gelesen, der sinngemäß geschrieben hat: *Was wollt ihr denn? Online-Durchsuchung ist doch für den Betroffenen viel schonender. Da müssen nicht immer Leute durch seine Wohnung laufen.* Das ist natürlich eine etwas verkürzte Sichtweise, denn der Eingriff liegt bei der Durchsuchung ja nicht in erster Linie bei den schmutzigen Schuhen. Und wenn wir eben die Anforderungen, die sonst an verdeckte Ermittlungsmaßnahmen gestellt werden – Stichwort Katalogtaten, Stichwort besondere Beachtung des Verhältnismäßigkeitsgrundsatzes usw. – heranziehen, dann wird schon deutlich, dass nach der Gesamtkonzeption der StPO der heimliche Onlinzugriff eben als besonders schwerwiegender Eingriff anzusehen ist.

Ein letzter Punkt: Die oftmals schwierige rechtliche und nicht zuletzt auch grundrechtliche Einordnung derartiger Maßnahmen. Wir uns darüber klar werden, welche Grundrechte betroffen sind. Womit ist das denn überhaupt vergleichbar? Herr Pfitzmann hat uns vorhin vorgehalten, dass wir überwiegend aus der Sicht des Informatikfachmannes ganz unzulängliche Vergleiche verwenden. Und wenn wir die Entwicklung der einfachrechtlichen Behandlung des Phänomens Internet der letzten zehn oder zwölf Jahre Revue passieren lassen, dann gibt es eine ganze Reihe von Beispielen, wo Unsicherheit darüber bestanden hat: Wie ist das jetzt überhaupt einzuordnen? Wenn ich etwa eine Email überwachen möchte, ist das Telekommunikation, obwohl es doch so wenig mit dem Telefonieren zu tun hat, wie wir es vorher gekannt haben? Oder ist das eine Postbeschlagnahme? Schon, als wir die ersten Regelungen in den 90-er Jahren bekommen haben, das Teledienstge-

setz und den Mediendienstestaatsvertrag, gab es die Einordnungsfrage: Was ist das überhaupt? Ist es mehr Individualkommunikation? Oder hat es mit Rundfunk, hat es mit Presse zu tun? Das Medium entzieht sich sozusagen unseren gewohnten Denkkategorien sowie unseren gewohnten rechtlichen Kategorien und es ist deshalb eine besonders schwierige Behandlung.

Ich möchte nun noch stichwortartig zu drei ausgewählten, aus meiner Sicht für die Problematik wichtigen, weil typischen, Problemfeldern etwas sagen:

Das erste ist aus strafprozessualer Sicht die Online-Durchsuchung. Herr Pfitzmann hat zwar betont, dass das ein „Nichtproblem“ ist, aber für die Strafprozessualisten ist es eben doch ein Problem. Solange wir noch nicht die technischen Voraussetzungen haben, die Sie ganz überzeugend als Ideal oder als günstiger skizziert haben, stellt sich eben das Problem einerseits als praktisches. Zum anderen ist es auch eine Sache, die natürlich die Politik, die die Medien interessiert hat.

Die meisten von Ihnen kennen ja vielleicht den Ablauf. Die Generalbundesanwaltschaft hatte die Durchführung einer solchen Onlineüberwachung beim Ermittlungsrichter am BGH beantragt. Der Ermittlungsrichter des BGH hat dann Ende 2006 die Durchführung der Maßnahme abgelehnt, anders als noch ein anderer Ermittlungsrichter ungefähr ein Jahr vorher, der das noch für grundsätzlich zulässig befunden hatte. Daraufhin ist die Generalbundesanwaltschaft in die Beschwerde gegangen. Dieser Beschwerde hat der Ermittlungsrichter nicht abgeholfen und anschließend auch nicht der dritte Strafsenat, der darüber zu entscheiden hatte. Das war dann die Entscheidung von Ende Januar, in der gesagt wurde: „*Nein, wir können das nicht zulassen*“.

Ich halte diese Entscheidung *de lege lata*, sprich, zum gegenwärtigen Gesetzesstand auf jeden Fall für richtig, weil meines Erachtens die Online-Durchsuchung nicht „*unter die gängigen*“, in der StPO niedergelegten strafprozessualen Ermittlungsbefugnisse zu subsumieren ist. Nachdem das auch der Bundesgerichtshof so sieht und nachdem – soweit das von der kriminalpolitischen Notwendigkeit her anders betrachtet wird – wir auch entsprechende Gesetzgebungsvorhaben haben, muss ich jetzt diese Beurteilung, sozusagen *de lege lata*, nicht Stück für Stück noch mal nachsubsumieren. Mir geht es eigentlich um etwas anderes: Zunächst um zwei, drei Punkte, die gerade bei der Online-Durchsuchung für unser Phänomen typisch sind.

Das erste ist die umstrittene Rechtslage. Wir haben immerhin sehr hochqualifizierte Juristen bei der Generalbundesanwaltschaft. Wir hatten ein Jahr vorher eine Entscheidung des Ermittlungsrichters. Wir haben jetzt hier den Ermittlungsrichter. Es ist also eine Sache, die kontrovers diskutiert ist, nicht zuletzt aus dem Grund, den ich vorhin angedeutet habe. Es besteht Unsicherheit über die Einordnung der entsprechenden Sachverhalte in das gängige strafprozessuale Instrumentarium.

Das zweite ist die Gefahr, dass man sich auf Grund dieser Unsicherheit sagt: „Versuchen wir es eben mal“. Dann wird eben mal eine entsprechende Maßnahme beantragt. Man hätte ja auch „*Glück*“ haben können und auf einen Ermittlungsrichter am BGH treffen können, der die entsprechende Maßnahme bewilligt hätte.

Der dritte Punkt ist die schwierige verfassungsrechtliche Zuordnung. Ich habe mich da in einer Anmerkung, die vor wenigen Wochen erschienen ist – noch zur Entscheidung des Ermittlungsrichters, aber der Senat hat ja im Prinzip nichts Neues dazu gesagt – etwas weit aus dem Fenster gelehnt und habe gesagt: Selbst wenn man jetzt der Ansicht ist, man muss hier eine entsprechende gesetzliche Grundlage schaffen, müsste man sich die

Frage stellen, ob das nicht notwendig mit einer Verfassungsänderung verbunden sein könnte. Denn man könnte hier ja eventuell auch in den Schutzbereich des Art. 13 GG, also, die Unverletzlichkeit der Wohnung, eindringen. Und wenn man das so sieht, dann lässt wohl die gegenwärtige Schrankensystematik des 13 GG eine solche Überwachung, noch dazu zu repressiven Zwecken, letzten Endes nicht zu.

Ich möchte noch eine Sache ergänzen zu der Frage, die Herr Rath auch ins Spiel gebracht hat, was eigentlich das Besondere, die besondere Qualität unter dem Gesichtspunkt der Missbrauchsmöglichkeiten ist. Eine Komponente könnte bei den Missbrauchsmöglichkeiten vielleicht sein, dass nach meinem Eindruck viele Leute heutzutage – und ich nehme mich da ganz bewusst nicht aus – prima facie ein – die Experten werden sagen: *“Ganz lächerlich und unbegründet“* – gewisses Vertrauen in Dinge haben, die irgendwo in einer Datei niedergelegt sind oder auf einem Bildschirm stehen. Und die werden dann als zutreffend und richtig erachtet. Das ist vielleicht noch aus der Zeit, als es nur das öffentlich-rechtliche Fernsehen gab, als wir davon ausgegangen sind, dass die Nachrichten im Großen und Ganzen stimmten.

