/// Big Brother is watching you

DIE RISIKEN VON „ANLASSLOSEN“ DATENSPEICHERUNGEN

GERALD SPYRA /// **Die Einführung der Vorratsdatenspeicherung ist ein Thema, das in der Öffentlichkeit noch immer kontrovers und heftig diskutiert wird. Trotz der teilweise erbittert geführten Diskussionen rund um die Einführung einer Vorratsdatenspeicherung wird einer Tatsache noch immer viel zu wenig Tribut gezollt: Es wird nämlich oftmals viel zu wenig thematisiert, dass wir in vielen Bereichen unseres Lebens schon längst eine Vorratsdatenspeicherung haben, die mit unkalkulierbaren Risiken einhergeht.**

Einleitung

Ob, wann und wie die staatliche Vorratsdatenspeicherung kommen wird, ist eine Frage, die derzeit heftig diskutiert wird. Beobachtet man die öffentlich geführte Diskussion, erinnert diese fast schon an ein Tauziehen. Bei diesem will sich kein Lager auch nur einen Schritt auf das andere zu bewegen. Man hat schon fast das Gefühl, dass die Kontrahenten Angst davor haben, dass ein Schritt in die andere Richtung den Sieg kosten könnte. Diese beinahe schon übervorsichtige Haltung ist nicht verwunderlich, denn durch die geplante Vorratsdatenspeicherung kommt es zu einem erheblichen staatlichen Eingriff in die Grundrechte der Bürger, der nur unter sehr eng gefassten und fest abgesteckten Bedingungen möglich sein darf.

Bei der Diskussion spielen im Wesentlichen zwei für das Leben in unserer Gesellschaft essenzielle Schutzgüter eine bedeutende Rolle.[1] Das ist zum einen die Freiheit. Durch die Einführung der Vorratsdatenspeicherung sehen Kritiker die Freiheit der Bürger massiv gefährdet. Falls die Vorratsdatenspeicherung kommen sollte, bestünde ihrer Ansicht nach die Gefahr, dass die Bürger nicht mehr „frei“ wären und sich ständig überwacht fühlen würden. Es bestünde damit die Gefahr, dass sich Deutschland Schritt für Schritt auf einen Überwachungsstaat zu bewegen würde. Daher schwingen in den Köpfen der Vorratsdatenspeicherungsgegner immer auch die Erfahrungen mit, die die Deutschen insbesondere mit den staatlichen Überwachungstätigkeiten im letzten Jahrhundert gesammelt

Quelle: @mt/fotolia.com

Wie durchschaubar, wie „gläsern“ sind wir bereits und was trägt der Einzelne selber dazu bei?

Bei der DISKUSSION steht Freiheit gegen Schutz.

haben. Verständlicherweise reagieren die Vertreter dieser Position deshalb sehr sensibel, wenn es um staatliche Eingriffe in ihre Privatsphäre geht.

Die Befürworter der Vorratsdatenspeicherung führen den Schutz der Sicherheit als wesentliches Gut ins Feld. Die Gewährleistung von Sicherheit sei eine Schutzverpflichtung des Staates, die er gegenüber seinen Bürgern habe. Aufgrund des Einsatzes der neuen Medien wie E-Mail, Internet etc. sei es notwendig, dass staatliche Strafverfolgungsbehörden auch hier nachvollziehen können müssen, was geschehen wird, bzw. was geschehen ist. So soll die Vorratsdatenspeicherung beispielsweise dazu dienen, Terroranschläge oder andere schwere Verbrechen gegen deutsche Bürger zu verhindern. Darüber hinaus sollen die im Wege der Vorratsdatenspeicherung aufgezeichneten Daten zur Aufklärung von Verbrechen herangezogen werden können, um die Rechtsstaatlichkeit und die effektive und effiziente Strafverfolgung zu gewährleisten.

Zugegebenermaßen lassen sich beide Argumentationslinien gut nachvollziehen, und es fällt schwer, sich (vollständig) einer Seite anzuschließen. Vielmehr zeigt die Diskussion um die Vorratsdatenspeicherung, wie wichtig es ist, die beiden, für unsere Gesellschaft essenziellen Interessen Freiheit und Sicherheit miteinander zu harmonisieren. Dass dies kein einfaches Unterfangen ist und oftmals minimale Abweichungen weitreichende Konsequenzen haben können, wird aufgrund der hohen Eingriffsintensität in die Grundrechte der Bürger, die mit der Vorratsdatenspeicherung einhergeht, schnell deutlich.

