STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz

Der Faktor Mensch

Frederick Richter, LL. M.

Zwei Dinge zeigten sich recht deutlich, als Mitte Januar die Geschichte vom großen „Datenklau" umging: Viele Leute differenzieren manchmal ungern. Und so manche Leute würden sich nur allzu gern auf andere Leute verlassen, und am liebsten auf den Staat.

Auslöser beider Phänomene war das Bekanntwerden einer umfangreichen unrechtmäßigen Offenlegung von personenbezogenen Daten. Ein junger Mann aus der Provinz hatte, anscheinend im Alleingang,[1] im Dezember 2018 in einer Art „Adventskalender" auf Twitter haufenweise Daten von Politikern und Prominenten veröffentlicht. Die nach dieser Aufdeckung sofort loseilende Berichterstattung erging sich nicht nur in Superlativen („Mega-Hack"), sie hielt sich auch nicht lange mit der Unterscheidung zwischen Datenschutz und Datensicherheit auf. Es wurde so munter vermengt und vermischt, dass oft unklar blieb, ob hier die Redakteure etwas verwechselten oder die jeweils zitierten Politikerinnen und Politiker oder beide.

Frederick Richter ist Ständiger Autor bei „Privacy in Germany". Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Schutz meint auch Sicherheit

Nun mag es Fachleuten zwar leichtfallen, zwischen dem Schützen der informationellen Selbstbestimmung und dem Persönlichkeitsrecht durch den Datenschutz einerseits und dem Sichern aller Daten, auch der anonymen, durch Regeln zur IT-Sicherheit andererseits saubere Trennlinien zu ziehen und die – durchaus vorhandenen – Überschneidungen deutlich zu machen. Doch könnte man sich angesichts der erwähnten Differenzierungsschwäche durchaus fragen, ob die jeweiligen Kenntnisse beider Fachgebiete nicht im Verbund vermittelt werden sollten.

1 Datenklau möglicherweise doch nicht von Einzeltäter begangen; Meldung im rbb vom 16.01.2019; abrufbar unter: www.rbb24.de/politik/beitrag/2019/01/datenklau-zweifel-einzeltaeter-kontraste.html.

Auch im Gesetz findet sich eine Verschränkung der beiden Themenkreise schon lange. Einige Jahre nach deren Verankerung im Bundesdatenschutzgesetz wurde eine Pflicht zu technisch-organisatorischen Maßnahmen zum Schutz gegen unrechtmäßige Verarbeitung auch in die EU-Datenschutzrichtlinie von 1995 aufgenommen.[2] Die weitere Festschreibung einer Pflicht zur „Sicherung der Verarbeitung" in Art. 32 DSGVO war daher nur konsequent, nachdem der Europäische Gerichtshof 2014 anerkannt hatte, dass das Grundrecht auf Datenschutz aus Art. 8 der Europäischen Grundrechtecharta auch den technisch-organisatorischen Schutz gegen Angriffe von außen umfasst.[3] Selbst wenn die DSGVO es nunmehr abstrakter angeht als zuvor § 9 BDSG-alt mit seiner dezidierten Anlage, so ist die Grundrichtung doch mittlerweile völlig klar: Kein Datenschutz ohne Datensicherheit. Und umgekehrt fördern Bemühungen um Datenschutz-Compliance auch die technische Sicherheit.[4]

Warum getrennt aufklären?

