

Hanspeter Thür, 64, hat an der Universität Basel Jura studiert. Er arbeitete als Gerichtsschreiber und Redaktor, bevor er in Aarau eine Anwaltskanzlei eröffnete. Hanspeter Thür war von 1987 bis 1999 Nationalrat für die Grüne Partei. Seit September 2001 ist er eidgenössischer Datenschutzbeauftragter, seit Mitte 2006 auch Öffentlichkeitsbeauftragter. Er ist Vater einer erwachsenen Tochter und lebt in Aarau.



DIGITALE HERAUSFORDERUNGEN

«Der mündige Bürger ist eine Notwendigkeit»

Seit die gross angelegte Internetüberwachung durch die US-amerikanischen Geheimdienste im Sommer aufgefliegen ist, ist das Thema Datensicherheit überall präsent. Der Datenschutzbeauftragte Hanspeter Thür sagt, was der Einzelne dafür tun kann. Und er warnt vor der Brille Google Glass, die bald auf den Markt kommen soll.

Interview **Stefan Wichmann** Fotos **Romed Fritsche**

Herr Thür, kleben Sie Ihre Webcam ab?

Schauen Sie (zeigt auf das Gerät), mein Laptop ist zugeklappt und an einen Monitor angeschlossen, der keine Kamera besitzt. Jeder Benutzer eines iPads oder Laptops sollte sich vergewissern, dass die Kamera ausgeschaltet ist, wenn sie nicht in Gebrauch ist.

Mehr und mehr technische Geräte wie zum Beispiel Flachbildfernseher und Spielekonsolen sind mit Kamera und Mikrofon ausgestattet. Beim Installieren von Apps erlaubt der Nutzer den Softwarefirmen, auf Webcam und Mikrofon zuzugreifen. Somit hebt er freiwillig den Datenschutz aus. Was halten Sie von dieser Entwicklung?

Sie ist unglaublich spannend, dynamisch und eine riesige Herausforderung, vor allem für den Nutzer. Er wird täglich mit neuen Möglichkeiten konfrontiert und ist letztlich überfordert, die gesamte Tragweite seiner Entscheidung zu erfassen. Der Anwender ist zu schnell bereit, den Datenschutzbedingungen zuzustimmen, das ist eine Realität. Den Leuten mitzuteilen, sie mögen das Kleingedruckte lesen, ist eine nette Aufforderung, welcher der gehetzte Nutzer selten nachkommt. Der Konsument muss sich bewusst sein, dass über die Geräte Informationen an Dritte gelangen, die er nicht weitergeben möchte. Wir dürfen nicht nur die technischen Vorteile eines neuen Produktes beachten, sondern stehen auch in der Verantwortung, die Kehrseite der Medaille zu beachten. Das ist der Appell meiner Behörde, den wir in regelmäßigen Abständen unter die Leute bringen.

Wäre eine bessere Auskunftspflicht über die technischen Möglichkeiten im Fachgeschäft oder beim Händler nicht sinnvoll?

Angesichts der Überforderung der Konsumenten wäre es angebracht, das System umzukehren. Die Hersteller sollten gewisse Forderungen bei der Produktion solcher Geräte oder Software beachten müssen. Ich fasse sie mit dem Stichwort «privacy by design» zusammen. Dies bedeutet, dass die Grundeinstellungen eines Produkts oder einer Dienstleistung grösstmöglichen Schutz der Privatsphäre gewährleisten müssen: Die Kamera an Laptops oder Flachbildschirmen ist in der Grundeinstellung ausgeschaltet, und jede Datenverarbeitung oder -nutzung von aussen bedarf der Zustimmung des Anwenders. Heute stellt der Benutzer seine Daten unwissentlich zur Verfügung und nutzt den Service oder das Programm kostenlos. Er sollte aber die Wahl haben, diesem Deal zuzustimmen oder aber den Dienst zu bezahlen und im Gegenzug seine Daten nicht preiszugeben. Diese Wahl ist nicht gegeben, die Hersteller und Entwickler stellen den User vor vollendete Tatsachen. Weiter müssen die Allgemeinen Geschäftsbedingungen verständlicher sein, sodass Datenschutzerklärungen nicht irgendwo unter «ferner liefern» abgehandelt werden. Es muss auf Gesetzesstufe geregelt werden, dass die Nutzer wählen können und dass Einstellungen mit dem grösstmöglichen Schutz angeboten werden.

Wie hat sich Ihre Arbeit seit der Aufdeckung von «Prism» geändert?