Es mutet deshalb umso befremdlicher an, dass viele Bürger, die sich auf der einen Seite vehement gegen die staatliche Vorratsdatenspeicherung aussprechen und diese verhindern wollen, durch ihr eigenes Verhalten eine Vorratsdatenspeicherung (durch private Unternehmen) aber tolerieren und massiv fördern. Gerade durch die Nutzung neuer Medien wie z. B. Smartphones, Internet, E-Mails usw. erfolgt in der Praxis eine Vorratsdatenspeicherung in noch viel größeren Ausmaßen als dies bei der staatlichen Vorratsdatenspeicherung der Fall sein soll.

Die meisten Informationen, die der Staat in nur wenigen, ganz klar vorgegebenen Konstellationen verwenden können soll, werden heutzutage von prominenten, international agierenden Weltkonzernen zu oftmals viel intransparenteren Zwecken permanent gespeichert, miteinander verknüpft und mit anderen Organisationen ausgetauscht. Durch die immer intensivere Nutzung der neuen Medien, z. B. durch das Surfen auf den unterschiedlichsten Webseiten, durch die Nutzung einschlägig bekannter Suchmaschinen, dem Einkaufen in Onlineshops, durch die intensive Nutzung sozialer Netzwerke und natürlich auch durch die extensive Nutzung von Smartphones unterstützen wir die fast grenzenlose Sammlung unserer Daten. Das Fatale hieran ist, dass wir aufgrund der intransparenten Datenverarbeitung oftmals gar nicht abschätzen können, wer alles aus der Masse von gespeicherten Daten welche Rückschlüsse ziehen

kann. Daher können wir auch nicht absehen, was sich aus diesen (anlasslosen) Datensammlungen schon heute und besonders auch in Zukunft für persönliche Konsequenzen ergeben können.

Der vorliegende Artikel hat deshalb zum Ziel, den Leser für die grundsätzlichen Problematiken von (anlasslosen) Datenspeicherungen, die sich besonders auch bei Big Data stellen zu sensibilisieren. Außerdem will er den Leser über die Gefahren, die aus zu vielen Daten bzw. digitalen Spuren, die wir u. a. bei der Nutzung der neuen Medien von uns hinterlassen, informieren.

Die Nutzung neuer Medien

Fast jeder Bürger nutzt die sogenannten neuen Medien wie Smartphones, Internet, E-Mail usw. So besitzt fast jeder Bürger heutzutage ein oder mehrere Smartphones. Das Wunderbare an diesen Smartphones ist, dass sie kinderleicht zu bedienen sind. Man kann seine E-Mails mit einmal Wischen und Tippen von überall auf der Welt her abrufen, mit ein paar Handbewegungen im Internet surfen, in fremden Städten mit seinem Auto zielgerichtet navigieren, über bestimmte Software (Apps) mit Freunden chatten und sogar kostenlos telefonieren. Durch das Design eines Smartphones sieht man allerdings nur das, was im Vordergrund – auf dem Bildschirm des Smartphones – passiert. Was im Hintergrund abläuft, sieht und bemerkt man jedoch nicht. Für die meisten Nutzer ist das auch nicht weiter interessant, denn das Gerät funktioniert ja so, wie sie es sich wünschen. Es läuft stabil und stürzt nicht ab. Oftmals ist das Smartphone sogar so schlau, dass es schon genau weiß, was man will, ohne dass man seinen Wunsch in irgendeiner Form bereits geäußert hätte.

Der Bürger liefert unbewusst und freiwillig **SELBER** viel Datenmaterial.