Ich möchte das an einem Beispiel illustrieren. Das gehört eigentlich gar nicht hierher, ist aber vielleicht ein Beispiel für die Naivität im Umgang mit dem Medium Internet: Ich war zwei Jahre an einer privaten Hochschule tätig. Es gab dort ein ausgefeiltes, von der Hochschulleitung zentralisiertes Evaluationssystem und wir hatten das Problem, dass wir relativ geringe Rücklaufquoten hatten. Ich habe gesagt, dann teilen wir doch am Ende der letzten Veranstaltung Zettel aus, statt das übers Internet zu evaluieren. Da soll jeder reinschreiben, was er gut findet, was er schlecht findet, fünf Minuten Zeit. Ich sammle anschließend alle Zettel ein. Von den Anwesenden in der Vorlesung habe ich dann 100 % Rücklauf.

Da haben dann die Studenten gesagt: *„Nein, nein, das ist ja ganz schrecklich. Sie kennen ja unsere Handschrift oder Sie beauftragen einen Graphologen und dann sehen Sie, wer was gesagt hat. Und dann bei der nächsten Klausur bekommen wir eine schlechtere Note, weil wir die Vorlesung kritisiert haben.“* Und auf meine Frage, wie sie diese Gefahr bei einer zentralen Evaluation über das Intranet sähen, dann: *„Ja, da steht drüber, das ist anonym und das wird nicht angeschaut.“* Schön, dass das da steht! Aber man musste sich – das wäre noch zu ergänzen – vor der Evaluation mit seinem Benutzernamen einwählen. Ich möchte niemandem etwas unterstellen, wahrscheinlich war das auch alles anonym, aber die Geschichte ist typisch für unseren Glauben: *„Das steht so auf dem Bildschirm und dann wird das schon seine Richtigkeit haben.“*

Nächstes Stichwort „Vorratsdatenspeicherung“: Dahinter steckt die Idee, dass die Verkehrsdaten bei verschiedenen Formen der Telekommunikation nicht mehr nur zu Abrechnungszwecken gespeichert werden dürfen, was nach gegenwärtiger Rechtslage etwa Streitfragen aufwirft: Wie ist es, wenn ich eine Flatrate habe? Kann dann etwas gespeichert werden oder nicht? Stattdessen steht in einem schon existierenden Entwurf zur Änderung des Telekommunikationsgesetzes die Speicherungspflicht für Verkehrsdaten, wo es dann eben heißt: *Wer Telekommunikationsdienste erbringt usw., der hat die Verkehrsdaten für die Zwecke der Strafverfolgung nach Maßgabe der folgenden Absätze sechs Monate im Inland zu speichern.* Und dann kommen Regelungen: Telefondienste, Dienste elektronischer Post, Internetzugangsdienste usw.

Dazu drei Anmerkungen: Es ist eingangs etwas vom *„Bürger unter Generalverdacht“* gesagt worden. Immerhin heißt es hier, *„es sind alle Daten zum Zwecke der Strafverfolgung zu speichern“*. Rein von der Wortwahl wird schon dieser Eindruck suggeriert – wenn auch

vielleicht gar nicht beabsichtigt – jeder könnte ja theoretisch ein Straftäter sein. Hier sieht man das Problem ganz gut.

Zweiter Gesichtspunkt: Es geht hier um die Umsetzung einer Europarichtlinie. Europa ist nicht nur sozusagen die *Bewahrerin der Grundfreiheiten*. Grundfreiheiten ist ein Thema bei Europa. Das andere Thema bei Europa ist schon immer Effektivität. Das gilt auch in diesem Bereich. Wenn wir das kritisch sehen, müssen wir sagen, hier drohen auch gewisse Gefahren von Europa.

Dritter Gesichtspunkt: Vorhin war von einem „Arbeitskreis Vorratsdatenspeicherung“ die Rede. Ich gehe davon aus, das ist kein Fanclub, sondern ein kritischer Arbeitskreis. Ich finde das gut und wichtig, dass es ungeachtet dessen, wie man im Detail dazu steht, eine Meinungsbildung gibt. Das ist – das richtet sich jetzt nicht gegen Sie – ein grotesker Widerspruch dazu, dass viele Bürger und Bürgerinnen gerade im Zusammenhang mit dem Internet mit ihren persönlichen Daten – man kann nicht nur sagen – leichtfertig, sondern geradezu vorsätzlich schludrig umgehen. Es gibt da Internet-Foren wie etwa „studivz“, in denen eingetragen wird: „Wer sind meine Freunde, was habe ich für Hobbys, wo wohne ich usw.“ Ohne jegliche Sensibilität.

Wenn wir über den Schutz der Bürgerrechte im digitalen Zeitalter sprechen, geht es auch darum, die Leute zu sensibilisieren, zu überlegen, gewissermaßen bewusstseinschärfend tätig werden, wie gesagt, unabhängig, wie man konkret dazu steht. Deswegen finde ich diese Initiative und dieses Ansinnen durchaus lobenswert, obwohl ich – jetzt muss ich mich leider wieder etwas outen – persönlich – ohne dass ich meine persönliche Einschätzung deswegen als Richtlinie für eine politische Entscheidung vorgeben würde – keine so großen Probleme damit hätte, wenn meine Telekommunikationsverbindungsdaten sechs Monate gespeichert werden. Ich habe mir vorhin die Kriterien mitgeschrieben, die Herr Roßnagel hinsichtlich der Schwere des Eingriffs angesprochen hat. Es geht ja nicht um irgendwelche Inhalte, es geht nur um die Verbindungsdaten. Also, wann habe ich mit welcher Telefonnummer telefoniert? Ich bin ohnehin bisher gewohnt gewesen, dass das schon zu Abrechnungszwecken gespeichert werden musste. So groß ist mein Vertrauen also vielleicht nicht. Die Intensität des Eingriffs, der hier in meinem persönlichen Lebensbereich gewonnen werden kann, halte ich eigentlich auch für nicht so groß. Auch daran, ob überhaupt der Kernbereich meiner Lebensgestaltung hier betroffen ist, hätte ich Zweifel. Ich sehe das jetzt also nicht gerade als den schlimmstmöglichen Angriff auf meine Rechte.

