www.jusletter-it.eu

Fritjof Haft

Spionage – einst und jetzt

The copious data spying by secret services, particulary by the National Security Agency (NSA) has been subjected to criticism world wide. Espionage certainly is not a new phenomenon. It has been practised for millennias. The article provides a brief overview, expresses skepticism regarding legal measures and points out, which technical barriers are hampering the analysis of large collections of data. Contrary to specific target persons, notably politicians, the mass of persons concerned can rest assured in this data portfolio, such as a single fish in the school in an attack of the predator. (ah)

Category: Articles
Field of law: Data Protection; Data Security
Region: Germany

Citation: Fritjof Haft, Spionage – einst und jetzt, in: Jusletter IT 15 May 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1 Einleitung

[Rz 1] Die Enthüllung der NSA-Spionage hat eine weltweite Diskussion ausgelöst. Kaum jemand bezweifelt, dass diese Praktiken verdammenswert sind. Die UNO-Vollversammlung hat am 18. Dezember18. 2013 auf Initiative von Deutschland und Brasilien eine – freilich nicht bindende – Resolution gegen Spähaktionen verabschiedet. Darin heißt es: «*Die gleichen Rechte, die Menschen offline haben, müssen auch online geschützt werden – vor allem das Recht auf Privatheit*». Die «*ungesetzliche und willkürliche Überwachung*» *von Kommunikationsdaten*» verletze die Privatsphäre und führe zur Einschränkungen der Meinungsfreiheit. Die USA und andere westliche Staaten haben eine Abschwächung des Dokuments bewirkt. Weder sie noch die NSA werden in dem Papier namentlich genannt. Menschenrechtsorganisationen wie Amnesty International und Human Rights Watch haben dies kritisiert. Dennoch ist die Resolution wichtig für den Schutz der Menschenrechte im Computerzeitalter. Das Thema bleibt auch auf der Tagesordnung der UNO. Die Menschenrechtskommissarin Navi Pillay wurde beauftragt, noch in diesem Jahr einen Bericht über geheimdienstliche Überwachungsprogramme und den Schutz der Privatsphäre vorzulegen, über den die Vollversammlung ab September 2014 beraten will.

[Rz 2] In Deutschland haben zu Beginn dieses Jahres 207 Wissenschaftler gegen die Online-Spähattacken der Geheimdienste protestiert und ein Ende der Grundrechtsverstöße gefordert. Zuvor hatten 560 prominente Schriftsteller weltweit eine Resolution gegen die Massenüberwachung der Zivilbevölkerung veröffentlicht. Zu den Unterzeichnern gehörten Nobelpreisträger wie Günter Grass, Elfriede Jelinek, Orhan Pamuk und J.M. Coetzee sowie Umberto Eco, Margaret Atwood, Joao Ribeiro, Henning Mankell, Richard Ford und David Grossmann.

[Rz 3] Die deutsche Bundesregierung zeigte sich hoffnungsvoll, eine vertragliche Lösung mit den USA zu finden. Aber die Ernüchterung folgte rasch. Am 14. Januar 2014 meldete die Süddeutsche Zeitung, das geplante No-Spy-Abkommen mit den USA stehe vor dem Scheitern. In einem Kommentar schrieb Heribert Prantl: «*Nichts ist trauriger als der Tod einer Illusion. Es war offenbar eine Illusion zu glauben, dass die USA ihre Spähaktionen in Deutschland, gegen Deutschland und gegen Deutsche aufgeben oder zumindest stark einschränken werden. Dem Totalzugriff des US-Geheimdienstes NSA auf die Kommunikationsdaten entspricht die Totalweigerung der US-Politik, sich wenigstens zur Mäßigung zu verpflichten.*»

[Rz 4] Gibt es ein Mittel gegen diese Praktiken? Die Antwort auf diese Frage erfordert zunächst einen historischen Rückblick. Er muss freilich kurz bleiben und sich auf wenige Erscheinungen beschränken. Denn Spionage gibt es schon seit sehr langer Zeit. Genauer: seit etwa 3'000 Jahren.