Weil das Smartphone seinem Nutzer praktisch jeden Wunsch von den Augen abliest, wird es immer vertrauter und unentbehrlicher. Im Laufe der Zeit avanciert es zum „besten Freund" und es begleitet seinen Nutzer deshalb auf Schritt und Tritt. Aufgrund des starken Vertrauensverhältnisses empfinden wir es als unproblematisch, diesem Gerät unsere intimsten Geheimnisse (Daten) anzuvertrauen. Weil wir nichts Auffälliges auf dem Smartphone-Bildschirm bemerken, gehen wir auch davon aus, dass die meist hoch sensiblen Daten immer nur (exklusiv) auf unserem Gerät sind und bleiben. Doch diese Annahme ist leider oftmals ein Trugschluss. Nur weil wir keinen (sichtbaren) Abfluss von Daten auf dem Smartphone bemerken, heißt das noch lange nicht, dass dieser nicht stattfindet. Das Gegenteil ist vielmehr der Fall. Man sollte sich vergegenwärtigen, dass vom Smartphone ständig Daten auf eine intransparente Art und Weise abfließen und von den entsprechenden Anbietern – zu welchen Zwecken auch immer – verarbeitet werden.[2]

Die Nutzung der neuen Medien ist u. a. auch deshalb so attraktiv, weil die meisten angebotenen Dienste kostenlos sind. Es ist möglich, all diese Dienste zu nutzen, ohne tatsächlich auch nur einen Cent dafür bezahlen zu müssen. Doch von diesen kostenlosen Angeboten

sollte man sich nicht täuschen lassen. Vielmehr sollte man sich bei einer Vielzahl dieser Dienste darüber im Klaren sein, dass die Erbringung dieser kostenfreien Leistungen zumeist aus eigenen, egoistischen, wirtschaftlichen Motiven der Anbieter heraus erfolgt und dabei alles andere als kostenlos ist. Man muss sich darüber bewusst sein, dass wir bzw. unsere Daten das eigentliche Produkt sind, mit dem die Anbieter dieser kostenlosen Dienste ihr Geld verdienen.

Wie der Handel mit unseren Daten vor sich geht bzw. von wem, wie und zu welchen Zwecken die von uns gesammelten Daten verwendet werden, wissen wir jedoch nicht und wir werden von den Anbietern hierüber auch im Dunklen gelassen. Daher lässt sich durchaus auch überspitzt sagen, dass die neuen Medien bei der Sammlung unserer teils sensiblen Informationen als Spione fungieren. Sie sammeln durch ihre umfassenden Funktionalitäten verdeckt bzw. im Hintergrund eine Masse an Informationen, die den Anbieter / Hersteller dieser Dienste über unser tägliches Leben, unsere zwischenmenschlichen Verhältnisse und unsere Bedürfnisse und Wünsche in Echtzeit informieren. Durch die Erkenntnisse, die die Anbieter aus den gesammelten bzw. übermittelten Daten ziehen können, erfahren sie ziemlich genau, was wir wollen. Deshalb sind sie z. B. auch in der Lage, persönliche, auf uns zielgerichtet zugeschnittene Werbung auf unser Smartphone zu schalten. Man sollte sich deshalb auch darüber im Klaren sein, dass man mit jeder Nutzung der neuen Medien eindeutige digitale Spuren von sich hinterlässt, die vollständig dokumentiert werden und faktisch nie wieder verschwinden. Bei praktisch all diesen Spuren gilt, dass sie ein Spiegelbild unserer Bedürfnisse, Wünsche usw. vermitteln.

Ob wir wollen oder nicht – alle unsere Handlungen haben immer einen sehr persönlichen Ursprung. Jede Handlung wie z. B. eine Suche bei Google erfolgt aus einer bestimmten, persönlichen Motivation heraus. Aus diesem Grund ist es z. B. Google auch möglich, durch die Analyse unserer digitalen Handlungen bzw. unserer digitalen Spuren unsere Motivationen, Einstellungen, Bedürfnisse oder sonstigen Umstände, in denen wir uns gerade befinden, abzuleiten und zu dokumentieren.

Das wiederum hat zur Konsequenz, dass je mehr digitale Spuren von uns aufgezeichnet wurden bzw. werden, desto genauere Rückschlüsse hierdurch auf unsere Person bzw. unsere Persönlichkeit gezogen werden können. Mithin werden wir durch die Nutzung der neuen Medien immer gläserner und bleiben es schließlich. Das Fatale hieran ist, dass wir gegen diese Profilbildung machtlos sind. Vielmehr wissen wir auch nicht einmal, welche Informationen die Anbieter von uns haben und was sie damit anstellen.