Dazu gehört dann auch noch der dritte Punkt: verfassungsrechtliche oder grundrechtliche Verortung. Ich hatte das vorhin schon kurz im Zusammenhang mit dem Wohnungsgrundrecht bei der Online-Durchsuchung angesprochen. Mit einem Kollegen zusammen habe ich da in einer Anmerkung geschrieben, hier hätten wir Schwierigkeiten mit Art. 13 GG. Dagegen kann man nun natürlich sagen: Soll es wirklich einen Unterschied machen, ob ich mein Notebook zu Hause im räumlichen Schutzbereich des Wohnungsgrundrechts benutze oder ob ich an irgendeinem Hot Spot irgendwo auf dem Bahnhof bin? Aber wir kennen etwa bei der Überwachung des nichtöffentlichen gesprochenen Wortes ja durchaus einen Unterschied zwischen kleinem und großem Lauschangriff. Findet das innerhalb der Sphäre der Wohnung oder nicht innerhalb der Sphäre der Wohnung statt? Irgendwo sehe ich da schon noch eine größere Schutzwürdigkeit. Diese größere Schutzwürdigkeit – und damit fügt sich das mit der Vorratsdatenspeicherung zusammen, den ich nicht für den schlimmstmöglichen Eingriff halte – des Grundrechts auf informationelle Selbstbestimmung, das hier üblicherweise diskutiert wird. Soweit es nicht um einen laufenden Telekommunikationsvorgang geht, ist das zumindest für mich, als nicht genuinen Verfas-

sungsrechtler, doch vergleichsweise amorph bzw. beschreibt im Grunde genommen aus meiner Sicht Maßnahmen sehr unterschiedlicher Intensität.

Wenn wir uns zurückerinnern, um welche Dinge wir beim Volkszählungsurteil gekämpft haben, ist das eine völlig andere Größenordnung als Videoüberwachung von öffentlichen Plätzen. Und das ist wieder eine völlig andere Dimension als etwa hier die Online-Durchsuchung. Im Grunde genommen umfasst die informationelle Selbstbestimmung als solche so weite Bereiche, dass sie vielleicht als Kriterium für die Konturierung von irgendwelchen Eingriffsbefugnissen möglicherweise zu unscharf ist.

Ich möchte jetzt nicht zu visionär sein, vielleicht wäre das unangebracht oder übertrieben. Aber man sollte sich vielleicht angesichts der Bedeutung, die dieser Bereich für unser Leben hat, die Frage stellen, ob wir zu einer verfassungsrechtlichen Absicherung nicht irgendwann auch eine neue verfassungsrechtliche Regelung schaffen müssen, die sozusagen den Art. 2 Abs. 1 GG konturiert. Wir haben ja etwa als Staatszielbestimmung auch vor einigen Jahren den Umweltschutz aufgenommen – neue Probleme, neue Sichtweisen von Problemen bedingen vielleicht auch, dass man hinsichtlich der Grundwerte, die einem besonders wichtig sind und die deshalb in der Verfassung festgeschrieben sind, reagiert. Und wenn ich hier einen Bereich habe, in dem die Bürgerrechte besonders betroffen sind, warum nicht auch der Versuch einer zumindest programmatischen grundgesetzlichen Festschreibung?

Herzlichen Dank.

Jerzy Montag

Danke, Herr Prof. Kudlich. Sie werden vielleicht erstaunt sein, aber so visionär ist das gar nicht. Darüber wird ganz konkret in unseren Reihen nachgedacht.

Ich will auch eine Anmerkung zu Ihrer Überlegung machen, ob Art. 13 u.U. geändert werden müsste. So wie ich jedenfalls die Entscheidung zum großen Lauschangriff gelesen habe, hat das Bundesverfassungsgericht zwar sehr wohl sehr traditionell die Wohnung als den fassbaren Rückzugsraum des Menschen in seine Privatheit unter Schutz gestellt, aber daneben in der Entscheidung auch sehr wohl die moderne, neue Situation erfasst und sozusagen die kommunikativen Vorgänge im höchstprivaten Lebensbereich unter diesen Schutz gestellt. So würde sich also aus der Rechtsprechung des Bundesverfassungsgerichts auch der Schutz – sage ich jetzt mal – der *Festplatte* ergeben, wenn die nicht unter meinem Bett im Schlafzimmer ist, sondern wenn sie virtuell oder mit mir herumgetragen würde. Ich glaube, dass sich da das gleiche Problem stellen würde.

Wir haben jetzt von zwei Seiten die verfassungsrechtliche und strafprozessuale Lage gehört und sehr engagiert von der anderen Seite die Erfordernisse der Strafverfolgung und die vielfältigen Probleme in der Praxis des Bundeskriminalamts. Das ist sicherlich Anlass für Nachfragen oder Bemerkungen. Deswegen schaue ich mich in der Runde um und sehe auch einige.

Fragen und Beiträge aus dem Auditorium

Sönke Hillbrans – Deutsche Vereinigung für Datenschutz

Eine Bemerkung und zwei kurze Fragen:

Die Bemerkung vorab richtet sich vor allem an Herrn Ziercke. Wir haben ja von den Herren Roßnagel und Pfitzmann schon heute gehört, dass wir die Brisanz einer neuen Methode auch von der rechtlichen und informationstechnischen Umgebung her beurteilen

müssen. Eine neue Methode mag sich vor dem Hintergrund schon vorhandener und schon längst implementierter Maßnahmen anders darstellen, als wenn wir sie isoliert betrachten.

Vor diesem Hintergrund vielleicht die Bemerkung: Wenn wir über Vorratsdatenhaltung bei Sicherheitsbehörden reden, müssen wir heute über weit mehr als 10 Millionen Datensätze im Polizeilichen Informationssystem INPOL reden. Und darüber können wir schon vor der TK-Vorratsdatenspeicherung heute reden. Und wenn Sie sagen, dass die Online-Durchsuchung kein Instrument der Schleppnetzjagd gegen Kinderpornographie ist, dann müssen wir wissen, dass es beim Bundeskriminalamt eine Abteilung ZARD gibt, die anlassunabhängige Internetrecherchen durchführt und die, wie wir von Herrn Ulrich Walter vernehmen konnten, im Prinzip jedenfalls theoretisch schon durch die Firma L-1 Solutions auch in die Lage versetzt worden ist, das automatisiert nach Kinderpornographie durchzuführen.

Aber meine Frage an Sie, Herr Ziercke, zielt in eine andere Richtung. Sie sprechen viele Millionen potenzieller Straftaten im Internet an, die sich mit Phishing und mit anderen recht einfachen Angriffen auf die IT-Sicherheit befassen. Was schätzen Sie, wie viele dieser Angriffe und dieser Straftaten eigentlich durch ganz einfache, für wenige Dollar oder durch wenige Updates erhältliche Schutzmaßnahmen durch die Betroffenen selbst hätten vermieden werden können?

Die zweite Frage richtet sich an Herrn Kudlich. Dem schicke ich voraus, dass die vielleicht seriöseste Darstellung der Online-Durchsuchung der verdeckten, im Rahmen mit jenem von Ihnen richtigerweise angesprochenen Senatsbeschluss des Bundesgerichtshofs wohl davon ausging, dass den Betroffenen durch eine CD das Ausforschungsprogramm zugespielt werden muss, wo ein Problem dann auch darin lag, den Betroffenen durch eine werbemäßig ansprechende Verpackung dazu zu bringen, das Ding aufzuspulen. Da liegt ein Element der Täuschung drin. Die verdeckte Online-Durchsuchung ist, anders als die Telefonüberwachung, mit einem Element der Täuschung verbunden. Dieses Täuschungselement kennt auch die offene Durchsuchung nicht. Sehen Sie da ein besonderes strafverfahrensrechtliches Problem?