2 Spionage – ein altes Gewerbe

[Rz 5] Die Spionage ist zwar nicht das älteste Gewerbe der Welt, aber doch ein sehr altes Gewerbe. Bereits in der Antike mühten sich die Machthaber, Informationen über ihre Feinde und,

vielleicht noch wichtiger, über ihre Untertanen zu gewinnen. Meder, Perser, Griechen, Römer – sie alle pflegten mit Hingabe dieses Gewerbe. Der griechische Geschichtsschreiber Herodot (um 485–ca. 424 v. Chr.) berichtete, dass Xerxes auf seinem Zug gegen die Griechen in Sardeis drei entarnte griechische Spione begnadigt habe, damit sie den Griechen von der Größe seines Heeres und seiner Flotte berichten konnten. Er hoffte, die Griechen würden dann ihren Widerstand aufgeben und sich unterwerfen – eine irrige Hoffnung, wie so häufig in der Geschichte der Spionage. So berichtete ZEIT Online am 13. Januar 2014, laut einer Studie der New America Foundation, einer US-amerikanischen Denkfabrik, habe die Datensammlung der NSA bislang nur wenig dazu beigetragen, Terroranschläge zu verhindern. Die traditionelle Strafverfolgung sei wesentlich effektiver. Nur in einem einzigen Fall habe das NSA-Programm Hinweise für Terrorermittlungen gegeben. Dabei sei es um einen Taxifahrer in San Diego gegangen. Dieser sei daraufhin verurteilt worden, weil er einer Terrorgruppe in Somalia Geld geschickt habe. Drei Komplizen seien ebenfalls verurteilt worden. Um einen drohenden Anschlag gegen die USA sei es nicht gegangen. Die NSA befindet sich insoweit also durchaus in der Gesellschaft des Perserkönigs Xerxes, der auch sonst nicht gerade mit Intelligenz geschlagen war; so ließ er nach einem fehlgeschlagenen Versuch, eine Schiffsbrücke über die Dardanellen zu errichten, das Meer auspeitschen.

[Rz 6] Für Cäsar war die Spionage (von lat. «spicare» = ausspähen) ein wichtiger Bestandteil der Kriegsführung. Bereits früher, seit dem Ende des Zweiten Punischen Kriegs (218–201 v. Chr.) gehörten jeder römischen Legion zehn «speculatores» an. Das waren zu Spionagezwecken ausgebildete Soldaten, die hinter den feindlichen Linien operierten und die gegnerischen Truppen observierten. Auch die Abwehr der Spionage war für Cäsar schon ein Thema. Der römische Schriftsteller Sueton (ca. 70–122 n. Chr.) schrieb, er habe ein nach ihm benanntes Verschlüsselungsverfahren verwendet, welches mit einer Verschiebung des Alphabets um drei Buchstaben gearbeitet habe.

[Rz 7] Im Mittelalter kam die Wirtschaftsspionage hinzu. Es ging darum, herauszufinden, wie andere Länder bestimmte Produkte erzeugten. Solche Geheimnisse wurden sorgfältig geschützt. Ein Beispiel bietet Chinas Geheimnis der Seidenherstellung. Die Kaiserin Xi Ling Shi, Ehefrau von Huang Di, soll vor etwa 4'600 Jahren die Kunst der Seidenspinnerei erfunden haben. Sie zupfte Raupen von den Blättern der Maulbeerbäume. Eine davon fiel in ihren Tee. Beim Herausfischen spulte sie einen hauchdünnen Seidenfaden ab. So entstanden die begehrten Stoffe. Für mehrere tausend Jahre hüteten die Chinesen dieses Geheimnis. Über die berühmte Seidenstraße gelangte die Seide nach Ägypten und Rom. Durch Wirtschaftsspionage wurde das Geheimnis dann im frühen Mittelalter in Europa aufgedeckt.