Seit den Veröffentlichungen von Edward Snowden und der dadurch publik gewordenen grossangelegten Überwachung durch die US-amerikanischen Geheimdienste haben sich die öffentliche Wahrnehmung und vor allem die Auseinandersetzung mit dem Schutz der eigenen Daten stark verändert. Auf zahlreichen Wegen, wie zum Beispiel Vorratsdatenspeicherung, Speicherung von Nutzerdaten in sozialen Netzwerken, kommen immer grössere Datenberge zusammen, die mit immer effizienteren Analyseprogrammen auf Korrelationen hin durchforscht werden. Dabei können unglaubliche Erkenntnisse gewonnen werden. Beispielsweise hat man herausgefunden, dass sich eine Scheidung anbahnen kann, wenn eine Frau plötzlich teuren Schmuck kauft. Oder: Im Auftrag einer Supermarktkette wurde das Einkaufsverhalten von Frauen analysiert, womit werdende Mütter identifiziert werden konnten.

Wie informieren Sie sich?

Wir haben IT-Spezialisten, die sehr breit aufgestellt sind und ein grosses Spektrum an technischen Entwicklungen überblicken. Sie setzen sich fortlaufend in Kenntnis, wobei alle Arten von Quellen erwünscht sind. Unser Pressedienst informiert sich ebenfalls über technische Neuerungen und wählt für den Datenschutz relevante Themen aus. Daraus ergeben sich dann Aufträge für unsere Techniker, Potenziale zu beurteilen und Strategien zu entwickeln: Wie lässt sich mit neuen Situationen datenschutzkonform umgehen? Diese hausinternen Analysen sind wichtig, um auf dem neuesten Stand zu bleiben. Weiter haben wir einen Testrechner, der abgekoppelt von unserem abgesicherten Netzwerk einen PC, wie er in jedem Haushalt stehen könnte, simuliert. An diesem Gerät können wir Beobachtungen im Internet vertiefen und Schwächen einzelner Programme oder Dienstleistungen aufdecken.

Wie steht es bei Business-Netzwerken wie Xing und LinkedIn um den Schutz der persönlichen Daten?

Wie bei jedem sozialen Netzwerk muss dem Anwender hier bewusst sein, dass der Anbieter mit den zur Verfügung gestellten Daten arbeitet und diese auswertet. Diese Netzwerke sind darauf fokussiert, Informationen auszutauschen. Der Nutzer wird darüber per E-Mail informiert und stimmt in den meisten Fällen den Neuerungen ungelesen zu. Unter Umständen ändern Anbieter die Geschäftsbedingungen laufend, sodass plötzlich ein Kreis von Leuten mit Informationen bedient wird, die man als Nutzer nicht im Auge hatte. Wer sich im Internet bewegt, muss dynamisch, flexibel und neugierig sein. Wir alle müssen uns ständig auf dem Laufenden halten. Der mündige Bürger ist eine Notwendigkeit, ohne die der Datenschutz nicht funktioniert. Ich kann mir keine Gesellschaft vorstellen, die nicht auf Selbstverantwortung basiert. Soll der Staat uns permanent richtiges Verhalten lehren? Das kann in einer liberalen Gesellschaft nicht das Ziel sein.

Wie steht es mit der Sensibilisierung bei den Jungen, etwa in den Schulen, in Bezug auf den richtigen Umgang mit sozialen Netzwerken?

Meine Behörde hat in den letzten Jahren zusammen mit privaten Organisationen diverse Kampagnen für Schülerinnen



und Schüler organisiert. Dabei geht es nicht um neue Lehrfächer, sondern eher darum, dass die Lehrpersonen den Umgang mit dem Internet und sozialen Netzwerken in den bestehenden Unterricht miteinfließen lassen. Viele Schulen wollen ihre Kommunikation über soziale Netzwerke abwickeln. Wir haben eine Reihe von Forderungen aufgestellt, die erfüllt sein müssen, um den Datenschutz jedes Beteiligten zu berücksichtigen. Diese haben wir der Erziehungsdirektion mitgeteilt, damit Rahmenbedingungen geschaffen werden, welche Firmen wie Microsoft und Apple daran hindern, die Daten einzelner Schüler zu sammeln. Die Schulen sind aufgefordert, die Verträge mit den Softwareherstellern diesbezüglich zu ändern.

Warum ist es grossen Firmen, wie zum Beispiel Amazon oder Facebook, gestattet, auf meine Daten zurückzugreifen?