Für vordergründig kostenlose Dienste der neuen Medien **BEZAHLEN** die Nutzer mit ihren Daten.

Ausmaße und Konsequenzen der Datensammlung

Die permanente Sammlung und Profilbildung unserer Informationen hat bereits erschreckende Ausmaße angenommen. Die Tentakeln der digitalen Daten-

kraken sind omnipräsent. Oftmals reichen den Datensammlern, aufgrund der schon von uns angefertigten Datenprofile bereits kleine Hinweise, um Geheimnisse herauszufinden, die man lieber vor dem Internet verheimlichen würde.

Wie schwer es beispielsweise ist, eine Schwangerschaft vor dem Internet geheim zu halten, hat eine Professorin der amerikanischen Princeton Universität in einem Selbstversuch getestet. Die zur Geheimhaltung erforderlichen Maßnahmen kommentierte sie mit dem folgenden, sinngemäß wiedergegebenen Satz, der zum Nachdenken anregen sollte: In Summe dürften alle Aktivitäten, die nötig waren, um ein (ungeborenes) Baby vor dem Internet geheim zu halten, mit denen vergleichbar sein, die bei Strafverfolgungsbehörden sofort den Verdacht erregen würden, dass man ein Verbrechen begehen will.[3]

In der Praxis erstellen die unterschiedlichsten Organisationen wie Hersteller von Smartphones, Software (Apps), Anbieter von sozialen Netzwerken, Suchmaschinen, Onlinewerbefirmen aber auch Regierungen Persönlichkeitsprofile von uns, die sie zunächst immer zu eigenen Zwecken nutzen. Doch weil diese Informationen oftmals nicht ausreichen, den jeweiligen Nutzer vollständig durchleuchten zu können, tauschen diese Protagonisten unsere Profile untereinander aus, kaufen selber welche oder verkaufen sie an andere Organisationen. Durch die hierdurch erhaltenen neuen Informationen können sie ihr eigenes, von den Nutzern angefertigtes Profil weiter verfeinern.

Ein Austausch unserer Profile erfolgt jedoch nicht nur aus finanziellen Interessen. Oftmals werden diese Anbieter von Regierungen bzw. Behörden verpflichtet, die von ihnen erstellten Persönlichkeitsprofile an sie auszuhändigen. Bei sozialen Netzwerken wie Facebook, Twitter und Co. erfolgt der Austausch sogar noch einfacher. Hier besitzen amerikanische Behörden einen eigenen, direkten Zugang zu allen Informationen, so dass sie diesbezüglich gar nicht mehr den Anbieter zur Herausgabe der Profile auffordern müssen. Durch diese Praxis können sich u. U. unangenehme Folgen für einzelne Bürger ergeben. So wurde z. B. einer jungen Frau von 18 Jahren aus Deutschland die Einreise in die USA verweigert, da US-Beamte ihre privaten und persönlichen Facebook-Nachrichten gelesen und darin ihrer Ansicht nach unliebsame Details gefunden hatten. Die junge Frau hatte sich mit ihren amerikanischen Gasteltern darüber ausgetauscht, wie sie sich bei der Einreise in die USA verhalten und auf Fragen der Zollbeamten antworten sollte.[4]

Mittels der Daten werden benutzerorientierte **PERSÖNLICHKEITSPROFILE** erstellt.

In Anbetracht der negativen Folgen, die mit der Erstellung und Speicherung von Persönlichkeitsprofilen einhergehen können, sollte man sich auch immer vor Augen führen, dass die von uns angefertigten Persönlichkeitsprofile online gespeichert sind. Größtenteils befinden sie sich auf riesigen, hochdimensionierten Servern. Gelangen Unbefugte wie z. B. Hacker daran, geben diese Profile ihnen mannigfaltige Möglichkeiten. Sie können unsere Profile in Ruhe analysieren, unsere persönlichen Schwachstellen herausfinden, uns über diese identifizierten Schwachstellen angreifen und so direkte oder indirekte (finanzielle) Schäden zufügen.