[Rz 8] An der Abwehrfront machten zu Beginn der Neuzeit die Verschlüsselungsmethoden Fortschritte. Um 1500 entstand das Voynich-Manuskript, ein 224 Seiten starkes Buch, dessen Verschlüsselung bis heute nicht entziffert werden konnte. Ein anderes Beispiel bietet die Beale-Chiffre, eine Schrift aus dem Jahre 1885, die angeblich beschreibt, wo ein gewisser Thomas J. Beale in den Jahren 1820/22 einen Goldschatz versteckt habe. Er konnte nur teilweise entschlüsselt werden. Die entscheidende Botschaft – der Ort des Verstecks – wurde bis heute nicht gefunden.

[Rz 9] Als 1618 der Westfälische Frieden ausgehandelt wurde und Kaiser Ferdinand nach vernichtenden Niederlagen seine Bereitschaft zum Friedensschluss nach Münster mitteilte, war der Chiffreschlüssel verlorengegangen, so dass das Dokument nicht entziffert werden konnte. Der Krieg wurde noch einige Wochen fortgesetzt, bis der Schlüssel eintraf und der Vertrag endlich unterschrieben werden konnte.

[Rz 10] Im Frankreich der Revolutionszeit zeigte Joseph Fouché (1759–1820), dass Wissen eine

Macht war, gegen die selbst ein Napoleon nichts ausrichten konnte. Fouché gehörte dem Konvent an und war Drahtzieher der Opposition gegen Robespierre, die dessen Sturz und Hinrichtung bewirkte. 1779 ernannte ihn das Direktorium zum Polizeiminister. Dies ermöglichte es ihm, ein ausgedehntes Spionagesystem über alle Klassen der Gesellschaft einschließlich der Familie des Ersten Konsuls zu organisieren. Napoleon versuchte vergeblich, ihn loszuwerden. Der Mann wusste zu viel. Der Diktator war Geisel des allwissenden, alles registrierenden, alles ahnenden Polizeichefs. Nach Napoleons Sturz schloss er sich den Bourbonen an. Napoleon ernannte ihn nach den 100 Tagen erneut zum Polizeiminister. Nach dem erneuten Sturz des Kaisers wurde Fouché wiederum Polizeiminister der Monarchisten. Als reicher Mann starb er in Triest. Eine vergleichbare Karriere gelang Talleyrand, der jedoch im Gegensatz zu Fouché sagen konnte, er habe stets Frankreich gedient, während Fouché immer nur der Mehrheit gedient habe. Als einmal bei einer kaiserlichen Redoute Fouché und der hinkende Talleyrand gemeinsam den Raum betraten, bemerkte Chateaubriand: «*Das Laster, gestützt auf den Verrat*».

[Rz 11] Im 19. und 20. Jahrhundert begann dann die Epoche der maschinengestützten Verschlüsselung. Eine eigene Disziplin namens Kryptographie entstand. Im Zweiten Weltkrieg wurde auf deutscher Seite die Enigma (von griech. «ainigma» = Rätsel») eingesetzt. Diese Schlüsselmaschine galt als «unknackbar», wurde jedoch in England von dem polnischen Mathematiker Marian Rejewski und dem Informatiker Alan Turing geknackt. Die so gewonnenen Informationen trugen wesentlich zum Sieg der Alliierten über Nazi-Deutschland bei.

[Rz 12] In den siebziger Jahren begann dann die Epoche der Verschlüsselung mit dem Computer. Jedem Fortschritt auf der Verschlüsselungsseite folgte ein entsprechender Schritt bei den Hackern. Im Januar 2014 veröffentlichte die Washington Post die Nachricht, die NSA strebe den Bau eines Quantencomputers an, der imstande sein soll, alle vorhandenen Verschlüsselungs- und Signaturverfahren zu brechen. Bislang ist das nur ein theoretisches Modell, doch ist nach aller Erfahrung mit seiner Realisierung in naher Zukunft zu rechnen.