Alles, was ich zur Verfügung stelle auf irgendeinem Kanal und somit im Internet öffentlich mache, können Dritte nutzen. Die Grenze des Erlaubten ist dort, wo die von einer Firma gesammelten Daten die Qualität eines Persönlichkeitsprofils erreichen, also eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit eines Menschen erlaubt. Erstellt eine Firma solch ein Profil aufgrund frei verfügbarer Daten, müsste sie die beschriebene Person darüber informieren, und der Betroffene könnte die Verbreitung ablehnen. Der Rechtsinhaber muss sich zur Wehr setzen können. Sollte sich herausstellen, dass dies in

I N N O V A T I O N E N

Neue Gefahr durch neue Technik

GOOGLE GLASS Der Suchmaschinen-gigant Google bringt bald die Brille Google Glass in den Handel. Mit Hilfe einer Kamera, dem permanenten Internetzugang und einem Miniprojektor, der die Daten auf dem Brillenglas abbildet, soll dem Konsumenten das Alltagsleben erleichtert werden. Das Persönlichkeitsrecht, welches die Veröffentlichung von Bildern von Privatpersonen ohne ihr Einverständnis verbietet, verliert damit seine Relevanz. Welche Daten Google aufzeichnet und was damit passiert, bleibt Firmengeheimnis.

ÜBERWACHUNG LEICHT GEMACHT Nach dem Erwerb eines Produktes sollte einem der Nutzen freistehen. Die Hersteller koppeln Betriebssystem und Software jedoch immer häufiger an den Computer: Microsoft ist es gelungen, sein Betriebssystem Windows RT fest an die Hardware zu koppeln, Apple beschränkt seine iPads schon lange. Ein Tausch etwa gegen die frei verfü-

bare Linux-Software ist für den Durchschnittsnutzer kaum möglich. Lediglich von Microsoft oder Apple zur Verfügung gestellte Apps lassen sich installieren. Bei einem grossen Teil der verfügbaren Apps willigt der Konsument zudem automatisch ein, der Softwarefirma Zugriff auf die Webcam, das Mikrofon und die gespeicherten Daten zu gestatten.

DATENSPEICHERUNG IN CLOUDS Durch immer grösser werdende Datenmengen auch bei Privatpersonen gewinnen Datenspeicherdienste, sogenannte Clouds, an Bedeutung. Hierbei speichert der Nutzer seine Daten extern auf grossen Servern, die über den gesamten Globus verteilt sind. Dem Nutzer wird aktiv ausschliesslich der praktische Nutzen, nämlich der ortsunabhängig unbeschränkte Zugriff auf die eigenen Daten, verkauft. Die dabei entstehenden Risiken verschweigen die Anbieter solcher Dienste dem Konsu-

menten. Sowohl die oft unzureichende Absicherung der Daten, zum Schutz vor Dritten, als auch die Auswertung der Daten durch den Anbieter sollten jedoch zur Vorsicht mahnen.

KREDITKARTEN MIT NFC Neuere Kreditkarten bieten die Möglichkeit des «kontaktlosen» Zahlens, durch sogenannte Near Field Communication. Hierbei wird ein RFID (Radio-Frequenz-Chip) in der Karte untergebracht, der mit dem Bezahlterminal kommuniziert. Die Anwendung dieser neuen Technik birgt aber Gefahrenpotenzial. Betrüger könnten versuchen, Geldbeträge mit Hilfe von eigens entwickelten Geräten abzubuchen. Damit dies nicht passiert, gibt es einen einfachen Trick: Falten Sie ein Stück Aluminiumfolie so, dass es das Geldscheinfach der Geldbörse ausfüllt. Das Portemonnaie ist nun gegen Strahlen abgeschirmt und somit sicher vor einem Zugriff durch Dritte.

grossen Stil erfolgt und somit gesetzeswidrig ist, können wir eingreifen und gegen diese Firma juristisch vorgehen. Im Fall Google Street View sind wir bis vor Bundesgericht gegangen, um einen besseren Persönlichkeitsschutz durchzusetzen.

Ist das Thema Internet und neue Technologien in der Politik ausreichend vertreten, oder besteht Handlungsbedarf bei den politischen Vertretern, um neue Gesetze zu erlassen?

Das Thema interessiert zunehmend auch Politiker, allerdings bisher eher vereinzelt. Die Sensibilität nimmt unter den Politikern zu, ist aber noch ausbaufähig. Immerhin: Der Einsatz von kleinen, mit Kameras bestückten Drohnen beschäftigt mittlerweile auch die Parlamentarier.

Was halten Sie vom zunehmenden Einsatz von Drohnen?

Wer mit Hilfe von Drohnen Menschen filmt oder fotografiert und diese Aufnahmen veröffentlicht oder verkauft, verstösst gegen das Gesetz. Die Frage ist nur, wie sich der Vollzug dieses Gesetzes gestaltet. Die Geräte werden immer billiger, potenter, kleiner und dadurch schlechter wahrnehmbar. Hier liegt das Problem in der unbemerkten Verletzung der Privatsphäre.