Der Mythos von „Ich habe doch nichts zu verbergen“

Oftmals ist es aber nicht mehr notwendig, dass Hacker diese Profile von Servern stehlen. Vielfach können versierte Angreifer schon mittels der über uns im Internet verfügbaren Informationen ein Persönlichkeitsprofil von uns erstellen. Dadurch, dass sich viele Leute über soziale Netzwerke mitteilen, offenbaren sie oftmals bewusst oder unbewusst Informationen von sich, die sie, wenn sie sich über die mögliche Reichweite dieser Informationsbekanntgabe bewusst wären, niemals preisgeben würden. Hierzu ein kleines Beispiel: Dem Namen des eigenen Haustieres messen wir oftmals wenig Bedeutung zu. Daher würde praktisch auch jeder es zunächst für unbedenklich halten, diesen Namen via Facebook oder Twitter der Welt mitzuteilen. Man sollte sich jedoch darüber im Klaren sein, dass sich aus diesem Verhalten erhebliche Konsequenzen ergeben können. Ist nämlich der Name des Haustieres z. B. zugleich das Passwort für das eigene E-Mailpostfach oder die Antwort auf die Sicherheitsabfrage zum Wechseln eines Passworts, sollte man mit dieser Information nicht unbedarft umgehen. Weil durch die Preisgabe dieser Information über Facebook, Twitter und Co. diese Information frei verfügbar ist, sind Unbefugte, ohne viel Aufwand betreiben zu müssen, in der Lage, sich Zugang zum E-Mailpostfach zu verschaffen. Dass dieses Szenario nicht fiktiv, sondern durchaus real ist, zeigt uns der im Jahre 2012 bekanntgewordene „Hack“ des E-Mailkontos des amerikanischen Präsidentschaftskandidaten Mitt Romney.[5]

Man sollte sich daher von der althergebrachten Auffassung verabschieden, dass die Daten, die man bei der Nutzung der neuen Medien preisgibt, unwichtig seien und man ja auch nichts zu verbergen habe. Computern in Verbindung mit der entsprechenden Software reicht oftmals schon eine kleine Sammlung eigentlich „inhaltsloser“ Daten (Metadaten) aus, um z. B. die genauen Umstände eines Sachverhaltes zu rekonstruieren. Zu den Metadaten zählt man alle Informationen, die nicht den Kommunikationsinhalt betreffen, sondern sich auf die Umstände einer Kommunikation beziehen. Hierzu zählen beispielsweise Information darüber, mit wem man zu welcher Zeit wie lange und von wo aus kommuniziert hat. Metadaten sind auch die Informationen, die im Rahmen der Vorratsdatenspeicherung durch die Telekommunikations-Dienstanbieter gespeichert werden sollen.

Um aufzuzeigen, welchen Informationswert Metadaten besitzen können, haben Forscher der amerikanischen Stanford Universität ein Experiment durchgeführt. Bei diesem analysierten sie mit Computern und der entsprechenden Software die von 500 freiwilligen Probanden gesammelten Metadaten. Nach Abschluss des Experimentes waren die Forscher schockiert, was für Informationen sie durch die Analyse dieser vorher als unbedeutend empfundenen Daten erhalten hatten. So konnten sie anhand der ihnen zur Verfügung stehenden Metadaten auf Geschlechtskrankheiten, außereheliche Affären, Waffenbesitz, Drogenhandel u. A. m. schließen.[6] Auch Projekte wie das des Holländers Ton Siedsma zeigen z. B. eindrucksvoll die Macht von Metadaten auf, die ein Smartphone von uns speichert.[7]

Dass sich die Strafverfolgungsbehörden für Metadaten so brennend interessieren, liegt daran, dass sie über die entsprechende Software verfügen, um an-

hand von Metadaten den Hergang bzw. die Umstände einer Straftat zu rekonstruieren. Es ist ihnen damit aber auch möglich, ziemlich exakte Vorhersagen über zukünftige Verhaltensweisen einer Person bzw. Gruppe zu treffen. Metadaten – in Verbindung mit weiteren Daten wie beispielsweise aus sozialen Netzwerken – werden schon heute dazu verwendet, um noch nicht verübte Verbrechen vorherzusagen.[8] Somit ist das, was in Hollywood-Filmen wie z. B. in „Minority Report" noch als Zukunftsvision dargestellt wurde, heute aufgrund unserer gespeicherten Daten Wirklichkeit geworden.