[Rz 13] Als Fazit bleibt festzuhalten: Der Wettlauf zwischen Verschlüsselern und Hackern gleicht dem Wettlauf zwischen Hase und Igel. Eine technische Lösung des Problems ist nicht zu erwarten. Sonderfälle wie das Voynich-Manuskript und der Beale-Chiffre widerlegen diese Feststellung nicht, zumal beim Voynich-Manuskript durchaus die Möglichkeit besteht, dass es überhaupt keinen sinnvollen Text enthält.

3 Die Suche nach einer rechtlichen Lösung des Problems

[Rz 14] Die Rechtsfragen des Computerzeitalters werden seit der Mitte des 20. Jahrhunderts diskutiert. Schon zu einer Zeit, als nur Rechner mit geringer Leistungsfähigkeit im Einsatz waren und Internet und digitale Kommunikation noch in ferner Zukunft lagen, wurde über «Privacy» diskutiert und das Schreckensbild des «gläsernen Menschen» gemalt. In Deutschland wurde bereits in den siebziger Jahren das Wort «Datenschutz» zu einem Begriff jener Gattung, die in den USA mit «Motherhood, Applepie and the Flag» bezeichnet wird. Dabei war und ist schon im Ansatz unklar, worum es eigentlich geht. Geht es um den Schutz des Menschen vor missbräuchlicher Datenverarbeitung? Geht es um das vom Bundesverfassungsgericht entwickelte Recht auf informationelle Selbstbestimmung? Geht es um den Schutz des allgemeinen Persönlichkeitsrechts? Geht es um den Schutz der Privatsphäre? Geht es um die Meinungsfreiheit? Geht es um die Abwehr des Überwachungsstaats? Geht es um die Freiheit der Kommunikation? Geht es um die

Entscheidungsfreiheit des Einzelnen?

[Rz 15] Wie auch immer – der deutsche Gesetzgeber reagierte rasch und gründlich. Das Bundesdatenschutzgesetz (BDSG) wurde bereits im Jahre 1977 verkündet. Parallel dazu erließen die Länder ihre Datenschutzgesetze. Diese Gesetze sind extrem kompliziert und verwenden eine unübersichtliche Verweisungstechnik, die ihr Verständnis schwer, wenn nicht unmöglich machen. Die erste Dissertation, die ich im Jahre 1982 nach Übernahme meines Tübinger Lehrstuhls für Strafrecht und Rechtsinformatik ausgab, wurde von Armin Herb verfasst und trug den Titel «*Mangelnde Normenklarheit im Datenschutz-Strafrecht*». Der Titel war Programm. So deckte die Arbeit u.a. einen Kreisverkehr in der verwendeten Verweisungstechnik nach folgendem Prinzip auf: § 4 verweist auf § 7, dieser auf § 9 und § 9 wieder auf § 4. Es gab damals ein allgemeines Unbehagen, das einen gesetzgeberischen Aktionismus auslöste, der zu Datenschutzbeauftragten in Bund, Ländern und Unternehmen führte, ohne dass geklärt war, worum es eigentlich ging.

[Rz 16] Das Zusammentreffen des Gesetzgebers mit einer modernen und in der Entwicklung befindlichen Technik ist auch sonst nicht immer glücklich verlaufen. So erwartete in Deutschland vor einem halben Jahrhundert ein komplett ausgearbeitetes Atomgesetz voller Spannung das Kritischwerden des ersten Mailers. Was dann wirklich geschehen würde – Stichwort «Fukushima» –, ahnte niemand. Und im Computerstrafrecht wurde in den achtziger Jahren mit einem neuen Tatbestand § 263a des Strafgesetzbuches (StGB) der Computerbetrug verpönt und als Beeinflussung des «*Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf*» beschrieben. Das ist alles höchst unklar und die Schlussvariante der «*unbefugten Einwirkung auf den Ablauf*» eines Datenverarbeitungsvorganges bietet den bemerkenswerten Fall, dass der Strafgesetzgeber nicht die leiseste Ahnung hatte, was das sein sollte – Fußtritte gegen das Gehäuse? Herausziehen des Steckers? Einleitung von Starkstrom? Was immer auch gemeint war, es wird jedenfalls mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