Sebastian Buckow – Humboldt Universität Berlin

Ich habe eine Vorbemerkung und eine Nachfrage.

Wir hatten ganz am Ende noch mal die grundrechtliche Dimension auch der Sicherheit als Grundrecht. Das ist ja auch eine nicht ganz neue Debatte. Es ist vielleicht hier nur in Erinnerung zu rufen, dass zumindest auf europäischer Ebene doch der Entwurf für die Grundrechte im Rahmen des EU-Verfassungsvertrags Sicherheit explizit nennt, was sicherlich, sollte er so kommen, auch für die Abwägung in Deutschland zu beachten wäre. In Deutschland kennen wir dieses Grundrecht – man muss fast sagen, zum Glück – noch nicht.

Der entscheidendere Punkt, und hier spreche ich aus politikwissenschaftlicher Sicht, ist die strategische Komponente, dass nach und nach Verfahren umgewandelt und erweitert werden. Wir hatten heute nun schon häufiger das Beispiel der Lkw-Maut gehört. Hier erscheint mir die Frage nach Glaubwürdigkeit und Legitimation doch entscheidend, dass einfach das Vertrauen in Politik gefährdet ist, wenn wir feststellen, dass Maßnahmen, die bei Inkraftsetzung oder bei Beschluss solcher Technologien als ausgeschlossen bezeichnet werden, dann fünf Jahre später – mit sicherlich guten Gründen und durchaus auch zu argumentieren – dann aber doch letztendlich entgegen der vorherigen Zusagen kommen. Ich glaube, man muss kein Prophet sein, auch im Rahmen der Speicherung vom Fingerabdruck oder ähnlichen biometrischen Merkmalen im Ausweis, in fünf bis zehn Jahren diese

Daten zentral zu sammeln, natürlich für den guten Zweck. Auch dies ist letztendlich eine Gefahr für die Legitimation von Politik. Deswegen ist diese Problematik gerade auf Seiten der Gesetzgebung doch offen und klar zu argumentieren.

Sie hatten am Rande kurz das Problem der nichtstattfindenden nachlaufenden Informationen bei verdeckten Ermittlungen angesprochen. Wir kennen Studien vom MPI und anderen wissenschaftlichen Einrichtungen, dass hier in der Vergangenheit nachlässig gearbeitet wurde und, ich wage zu behaupten, weiterhin suboptimal nachlaufend informiert wird. Auch das ist ein Punkt, der letztendlich Glaubwürdigkeit betrifft.

Man kann sicherlich argumentieren, dass verdeckte Ermittlungen in gewissen Fällen notwendig sind, unbestritten. Aber ich glaube, es ist rechtsstaatlich zwingend erforderlich mehr Maßnahmen zu ergreifen. Da die Frage, welche Maßnahmen da angedacht werden, diese nachlaufende Information der Betroffenen tatsächlich sicherzustellen und zu gewährleisten, und dass nicht nur im Einzelfall, sondern generell hier Betroffene nach Abschluss der Ermittlungen hier auch umfassend darüber informiert werden, dass und wie weit sie überwacht wurden.

Herr Jünemann – Deutscher Richterbund

Ich wollte noch mal auf die Vorratsdatenspeicherung zu sprechen kommen, die ja national als Umsetzung einer europäischen Richtlinie gedacht ist, und noch mal Herrn Kudlich und auch Herrn Roßnagel fragen, ob Sie sich schon mal mit der Grundlage, also mit der europäischen Richtlinie und der Kompetenz der Europäischen Union zu dieser Richtlinie befasst haben. Meines Wissens ist die höchst zweifelhaft. Mir ist so im Hinterkopf, als hätte die Europäische Union eine Vorschrift, eine Rechtsgrundlage verwendet, die sie üblicherweise braucht, um die Wettbewerbsfähigkeit innerhalb der Europäischen Union zu stärken und die gar nichts mit dem in der dritten Säule zu platzierenden Strafrecht, Strafverfahrensrecht zu tun hat.

Hans Kudlich

Ich möchte mit der Anfrage von Herrn Hillbrans beginnen. Dieses Element der Täuschung, je nach dem, wie da vorgegangen wird, ist ja auch schon in den technischen Teilen teilweise angeklungen. Man wird wohl oft so vorgehen müssen bzw. es ist zumindest eine Möglichkeit. Der Gedanke der Täuschung ist natürlich etwas, was im Grunde genommen vielen verdeckten Ermittlungsmaßnahmen immanent ist. Wenn ich verdeckte Ermittler einsetze, kann ich natürlich sagen, „der verdeckte Ermittler hat aber, als er den Verdächtigen getroffen hat, nicht gesagt *ich bin ein verdeckter Ermittler*“. Das hat er nicht explizit gemacht, aber irgendwo, könnte man sagen, ist das eigentlich so eine Art Geschäftsgrundlage jedes Gespräches. Da gibt es immer ein täuschendes Element.

Wir haben in der Strafprozessordnung eine Vorschrift, die Täuschungen (*in der schwierigen Abgrenzung zur kriminalistischen List*) im Bereich der Vernehmungen generell untersagt, § 136 a StPO. Inwiefern dieses Täuschungsverbot auch außerhalb von Vernehmungssituationen im engeren Sinn, im Sinn des formellen Vernehmungsbegriffes, zu beachten ist, ist unter den Strafprozessualisten eine heftig geführte Kontroverse. Man kann aber sagen, dass die wohl herrschende Meinung, dass insbesondere die Gerichte nicht davon ausgehen, dass dieses Täuschungsverbot über die formelle Vernehmungssituation auszudehnen ist.

Das Zweite wäre: Wenn wir eine entsprechende gesetzliche Vorschrift hätten, in der das geregelt wird, dann müsste man wohl schon in der grundsätzlichen Gestattung der Maßnahme Online-Durchsuchung davon ausgehen, dass der Gesetzgeber sozusagen die Dinge, die dazu im Vorfeld erforderlich sind, mit genehmigt wissen möchte, so wie es etwa auch

zum Einbau einer Wanze beispielsweise in einen Pkw u.U. erforderlich ist, diesen Pkw zu öffnen und da vielleicht in der Verkleidung zu bohren und dergleichen, also, dass da irgendwelche Dinge im Vorfeld schon mit geregelt sind. Also, wenn wir eine gesetzliche Grundlage bekämen, dann wäre das – jedenfalls nach der neuen lex lata – kein zusätzliches Problem.

Bei der Frage nach der nachlaufenden Beteiligung bin ich nicht ganz, ob die sich auch an mich gerichtet hat oder ob das mehr eine Anmerkung war. Man kann natürlich in Gesetze viel hineinschreiben. Wenn man schriebe „*Der Betroffene muss irgendwann benachrichtigt werden*“ und das nicht für kriminaltaktisch ungeschickt halten würde, wäre das etwas, was vergleichsweise leicht durchzusetzen ist. Es gibt ja bei diesen Maßnahmen dann auch entsprechende Regelungen, dass etwa parlamentarische Berichtspflichten bestehen.