Die meisten Nutzer geben ihre Metadaten zu SORGLOS preis.

Dieses und die zuvor genannten Beispiele sollen verdeutlichen, dass man mit der Aussage, dass die Daten, die man durch die Nutzung der neuen Medien von sich preisgibt, unbedeutend seien, vorsichtig sein sollte. Vielmehr sollten wir uns eingestehen, dass wir bereits heute nicht mehr in der Lage sind, alle potenziellen Risiken bzw. Gefährdungen vorherzusehen und einzuschätzen, die sich aus den über uns bereits gesammelten digitalen Daten ergeben können.

Aus der Vergangenheit lernen

Dass bestimmte, auch im Internet dokumentierte Verhaltensweisen, Positionen oder persönliche „Besonderheiten" heutzutage gesellschaftlich erwünscht und vielleicht sogar gefördert werden, heißt noch lange nicht, dass dies in 10 oder 20 Jahren auch so sein wird. Die Vergangenheit zeigt, dass es oftmals sehr nachteilig für manche Menschen sein kann, wenn andere Personen z. B. Kenntnis von ihrer Religion, ihrer sexuellen Orientierung oder anderen persönlichen Besonderheiten hatten. So extrem und drastisch es auch klingen mag – aber hätten die Nationalsozialisten damals über die Informationen verfügt, die heute frei im Internet verfügbar sind und hätten sie die Auswertungsmöglichkeiten gehabt, die uns moderne Computer und Software heute bieten, wären die Ausmaße und Folgen der Naziherrschaft höchstwahrscheinlich noch viel katastrophaler geworden als sie es waren.

In der Vergangenheit haben die meisten Bürger dem Schutz ihrer Daten keine große Bedeutung beigemessen, wohl auch deshalb, weil ihre Daten nicht wahllos gesammelt und mittels Computer sortiert und abgespeichert wurden. Vielmehr befanden sich die über sie gesammelten Daten verteilt in vielen dicken Akten bzw. unterschiedlichen Archiven. Mangels der Fähigkeit, diese Daten auf unterschiedliche Weise miteinander in Verbindung zu setzen, war es so auch nur schwer möglich, aus den gesammelten Daten entsprechende Rückschlüsse zu ziehen bzw. Zusammenhänge herzustellen. So konnte man sich in Sicherheit wiegen, „anonym" zu bleiben bzw. sicher sein, dass die in den Akten enthaltenen „Geheimnisse" auch geheim bleiben.

Doch auch schon in der Vergangenheit lassen sich mahnende Beispiele dafür finden, dass eine systematische Datensammlung und Auswertung von Personen mit bestimmten „Kriterien" für

die Betroffenen erhebliche Konsequenzen nach sich ziehen kann. Ein schreckliches und wenig bekanntes Beispiel ist hierfür die sogenannte „Rosa Liste". In dieser Liste wurden seit der Kaiserzeit alle männlichen Homosexuellen registriert, um sie auf Straftaten hin nach dem damaligen § 175 des Strafgesetzbuches zu überwachen. Nachdem diese Liste in die Hände der Nationalsozialisten fiel, ergaben sich hieraus tragische Konsequenzen für diejenigen, die darin verzeichnet waren. Weil sie auf Grund ihrer homosexuellen Neigungen der Ideologie der Nationalsozialisten nach als minderwertig galten, wurden sie systematisch verfolgt, deportiert und oftmals auch ermordet.[9]

Fazit

Durch die vorangegangenen Ausführungen sollte deutlich werden, dass eine anlasslose Speicherung von Daten auf Vorrat insgesamt als sehr problematisch anzusehen ist. Man sollte sich auch davon verabschieden, zwischen einer (bösen) „staatlichen" und einer (guten) „privaten" Vorratsdatenspeicherung zu unterscheiden. In beiden Fällen können zu viele Informationen ungeahnte negative Konsequenzen für die Betroffenen nach sich ziehen. Sind unsere Daten erst einmal vorhanden, können sie durch den Einsatz von Computern und der entsprechenden Software von wem und zu welchen Zwecken auch immer ausgewertet werden.