[Rz 17] Ähnlich verhält es sich heute. Alle guten Menschen sind sich in der Verdammung der NSA-Praktiken einig, aber was da eigentlich geschieht, wie es geschieht, und welche konkreten Gefahren und Nachteile drohen, denen womöglich auch positive Folgen gegenüberstehen, wird kaum geprüft. Rechtliche Regelungen, die wirklich greifen, sind da nicht zu erwarten. Es kommt hinzu, dass die Datenspionage international betrieben wird, was nationalen Gesetzgebern und Strafverfolgern Grenzen setzt. Bei Straftaten mit Auslandsbezug gibt es für den nationalen Gesetzgeber zwei prinzipielle Möglichkeiten: Er kann an die Staatsangehörigkeit des Täters anknüpfen (Personalprinzip) oder an den Begehungsort (Territorialitätsprinzip). Im deutschen Strafrecht gilt das letztere. Maßgeblich ist, ob die Straftat in Deutschland «*begangen*» wurde. Dies ist der Fall, wenn der Täter hier «*gehandelt*» hat oder wenn hier der zum Tatbestand gehörende «*Erfolg*» eingetreten ist. Die in Deutschland relevanten §§ 202a StGB (Ausspähen von Daten) und 202b StGB (Abfangen von Daten) sind als Erfolgsdelikte ausgestaltet, bei denen das «*Sich- oder einem anderen-Verschaffen*» von Daten der Erfolg ist. Im Falle NSA sitzen sowohl der Spähende als auch der andere aber in den USA, so dass eine Anwendbarkeit des deutschen Strafrechts ausscheidet. Derartige Friktionen sind unvermeidlich, wenn der Gesetzgeber aus der Hüfte schießt ohne die Realität zu kennen, die er regeln möchte.

[Rz 18] Es bleiben noch die internationalen Verträge, aber es wäre naiv, hiervon eine Bändigung der weltweiten Datenspionage zu erwarten.

[Rz 19] Auch vom Recht ist daher keine Lösung des Problems zu erwarten.

4 Das Problem: Unstrukturierte Daten

[Rz 20] Wenn man mit etwas leben muss, was man nicht ändern kann, ist es sinnvoll, dieses «Etwas» genauer zu betrachten. Natürlich sind die Computerprogramme von NSA & Co streng geheim, aber die Aufgaben, die sie lösen müssen, sind nicht geheim, und die prinzipiell vorhandenen Lösungswege sind es auch nicht. Betrachten wir diese einmal näher.

[Rz 21] Auf der einen Seite steht die digitale Kommunikation. Das sind geschriebene oder gesprochene Texte sowie Grafiken (Fotos, Pläne, Zeichnungen usw.) Sie werden elektronisch über E-Mails, Internet, Handys usw. übermittelt und können dabei abgefangen werden. Auf der anderen Seite stehen Fragestellungen, die in entsprechender Weise formuliert werden müssen. Soll beispielsweise ein terroristischer Anschlag erkannt werden, muss dieser in einer Frage beschrieben werden. Die vorhandenen Daten müssen dann anhand dieser Frage durchsucht werden. Es muss geprüft werden, ob zwischen der Frage und den erfassten Daten Relevanz besteht. Allgemeiner gesprochen: Man hat auf der einen Seite Inhaltsdaten, auf der anderen Seite Fragedaten, und man muss prüfen, ob die Inhaltsdaten Antworten auf die Fragen enthalten. Dies muss wegen der Menge der Inhaltsdaten computergestützt geschehen. Die Zeiten, da Geheimdienstleute Briefe öffneten und lasen, sind vorüber.