Andererseits: Ich war vor ungefähr vier Wochen zu einem Vortrag bei der Deutschen Richterakademie. Die anwesenden Staatsanwälte haben alle gesagt. *“Das ist ganz schrecklich, da habe ich schon gar keine Lust, die Maßnahme durchzuführen oder jedenfalls, wenn, ist es mir am liebsten, ich habe dann irgendein Formblatt.”* Das ist ein kritischer Punkt.

Als Letztes die Frage nach der Kompetenz für den Erlass einer Richtlinie auch mit strafrechtlichen Auswirkungen: Ich gehe davon aus, dass Herr Roßnagel europarechtlich beschlagener ist als ich. Aber es ist in der Tat ein Problem (das wir auch in anderen Bereichen kennen), dass die EU eigentlich in der ersten Säule – in der dritten Säule, Zusammenarbeit, geht das noch – keine Strafgesetzkompetenz hat, dass sich aber immer wieder bei bestimmten Regelungen, die etwa wettbewerbs- oder grundfreiheitsrelevant wären, die Frage stellt: Verzerrt nicht eine strafrechtliche Regelung, die in einem Land so und in einem anderen anders ist, auch diesen Wettbewerb? In dem einen Land werden dem Provider irgendwelche Speicherpflichten auferlegt. Das macht für die mehr Aufwand, macht sie weniger attraktiv usw.

Wir hatten ja vor noch nicht all zu langer Zeit eine Entscheidung aus dem Bereich des Umweltschutzes, wo nach meiner Erinnerung der Europäische Gerichtshof im Grundsatz solche strafrechtlichen Annexregelungen jedenfalls als möglich erachtet hat. Aber die Übertragung auf unsere Frage wäre da nicht unproblematisch.

Jerzy Montag

Die letzte Bemerkung reizt mich irrsinnig zum Widerspruch, aber das unterdrücke ich jetzt und bitte Sie, Herr Ziercke, zu antworten.

Jörg Ziercke

Ich würde gern mal auf den Hinweis „*Struktureingriff*“ – so habe ich das jedenfalls verstanden – „*in Technik*“ eingehen. Das war ja auch Ihr Argument. Ich darf noch einmal daran erinnern, dass die Software, die wir einsetzen wollen, keine Schadroutine aufweist, nicht löscht, nicht verändert, sondern einen ganz anderen Funktionsumfang als eine Schadsoftware hat. Sie ist beherrschbar und wird kontrolliert. Sie bleibt auf den Einzelfall bezogen, wo wir im Grunde – das ist der Hintergrund verdeckter Maßnahmen – in solchen Einzelfällen ganz dicht an diesen Personen dran sein müssen, um überhaupt zu erkennen: „Was hat der für ein System? Wie arbeitet der überhaupt?“ Nur dann ist ein Einsatz einer solchen Software überhaupt möglich. Die Vorstellung, die hier auch immer wieder im Raum geistert: „Da schickt man irgend so einen Trojaner in die Welt und da wird man schon sehen, was daraus wird.“ Geht völlig an der Realität vorbei. So was ist Kinderkram. So funktioniert kriminalpolizeiliche Arbeit im verdeckten Bereich nicht, um das mal klar zu sagen.

Ich kann überhaupt nicht nachvollziehen, inwieweit in so einem Einzelfall ein Struktur- eingriff – so habe ich Sie verstanden, vielleicht erläutern Sie das noch mal – in Technik stattfindet. Wir bauen hier keine Sicherheitslücken in Computersysteme ein. Wir lassen keine Hintertüren offen. Das ist wirklich Kinderei, wer glaubt, solche Argumente ins Feld führen zu können.

Sie haben von der zentralen Recherchestelle im BKA gesprochen. Diese hat ja mit Online- Durchsuchung überhaupt nichts zu tun, wie Sie wissen. Dort setzen wir Programme ein, um im Internet Seiten zu erkennen, die möglicherweise z.B. pornographische Inhalte haben. Das ist Online-Recherche. In diesem Bereich geht es darum, Programme zu verwenden, um auf solche inkriminierten Seiten überhaupt aufmerksam zu werden und dann Ermittlungen anzustellen z.B. bezogen auf das Alter der Kinder, im Hinblick auf den Ursprung der Bilder. Können wir den Raum identifizieren, wo diese Aufnahmen vielleicht gemacht wurden? Da geht es ganz konkret auch um den Schutz der Opfer. Insofern kann ich den Zusammenhang zur Online-Durchsuchung gar nicht nachvollziehen.

Und wenn Sie sagen: „Durch wenige Dollars kann man das alles vermeiden“, also, ich glaube, die Vorträge haben hier eindeutig gezeigt, dass das nicht möglich ist.

Zu Ihrem Nachbarn von der Humboldt-Universität: Bei Ihren Beispielen kam der Zweifel überall durch. Sie wissen es im Grunde gar nicht, aber Sie behaupten es einfach – es wäre suboptimal, was da heute so alles läuft. Ich habe mich da gefragt, was wäre eigentlich, wenn wir heute in Deutschland eine Diskussion darüber führen müssten, ob eine Blutentnahme wegen Alkohol im Straßenverkehr zulässig ist? Blut-DNA speichert man bei der Gerichtsmedizin, damit könnten Sie theoretisch alles machen. Oder wenn Sie heute die Diskussion führen würden: Soll der Polizeibeamte in Deutschland eine Schusswaffe tragen – im Lichte dieser Diskussion hier, mit all den Zweifeln, mit all den Behauptungen, die in den Raum gestellt wurden? Eine solche Art von Argumentation, die von vornherein darauf angelegt ist, dem anderen zu unterstellen, er missbrauche im Grunde diese Kompetenzen, ist unsachlich. Ich habe ja viele Beispiele gebracht. Sie müssten mir da mal die Frage beantworten: Was wollen Sie denn tun? Welchen Preis der Freiheit wollen Sie ggf. bei eigener Betroffenheit bezahlen?

Ich habe sehr viele verfahrensrechtliche Sicherungsmaßnahmen hier genannt. Solche sind für mich selbstverständlich.

Einwurf: Ein Richter kann den Quellcode doch nicht nachvollziehen!

Das muss doch nicht der Richter. Der muss das, was er hat, in Gewahrsam nehmen, damit er sicher ist, dass er hinterher nicht ausgetauscht worden ist. Darum geht es. Und Experten, wie Sie [an den CCC gewandt], kommen dann und können das dann im Einzelnen analysieren und begutachtend darstellen. So ist es gemeint, nicht der Richter selbst muss den Quellcode nachvollziehen, aber er ist der Garant für Nachvollziehbarkeit der Beweiskette.