Ein grundsätzlich RESTRIKTIVER Umgang mit dem persönlichen Datenmaterial ist ratsam.

Aus diesem Grund ist es essenziell, dass die Erhebung und Verarbeitung unserer Daten nicht nur für die staatliche Tätigkeit reglementiert wird, sondern vielmehr auch für den privaten Bereich. Die derzeitigen gesetzlichen Regelungen verhindern nach Erfahrung des Verfassers nicht, dass die außerstaatliche Vorratsdatenspeicherung aufhört. Vielmehr ist das Gegenteil der Fall. Aufgrund der Internationalität der Datensammler, der damit einhergehenden Intransparenz der Datenverarbeitung und der fehlenden Ressourcen für die Verfolgung von Verstößen seitens der Aufsichtsbehörden wird es immer illusorischer, auf Abhilfe zu hoffen. Daher wird es für jeden Einzelnen immer wichtiger, sich datensparsam zu verhalten. Denn wenn man keine Daten von sich preisgibt, muss man auch keine Angst haben, dass sich hieraus unkalkulierbare Risiken für einen ergeben.

Es empfiehlt sich dringend, die Verantwortung nicht nur auf andere abzuschieben, sondern sich auch selber vor den Fangarmen der Datenkraken zu schützen. Das erfordert aber auch, dass man sich von lieb gewonnenen Funktionalitäten und Mehrwerten der neuen Medien distanzieren muss. Im Prinzip sollte jeder ein persönliches Risikomanagement durchführen und sich hierbei mit der Frage, „Können der Mehrwert und die vermeintlichen Vorteile, die uns die neuen Medien und die kostenlosen Dienste bringen, den Preis aufwiegen, den wir bezahlen, wenn wir unsere persönlichen Daten an Wildfremde herausgeben?", auseinandersetzen.

Eine allgemein gültige Antwort bzw. Empfehlung dazu kann der Verfasser nicht geben. Vielmehr ist es eine sehr persönliche Entscheidung, die jeder Einzelne von uns selber für sich treffen muss. Wichtig ist hierbei jedoch, dass man ehrlich zu sich selbst ist und sich

Jeder hat sein Datenmanagement und somit auch sein diesbezügliches Risiko **SELBER** in der Hand.

kritisch u. a. mit den vorstehend dargestellten Hintergründen der Nutzung der „neuen Medien“ auseinandersetzt. ///

/// GERALD SPYRA, LL.M.

ist Rechtsanwalt mit Spezialisierung auf das Datenschutz- bzw. IT-Recht. Darüber hinaus ist er externer betrieblicher Datenschutzbeauftragter mit hoher Affinität für Themen aus dem Bereich der IT-Sicherheit, Köln.

Anmerkungen

[1] Einen guten Überblick über die Problematik und die einzelnen Positionen gibt http://de.wikipedia.org/wiki/Vorratsdatenspeicherung

[2] Nähere Informationen zu diesem Problem und Empfehlungen, wie man sich vor dem ungewollten Abfluss (auf Android) Smartphones schützen kann, gibt das vom Verfasser und seinem Geschäftspartner Herr Kuketz ins Leben gerufene Projekt „Your Phone – Your Data“, abrufbar unter http://www.kuketz-blog.de/your-phone-your-data-teil1/

[3] http://mashable.com/2014/04/26/big-data-pregnancy/

[4] https://netzpolitik.org/2013/usa-beamte-konnen-facebook-nachrichten-von-einreisenden-lesen/

[5] http://www.spiegel.de/netzwelt/netzpolitik/mitt-romneys-e-mail-account-gehackt-a-837228.html/

[6] http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html und http://sz.de/1.1916548

[7] https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/

[8] http://www.basicthinking.de/blog/2014/07/03/predictive-policing-strafverfolgung-per-algorithmus/

[9] http://de.wikipedia.org/wiki/Rosa_Liste und http://de.wikipedia.org/wiki/Homosexualitaet_in_der_Zeit_des_Nationalsozialismus

[10] https://www.datenschutz-hamburg.de/news/detail/article/datenschutz-erfordert-schlagkraeftige-kontrollbehoerden.html