Denken Sie, wir gewöhnen uns daran und Datenschutz spielt in 20 Jahren keine Rolle mehr?

20 Jahre in die Zukunft zu schauen, ist schwierig. Orwell hätte sich wohl nicht vorstellen können, dass das, was er vor 60 Jahren geschrieben hat, heute bei weitem übertroffen wurde. Die Realität ist viel dramatischer, als es seine Vorstellungskraft war. Wir müssen Entwicklungen immer auf ihr Missbrauchspotenzial hin prüfen und gegebenenfalls Gesetze anpassen. Das Gesetz hinkt der Realität stets hinterher, manchmal nicht nur ein bisschen, aber dies ist nicht anders möglich. Das Potenzial der Überwachung und Analyse entwickelt sind ständig, entsprechende Gesetze zu verfassen, wird immer komplizierter. Doch weitere Missbräuche und Übergriffe werden den Datenschutz wieder ins Bewusstsein rufen, ähnlich wie nach der Aufdeckung von «Prism». Es wird Gegenbewegungen geben, weil der Mensch sich nicht permanent und in seiner Totalität überwachen und kontrollieren lassen will. Unternimmt der Gesetzgeber beispielsweise im Bereich Drohnen nichts, wird mit Sicherheit jemand Gegenstrategien auf technischer Ebene entwickeln, wie man solche Geräte ausschalten kann.

Wie reagierte Google auf den Brief, in dem Sie zusammen mit Datenschützern aus der ganzen Welt zum Dialog aufrufen bezüglich Google Glass, einer Brille, mit der man unbemerkt filmen und fotografieren kann? Dieses Gerät, das bald auf den Markt kommen soll, hat das Potenzial, den Datenschutz auszuhebeln.

Google kommuniziert sehr spärlich und gibt sich bedeckt, ähnlich wie die Firma Facebook, die nur in sehr seltenen Fällen reagiert.

Warum wird ein Verkaufsverbot nicht in Betracht gezogen?

An sich wäre das die letzte Möglichkeit. Dafür müsste sich aber schon ein gesamter Wirtschaftsverbund wie zum Bei-



KOMMENTAR STEFAN WICHMANN

Fortschritt vor Ethik

In einer zunehmend digitalisierten Welt, wo Computersysteme ganze Wirtschaftszweige und infrastrukturelle Einrichtungen übernehmen, zum Beispiel bei Aktienkäufen oder der Verkehrssteuerung, steht der technische Fortschritt im Vordergrund. Sowohl im Hardwarebereich als auch im Softwaresektor stellen die Produzenten den Konsumenten immer öfter vor vollendete Tatsachen und verwehren ihm Wahlmöglichkeiten: Ob Mikrophon und Kamera am Flachbildfernseher oder der neuen Spielekonsole eingeschaltet sind, bestimmen sie. Das Internet und seine Industrie entgleiten zunehmend der Kontrolle der Volksvertreter, begünstigt durch die Monopolstellung der grössten beteiligten Firmen. Nationales Recht gerät somit ins Hintertreffen gegenüber der Geschäftspolitik multinationaler Konzerne wie Google, Facebook & Co. Der Bürger ist meist ahnungslos und verkennt die Gefahr. Das seitenlange Kleingedruckte lesen wir äusserst selten, stimmen den Nutzungsbedingungen zu und machen den Weg frei für völlige Kontrolle und Überwachung. Die Datenschutzbeauftragten und Verbraucherschützer stehen vor einer schweren Aufgabe, gilt es doch, Errungenschaften wie das Recht auf Privatsphäre als auch die Presse- und Meinungsfreiheit zu schützen. Der Kernpunkt besteht darin, den Bürger und Konsumenten für bestehende und kommende Herausforderungen in Bezug auf das Internet und die damit verbundenen technischen Entwicklungen zu sensibilisieren. Beim Erwerb eines Produktes gilt es, genauer hinzuschauen beziehungsweise sich zu informieren, welche Folgen technische Neuerungen für jeden Einzelnen haben.

spiel Europa zusammentun. Aber bei der momentanen wirtschaftlichen Lage schein dazu kein Land bereit zu sein.

Was halten Sie persönlich von der Google-Glass-Brille?

Ich halte dieses Gerät für hochgradig gefährlich, weil man nicht sieht, was der Träger damit macht. Jeder Brillenträger könnte mich potenziell filmen, fotografieren, überwachen oder Informationen über mich aus dem Netz abrufen. Mit dieser Brille kann sehr viel getan werden, was den Persönlichkeitsschutz gefährdet. Ich schliesse nicht aus, dass künftig der eine oder die andere einen Google-Glass-Nutzer auffordert: «Brille weg, aber sofort!» ■