[Rz 22] Wäre es möglich, den Vorgang des Verstehens formal zu repräsentieren, wäre es vorstellbar, diese Prüfung maschinell vorzunehmen. Davon kann aber keine Rede sein. Das Verstehen ist ein Vorgang, mit dem sich die Hermeneutik seit der Antike beschäftigt. Im 19. Jahrhundert war sie die zentrale Disziplin der Geisteswissenschaften. Nach Wilhelm Dilthey (1833–1911) bedeutete Verstehen, aus äußerlich gegebenen, sinnlich wahrnehmbaren Zeichen ein «Inneres», Psychisches zu erkennen. Alle Versuche, im Computer diesen Vorgang abzubilden, sind bislang gescheitert. Wenn heute in diesem Zusammenhang von «Künstlicher Intelligenz» die Rede ist, liegt bereits begrifflich ein Missverständnis vor. Es handelt sich um eine Übersetzung von «artificial intelligence», wobei «intelligence» im Sinne von «Information», «Nachricht» zu verstehen ist. So ist die US-amerikanische Central Intelligence Agency (CIA) nicht etwa eine Intelligenz-Agentur, sondern ein Nachrichtendienst. Bei der sog. «Künstlichen Intelligenz» geht es nur darum, ein menschenähnliches Verhalten zu simulieren. Ein Beispiel bietet das in den 1960er Jahren von Joseph Weizenbaum (1923–2008) am MIT entwickelte Programm ELIZA, welches den Dialog eines Psychiaters mit einem Patienten simulierte. Die Wirkung des Programms war damals überwältigend, aber wenn man die Regel bedenkt, dass Psychiater niemals Fragen beantworten und auf jede Antwort mit einer Frage reagieren, legt sich die Überwältigung wieder.

[Rz 23] Ich selbst habe in den 1980er Jahren an einem Forschungsprojekt LEX mitgearbeitet, bei dem es darum ging, juristisch relevante Sachverhalte im Computer so zu bearbeiten, dass Fragen richtig beantwortet wurden, die in natürlicher Sprache, und zwar gesprochen, gestellt wurden. Diese Forschung war lehrreich, um die dabei zu lösenden Probleme zu erkennen. Wir bildeten drei Wissensbasen. Die erste war eine juristische Wissensbasis; sie war am leichtesten nachzubauen, weil es im kontinentaleuropäischen Recht eine seit Jahrhunderten gut durchstrukturierte sog. Dogmatik gibt, auf der wir aufsetzen konnten. Die zweite war eine linguistische Wissensbasis. Hier waren einige Fortschritte möglich, wie man heute an den Arbeiten zur maschinellen Sprachübersetzung erkennen kann; wirklich überzeugend ist diese aber noch nicht gelungen. Als unlösbar erwies sich das Problem der dritten Wissensbasis. Sie sollte das Common-Sense-Wissen enthalten, über welches wir alle verfügen, ohne uns dies bewusst zu machen. Wenn ich z.B. sage: «Ich bin gestern von München nach Frankfurt gefahren», dann weiß jedermann, dass ich gestern zuerst in München und später in Frankfurt war, obwohl ich dies nicht gesagt habe. Ich habe le-

diglich eine Fahrt beschrieben. Inzwischen gibt es hierzu Datenbanken, z.B. Cycorp, in der sich zahlreiche Regeln befinden wie die, dass Wasser nass ist. Aber von einer Lösung dieses Problems sind wir noch weit entfernt.