Im Hinblick auf die suboptimalen Aspekte, da ist die Staatsanwaltschaft die Adresse, das ist nicht das Bundeskriminalamt, um das klar zu sagen. Ich glaube, auch dort ist eine ganze Menge geschehen. Und auch da muss man eines berücksichtigen: Es gibt in herausragenden Ermittlungsverfahren des Terrorismus, der Organisierten Kriminalität netzwerkartige Strukturen. Hier muss man sich unter Abwägung aller verfahrensrelevanten Aspekte entscheiden, ob man im Einzelfall eine Benachrichtigung durchführt. Das muss der Staatsanwalt entscheiden, ob er eine Benachrichtigung durchführt oder nicht, ob er sie noch aufschiebt oder nicht, weil der Sachverhalt möglicherweise insgesamt noch

nicht aufgeklärt erscheint. Grundsätzlich bin ich der Meinung, es muss selbstverständlich benachrichtigt werden.

Jerzy Montag

Bevor Herr Roßnagel auf die Fragen antwortet, wollte ich zu der Kontroverse, die hier entstanden ist, Herr Ziercke, noch eines sagen:

So, wie ich den Kollegen von der Humboldt-Universität verstanden habe, bezog er sich auf die vom Deutschen Bundestag oder von der Bundesregierung in Auftrag gegebene Studie des Max-Planck-Instituts Freiburg über das Funktionieren der Telekommunikationsüberwachung in Deutschland. Und da haben wir tatsächlich, das kann man nicht infrage stellen, sozusagen Schwarz auf Weiß zu lesen bekommen, dass die Überprüfung, die richterliche Kontrolle und die Benachrichtigungspflichten weniger als suboptimal, sondern richtig schlecht sind.

Einwurf Ziercke: Aber das war 2003, wenn ich richtig informiert bin, und wir haben ja davon gesprochen, wie es jetzt aussieht. Das war das Suboptimale, so habe ich Sie auch verstanden, dass Sie auch heute das behaupten, dass sich da nichts geändert hat.

Sebastian Buckow

Nein, ganz kurz zum Verständnis, ich bezog mich tatsächlich auf die von Ihnen angesprochene Studie. Meine Frage zielte darauf, wie sichergestellt wird, dass eben diese – ich konkretisiere – damals suboptimalen Verhältnis so nicht wieder vorkommen. Weil – das haben Sie ja völlig richtig dargestellt – der Aufwand bei Netzwerken die Betroffenen zu informieren, sehr viel höher ist als in der einfachen Telefonüberwachung, aber eben aus rechtsstaatlichen Gründen, glaube ich, unabdingbar – da sind wir uns ja einig –, dass auf jeden Fall zu einem möglicherweise sehr späten, aber doch irgendwann definierten Zeitpunkt informiert werden muss.

Jerzy Montag

Dazu die Information für alle im Saal: Das wird frühestens am Freitag zu debattieren sein, wenn meine Fraktion unseren Reformvorschlag zur Reform der Telekommunikationsüberwachung im Bundestag vortragen wird. Da sind alle diese Vorschläge dann auch in Gesetzesform niedergeschrieben.

Alexander Roßnagel

Zur Rechtsgrundlage für die Vorratsspeicherung im europäischen Recht
Zuerst war ja vorgesehen, dass das in der dritten Säule beschlossen wird. Dagegen hat sich dann das Europäische Parlament gewandt, weil es unzureichend beteiligt worden wäre, und hat Wert darauf gelegt, dass das im Rahmen des EG-Vertrags stattfindet. Wenn man einen bestimmten Blickwinkel einnimmt, kann man das auch sehr gut vertreten, denn die Vorratsspeicherung ist aus diesem Blickwinkel in erster Linie eine Pflicht der Provider. Dies europaweit – entsprechend den Wettbewerbsbedingungen – gleich zu regeln, ist eine Aufgabe, die im EGV angesprochen ist. Was dabei unberücksichtigt bleibt, ist der damit verbundene Grundrechtseingriff in die Rechte der Betroffenen, deren Daten gespeichert werden.

Ich möchte noch ganz kurz auf Herrn Kudlich und seine Bemerkung eingehen, dass die Vorratsspeicherung für ihn weniger gravierend als andere Maßnahmen ist, die wir hier besprochen haben. Ich sehe es ein klein wenig anders. Wenn man die Kriterien des Bundesverfassungsgerichts zugrunde legt, muss man feststellen, dass die Maßnahme eine irrsinnig hohe Streubreite hat. Die kann gar nicht größer sein, denn es werden etwa 500 Mio. Europäer davon erfasst, und zwar ohne dass ein einziger einen Anlass dafür gegeben

hat. Gravierender kann an der Stelle der Eingriff gar nicht mehr sein. Es werden zwar nur Verkehrsdaten gespeichert, aber die sind – über ein halbes Jahr betrachtet – dann doch ziemlich aussagekräftig. Man kann also schon sehen, wer mit wem wie lange telefoniert. Man kann Kommunikationsprofile erstellen und man kann darauf aufbauend auch Beziehungsprofile erstellen.

Es gibt heftigere Eingriffe in den Kernbereich der privaten Lebensgestaltung, das gebe ich gern zu, aber diese Möglichkeit der Profilierung ist in meinen Augen nicht vernachlässigbar.

Was mich am meisten beunruhigt, ist der Infrastrukturcharakter des Ganzen. Eingeführt wird das Ganze, weil man im Rahmen der Strafverfolgung in vielen Fällen sicher Erfolge erzielen kann. So kann man vielleicht beispielsweise einen Kinderpornograph auf diese Art und Weise feststellen. Aber das hat dann ja Weiterungen. Jetzt gibt es die technische Möglichkeit. Jetzt sind die Daten so lange verfügbar. Und siehe da, die Richtlinie zur Durchsetzung der Urheberrechte führt ja schon dazu, dass aus privatrechtlichen Ansprüchen heraus jemand, der behauptet, ein Urheberrecht zu haben, die Möglichkeit hat, einen Provider zu zwingen, dass er ihm diese Daten herausgibt.

Und jetzt soll mir mal einer erklären, warum das für Urheber möglich sein muss, aber für alle anderen, die privatrechtliche Ansprüche geltend machen, dann nicht gelten soll. Die Weiterung ist also schon angelegt. Am Schluss ist es dann ein Mittel, das für alle möglichen Konflikte benutzt werden kann, um rauszufinden, wer wann mit wem telefoniert oder auf andere Weise kommuniziert hat. Dafür ist die Vorratsspeicherung doch eigentlich gar nicht gedacht, aber das wird am Schluss das Ergebnis sein, weil man hier eine Infrastrukturmaßnahme ergreift, die alle betrifft. Da sehe ich einen ganz, ganz großen Unterschied zu vielen anderen Maßnahmen, über die wir gesprochen haben. Die bleiben in ihrer Wirkung isoliert. Aber die Vorratsspeicherung bleibt nicht isoliert. Sie trifft alle und schafft für diese eine neue Überwachungsinfrastruktur.

Ich gebe gern zu, dass – wenn die Daten in Deutschland nur für sechs Monate gespeichert werden – es über die Speicherung zu Abrechnungszwecken nicht sehr weit hinausgeht. Das bewirkt dann vielleicht nur zwei Monate Differenz. Aber wir hatten ja vorhin kurz angesprochen, dass es Leute mit einer Flatrate gibt, deren Daten überhaupt nicht zu Abrechnungszwecken gespeichert werden dürfen und vergleichbare Ausnahmen. Also, es gibt schon viele Fälle, in denen es zu einer Speicherung kommt, die im Normalfall nicht stattfinden würde.

Markus Beckedal – Netzpolitik.org

Herr Ziercke, Sie sprachen davon, Schlüsselbegriffe können verwendet werden, um die Privatsphäre zu schützen. Soweit ich weiß, ist es bei Telekommunikationsüberwachung immer so, dass die Opfer oder diejenigen, die überwacht werden, dann einfach andere Worte verwenden – also, statt „Attenta“t sprechen die dann von „Kindergeburtstag“ usw. Wie soll das Ihre Software denn checken können? So ist Ihr Argument kein Argument mehr.

Herr Pfitzmann, wir haben gerade als Argument gehört, Quellcodes könnten beim Richter hinterlegt werden, damit man sie nachvollziehen kann. Ja, was sagen Sie dazu aus technischer Sicht? Wenn ein Quellcode beim Richter liegt, kann man technisch nachvollziehen, dass dieser hinterlegte Quellcode, ob ausgedruckt oder auf irgendeinem Speichermedium, tatsächlich der Trojaner ist, der irgendwann untergeschoben wurde?

Zweitens können anscheinend eine ganze Menge Probleme gelöst werden, wenn man sich mit den Botnetzen beschäftigt. Da ist mein Gefühl, das betrifft eigentlich alles Programme eines Herstellers aus den USA, Microsoft. Kann man da nicht mal über Produkthaftung im Sinne des Verbraucherschutzes sprechen, dass man diesem einen Anbieter irgendwie mal härtere verbraucherrechtliche Maßnahmen aufdrückt, damit man die Botnetze aus der Welt bekommt?

Andreas Pfitzmann

Natürlich kann man einen Quellcode beim Richter hinterlegen. Ich unterstelle mal, dass speziell beim BKA dort dann auch wirklich der Quellcode hinterlegt wird, der verwendet wurde. Unterstellen wir das mal. Aber das ist eigentlich nicht das, was den Richter wirklich interessieren wird, sondern die entscheidendere Frage ist: Was bewirkt das compilierte Programm in dieser Umgebung? Dazu muss man jetzt Einiges sagen.

Es ist heute – so wie die Systeme sind – bereits extrem schwierig, gute Software für eine Umgebung zu schreiben, die man genau kennt. Gute Software für eine Umgebung schreiben zu wollen, die man nicht genau kennt, ist extrem risikoreich. Also nicht, dass man an der Stelle schlechte Absichten hat, aber der sprichwörtliche Elefant im Porzellanladen reißt mit seinem Hinterteil auch Regale um, selbst wenn er keinen Vorsatz hat. Ich wäre extremst verwundert, wenn die Kenntnisse beim Bundeskriminalamt im Bereich Softwaretechnik das, was wir in der öffentlichen Forschung können und wissen, im viele Größenordnungen übersteigen würde. Das kann man an der Stelle nur sagen.

Ich glaube also, mit dieser Unbefangenheit über Informatik zu reden – Herr Ziercke nehmen Sie es nicht persönlich –, kann nur jemand, der nicht selber mit Informatikmethoden arbeitet. Ich kann mir nicht vorstellen, dass das, was Sie ...

Einwurf Ziercke: So haben es mir meine Informatiker versichert.

Dann möchte ich an der Stelle, dass sich Ihre Informatiker in so eine Runde begeben und sich den Spott persönlich abholen. Das wäre fair. Das können wir gerne machen. Dem stelle ich mich gerne. Ich kann an der Stelle nur sagen: Vermutlich bin ich der erste gewesen, der zumindest im deutschen Sprachraum solche Begriffe wie *universelles trojanisches Pferd* gebracht hat. Ich glaube also schon, dass ich weiß, worüber ich rede. Ich kann also hier nur zu Protokoll geben:

Fehlerfreie Software schreiben zu wollen, ist extrem schwierig. Fehlerfreie Software für unbekannte Einsatz- und Ausführungsumgebung zu schreiben, ist praktisch unmöglich.

Einwurf aus dem Auditorium: Doch, das ist aber genau das, was Sie wollen. Sie schicken Ihre Software in eine Umgebung, die Sie – bevor Sie sie schicken – nicht genau kennen. Das genau ist das Problem.

Einwurf aus dem Auditorium: Wissen Sie, jetzt haben Sie ein Henne-Ei-Problem. Wenn Sie eh schon behaupten, Sie kennen alles, was auf dem Rechner ist, bitte, dann brauchen Sie keine Software mehr. Herr Ziercke, Entschuldigung, da ist jetzt ein logischer Bruch. Wir können das nachher in kleiner Runde noch weiter besprechen, aber aus meiner Sicht ist das gerade eine unakzeptable Argumentation.

Jerzy Montag

Herr Pfitzmann, der Kollege vom Chaos-Computer-Club und Herr Ziercke entfernen sich jetzt von dem Niveau, auf dem wir Ihnen noch folgen können. Den Vorschlag, dass Sie auf einer völlig fachmännischen Ebene zum Nutzen und Frommen des BKA zusammentreffen, finde ich sehr konstruktiv, aber das können wir heute nicht leisten.

Andreas Pfitzmann

Dann fangen wir jetzt vielleicht mit den ganz einfach Sachen an. Herr Kudlich, für Sie ist Vorratsdatenspeicherung kein Problem. Ist es für Sie auch dann kein Problem, wenn anhand dieser über Sie gespeicherten Daten die organisierte Kriminalität feststellt, wann der günstigste Zeitpunkt ist, Ihre Wohnung auszuräumen? Das ist anhand dieser Daten nicht schwierig festzustellen. Die Geschichte ist voll von solchen Beispielen.

Die zweite Frage: Ist die Sache wirklich harmlos? Falls es Leute gibt, die über Telekommunikation Dinge tun, die sie nicht anderen, ihrem Ehepartner oder wem auch immer, zugänglich sein lassen wollen, ist da ein Erpressungspotenzial. Fremde Geheimdienste werden genau diese Daten nutzen, um Agenten mit der kleinen Bemerkung – *wenn Sie mit uns nicht kooperieren, bekommt Ihr Ehepartner einige Informationen, die Ihrer Beziehung nicht gut tun* – anzuwerben. Das ist jetzt nicht Erfindung, sondern die Geschichte ist voll von solchen Beispielen. Insoweit ist möglicherweise doch zumindest für manche Vorratsdatenspeicherung ein Problem.

Zu Herrn Ziercke und seinen Beispielen: Fangen wir wieder mit einem einfachen an, wo Sie sagten, *ist ja schrecklich, müssen wir unbedingt was tun* – Kreditkartenbetrug.

Ich habe den Banken 1986, das ist mehr als 20 Jahre her, gesagt, dass es eine extrem dumme Idee ist, ein Zahlungssystem zu haben, wo man an einem fremden System seine Bankdaten, sprich, seine Kreditkartennummer und womöglich noch ein vermeintliches Geheimnis wie eine PIN oder TAN, eingibt. Wenn die Banken es in 21 Jahren nicht schaffen, elementarste Sicherheitsbedingungen zu schaffen, dann – meine ich – müsste eigentlich das BKA gegen die Banken ermitteln und nicht gegen die Phisher.