[Rz 24] So what? Aktuell gibt es zahlreiche Systeme, um unstrukturierte Daten zu durchforsten. Ein Beispiel bietet das IBM-System Watson. Es hat seinen Namen nicht etwa von Dr. Watson, dem leicht beschränkten Fragepartner von Sherlock Holmes, sondern von Thomas J. Watson (1874–1956), einem Gründungsvater der IBM. Watson steht in der Tradition der IBM Rechners Deep Blue, eines Großrechners, dem es 1997 erstmals gelang, in einem Mensch-gegen-Maschine-Wettbewerb zu gewinnen. Deep Blue konnte 200 Millionen mögliche Schachzüge pro Sekunde berechnen und besiegte in einem Schachwettbewerb den damaligen Weltmeister Garry Kasparov. Watson verfügt über deutlich mehr Rechenkapazität und beruht auch auf einem neuen Ansatz: Watson soll die menschliche Sprache (konkret Englisch) «verstehen» und deren Wörter und Kontext so analysieren, dass der Rechner Antworten auf Fragen in natürlicher Sprache geben kann. Das Ziel besteht darin, lernende Computersysteme für verschiedene Einsatzbereiche zu schaffen. In einem spektakulären Einsatz, vergleichbar dem Schachspiel von Deep Blue, hat Watson 2011 in einer Fernseh-Quiz-Show namens «Jeopardy» (englisch = Gefahr) gegen zwei menschliche Champions ein Preisgeld von 1 Mio. US-Dollar gewonnen (und gemeinnützigen Zwecken zugeführt). Bei Jeopardy geht es darum, zu einer gegebenen Antwort die passende Frage zu finden. Beispielsweise fand Watson zu der Antwort: «In ´Der Fuchs und der Igel' führte dieser russische Graf sein Geschichtsverständnis aus» die richtige Frage: «Wer ist Tolstoi?». Zu der Antwort «Heitor Villa-Lobos widmete seine zwölf Etüden für dieses Instrument Andres Segovia» fand er die Frage «Was ist eine Gitarre?» Die Stimme von Watson ähnelte dabei frappierend der des Supercomputers HAL in Stanley Kubricks Film «2001».

[Rz 25] Der Computer soll also imstande sein, selbstständig Informationen aus Daten zu gewinnen und Schlüsse zu ziehen. Damit soll er sich den kognitiven Fähigkeiten des Menschen annähern. Am 9. Januar 2014 teilte IBM mit, man werde $ 1 Milliarde in einen neuen Geschäftsbereich namens Watson Group investieren. Binnen einer Dekade soll ein $ 10 Milliarden Geschäft entstehen. Dieses Vorhaben zeigt, wie weit man noch von einer Lösung des Problems entfernt ist, kognitive menschliche Fähigkeiten formal zu repräsentieren. Die Washington Post zitierte in dem erwähnten Artikel über das Telefondaten-Sammeln der NSA die Forschungsstudie mit den Worten: «*Im Großen und Ganzen liegt das Problem der Anti-Terror-Beamten nicht darin, dass sie größere Mengen Information aus den massenhaften Überwachungsprogrammen bräuchten, sondern darin, dass sie die Informationen, die sie bereits besitzen und die mit herkömmlichen Techniken gewonnen wurden, nicht ausreichend verstehen oder teilen*».

5 Vorläufiges Fazit

[Rz 26] Die weltweite Empörung hält also einer nüchternen Betrachtung nicht stand. Wer in seinen Telefonaten nicht etwa schlechte Scherze macht und evidente Reizwörter benutzt, kann sich so sicher fühlen wie ein Fisch in einem Schwarm, den ein Raubfisch angreift.

[Rz 27] Die vielen Aufschreie kontrastieren zudem eigenartig mit der Tatsache, dass nicht nur unzählige Privatpersonen, sondern auch viele Politiker nichts besseres zu tun haben, als private und berufliche Informationen in sozialen Netzen preiszugeben und dabei eine Unmenge an Spuren im Internet zu hinterlassen. Solche Daten liegen schon längst nicht mehr auf einem Server,

den es zu schützen gilt. Das «Netzwerk» ist das System. Dass wir irgendwann «gläsern» werden, ja, es vielfach heute schon sind, ist nicht mehr zu vermeiden. Amazon zeigt es uns bei jeder Bestellung. Hier kann aber allenfalls persönlicher Schaden entstehen. Dramatischer wäre es, wenn das Internet von irgendwelchen Schurkenstaaten «übernommen» würde. Es ist kaum vorstellbar, was geschieht, wenn die Kommunikationswege des Internets manipuliert oder sogar blockiert würden. Ganze Staaten könnten gezielt handlungsunfähig gemacht werden. An dieser Stelle erscheint gezielte Spionage – oder anders gesagt: professionelle Überwachung – als das kleinere Übel.

Prof. Dr. Fritjof Haft war Inhaber des Lehrstuhls für Rechtsinformatik und Strafrecht an der Universität Tübingen und ist Geschäftsführer der von ihm gegründeten Normfall GmbH in München (www.normfall.de).