Um das ganz deutlich zu sagen: Die Verantwortung für das, was passiert, liegt zumindest in der moralischen Ebene an einer ganz anderen Stelle. Und dann zu sagen, *weil die Banken absolut in ihrer Sicherheitstechnik versagen, brauchen wir jetzt große Ermittlungsbefugnisse*, finde ich abenteuerlich.

Zweite Frage an Sie, Herr Ziercke: Bei Kinderpornographie wird es an der Stelle viel, viel ernster, weil es jetzt geht nicht mehr um Geld geht. Die Banken werden übrigens ihre System ändern, weil sie zu teuer werden. Da geht es um Geld.

Sie sagen Kinderpornographie nimmt zu – haben Sie Zahlen, ob der Missbrauch von Kindern zunimmt oder „nur“ die Zahl der Kopien von Bildern? Ich will jetzt nicht die Kopien von Bildern verharmlosen. Ein Kind, was da mal missbraucht wurde, und die Bilder vagabundieren durchs Netz, das ist schlimm genug. Aber das, was wir eigentlich primär schützen müssen, sind die Kinder. Auch an der Stelle muss ich sagen: Etwas mehr Zivilcourage im familiären Umfeld wäre vermutlich das Beste, was den Kindern passieren kann, noch weitaus wirkungsvoller als Vorratsdatenspeicherung.

Die letzte Sache, inwieweit Ihre Software alles Mögliche kann, vertiefen wir zu anderer Zeit.

Hans Kudlich

Ich hatte ja betont, dass ich meine individuelle Einschätzung nicht unbedingt als Grundlage einer politischen Entscheidung heranziehen wollte und durchaus die Problematik sehe. Ihre beiden Aspekte, Ihre beiden Beispiele würde ich zusammenfassen zum „Missbrauch durch Dritte“, ob das jetzt die Organisierte Kriminalität ist oder der ausländische Geheimdienst. Da muss ich zugeben, dass ich letztlich – thematisch aus der Diskussion und wo sie herkommt – jetzt vor allem an diese Dimension Schutz des Bürgers vor dem Staat gedacht habe und diese andere Dimension außen vor gelassen habe. Die haben wir

natürlich auch an anderen Stellen, aber wenn Ihnen Fachleute sagen, das ist ein ganz großes Risiko, dann wäre das natürlich im politischen Prozess zu berücksichtigen.

Jörg Ziercke

Zum Kreditkartenbetrug: Verzeihen Sie mir, aber Ihre Äußerung, dass die Banken haften sollen, halte ich für absurd.

Zur Kinderpornographie habe ich die Zahlen genannt, 2005 8.200 Fälle, 13,25 % mit 6.400 Tatverdächtigen allein in Deutschland.

Nachfrage Pfitzmann: Können Sie differenzieren zwischen Kindesmissbrauch und Verbreitung von Kinderpornographie? 8.200 Fälle, 13,25 %, 6.400 Tatverdächtige. Daneben gibt es den großen Graubereich.

Nachfrage Pfitzmann: Von was? Die Verbreitung von Bildern oder den Missbrauch?

Für einzelne Fälle von Kindern, Einzelfälle, nicht Bilder. Wir zählen keine Bilder, wir zählen die Fälle, die Betroffenen. Das sind die Fälle übers Internet. Insgesamt gibt es eine Steigerung von 14.000 auf 16.000.

Jerzy Montag

Ich kann mich nun nur für die rege Teilnahme in meinem zweiten Panel bedanken. Zu den Schlussworten übergebe ich an meinen Kollegen Wieland.

Zusammenfassendes Schlusswort

Wolfgang Wieland MdB, Sprecher für Innere Sicherheit

Vielen Dank, Jerzy. Ich fand diese Veranstaltung spannend, kompakt und wirklich gut. Der Spannungsbogen war sehr weit, so dass die Diskussion auf der fachlichen Ebene – wenn ich das mal so sagen darf – zwischen diesem Teil der Zivilgesellschaft, dem Chaos Computer Club, der digitalen Zivilgesellschaft und zwischen den Sicherheitsbehörden fortgesetzt werden wird. Ich danke Ihnen, euch für das Erscheinen. Ich danke natürlich den Vertretern der Wissenschaft, die zum Teil gefordert haben, die Wohnung ganz anders zu bauen, was zu der Frage von Herrn Pfitzmann an Herrn Ziercke führte, ob er denn dann noch reinkommt, wenn sie ganz anders gebaut wird. Aber vielleicht ist sie ja dann so, dass gar niemand mehr reinkommt, dass man da auch keine Verbrecher mehr, also, niemand Unbefugtes mehr jagen soll.

Das waren interessante Ansätze. Ich fand es auch sehr zuvorkommend, Herr Walter, dass Sie als Vertreter der Wirtschaft – obwohl hier nicht die für Sie primäre Zielgruppe zu erkennen war – uns gesagt haben, was auf dem Markt ist, was wir zu erwarten haben, woran Sie arbeiten. Ich denke, das hat uns hier alle auch weitergebracht.

Die europarechtlichen, die verfassungsrechtlichen Aspekte: Herr Kudlich, ich sah hier noch mal 1984. Ich gehöre noch zu denen, die noch zehn Jahre – bis 1984 – gewarnt haben. Nun ist das 20 Jahre zurück und ich musste erleben, dass man heutzutage Wahlkampf macht, indem man in den Big-Brother-Container geht und das niemand mehr negativ findet. Ich sage immer: Wer wissen will, wie es um den Schutz der Privatheit im Bewusstsein der Menschen heute bestellt ist, der braucht nur einmal mit dem ICE von Berlin nach Hannover zu fahren und ungewollt Ohrenzeuge von 15 lautstarken Telefonaten zu werden – bis hin zur Vereinbarung von Straftaten.

Das heißt, es ist ein weiter Weg, bis wir dieses Bewusstsein der Privatheit wieder erreichen. Wir, die wir hier sitzen, haben das als Ziel. Wir haben gute verfassungsrechtliche Argumente gehört. Wir haben auch von Herrn Helmbrecht – sozusagen auf der pragmatischen Ebene – gehört, wie er sich bemüht, die Datensicherheit zu heben. Aber ich denke, auch insgesamt in der Gesellschaft muss diese Diskussion geführt werden: Was ist uns das heute eigentlich noch wert?

Wie geht es hier nun weiter? Zunächst wird eine Zusammenfassung dieses Gesprächs gemacht. Was geschieht mit der wohl? Sie wird ins Internet gestellt werden. Dann werden wir aber auch eine ausführliche Zusammenschrift der Dinge machen, die hier gesagt wurden, die dann auch autorisiert werden und den Formalien unterliegen, die dafür üblich sind. Das wird geschehen.

Dank an alle, die uns hier als Referentinnen, Referenten zur Verfügung gestanden haben. Dank auch an unsere Mitarbeiterinnen und Mitarbeiter, die das alles sehr liebevoll vorbereitet und einen wesentlichen Anteil daran haben, dass wir mit doch guten Ergebnissen jetzt getrost nach Hause oder zur weiteren Arbeit gehen können.