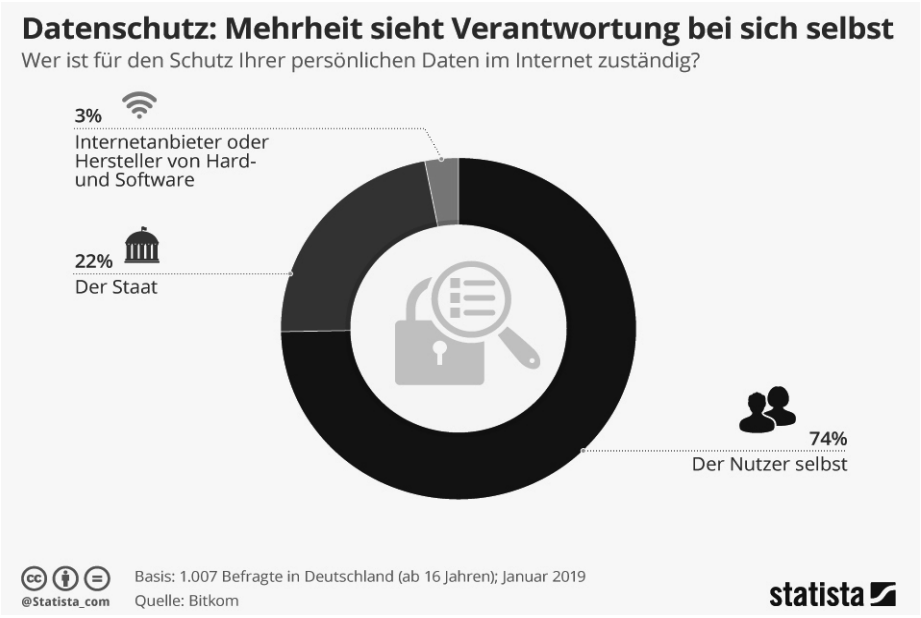
Läge es dann nicht nahe, beide Materien den Nutzerinnen und Nutzern gemeinsam zu erklären und zu vermitteln? Die klassische Unterscheidung zwischen IT-Sicherheit und Persönlichkeitsschutzrechten mag juristisch und technisch völlig gerechtfertigt sein. Doch scheint es keinen Vorteil zu bringen, hier getrennt zu marschieren, wie ich bereits an anderer Stelle anmerkte.[5] Ein Zusammenspiel aller Stellen würde Erfolge bei der Sensibilisierung der Menschen für die Gefahren des Datenumgangs im Netz vereinfachen. Das für die Sicherheit der Daten zuständige Bundesamt muss daher ebenso gut ausgestattet werden wie die für den Schutz der Daten zuständigen Einrichtungen. Warum sollten Programme wie „BSI für Bürger" nicht mit Aktionen wie „Datenschutz geht zur Schule" zusammenarbeiten?

Geht der Blick in Sachen „Datenklau" von öffentlichen Aufklärungsinitiativen dann hinüber zu den privaten Verbraucherinnen und Verbrauchern, so wird eines klar: Es wird nicht ohne deren Mithilfe gehen. Und damit sind wir wieder beim Selbstdatenschutz. Dieses Element der Abwehr von Datenmissbrauch bleibt unverzichtbar, auch wenn manche es nicht hören wollen. Das heißt nicht etwa, von allen Leuten eine IT-Fortbildung zu verlangen. Das heißt auch nicht, die Leute alleinlassen zu wollen mit der Last der Sicherung ihrer informationstechnischen Infrastruktur. Niemand wird sich in die Tiefen der asymmetrischen Verschlüsselung einarbeiten wollen, der nicht eine besonders ausgeprägte Technikaffinität hat. Selbstdatenschutz zu verlangen, heißt aber, die Menschen nicht völlig aus der Verantwortung zu lassen. Mit anderen Worten: Weder ganz tolle Aufklärungsprogramme noch die Hersteller der digitalen Systeme oder der Staat werden den Faktor Mensch ganz abdecken können. Und die Leute erwarten dies auch gar nicht, sondern sehen sich selber in Pflicht, wie eine Umfrage zum Jahresbeginn zeigte.[6] Sie werden schlicht nicht verhindern können, dass unbedarfte Nutzer auf Links in Phishing-Mails klicken. Der Nutzer wiederum wird solche Fehltritte auch nicht immer komplett vermeiden können, doch wäre etwas mehr Zurückhaltung hilfreich, frei nach einem Motto „think a little bit before you click on it".

Nicht nur auf andere verlassen

Zwar wäre es durchaus sinnvoll, die Anbieter von Hard- und Software hinsichtlich Sicherheitsupdates stärker in die Pflicht zu nehmen. Auch könnten sie intensiver an den Leitplanken gegen schwache Passwörter arbeiten und die Vorgaben so einstellen, dass „123456" von nachlässig Nutzenden schlicht nicht mehr gesetzt werden kann. Doch wird es auch mit strengsten, womöglich gesetzlichen, Vorgaben niemals möglich sein, den Schlendrian vollständig zu verbannen. Wer sich partout nicht um die Sicherung seiner IT-Strukturen und „seiner" Daten kümmern will, der lässt sich nicht vor sich selbst schützen. In dieser Hinsicht müssen sich jene, die der Verbraucherschaft am liebsten ein Rund-um-Sorglos-Paket von Gesetzgeber und Industrie anbieten würden, ehrlich machen. Wenn jede Person im Netz ein paar der bekannten Grundregeln beherzigte, wäre schon viel gewonnen. Da darf dann auch gern einmal eine gesunde Portion Skepsis enthalten sein. Denn wer allem und jedem im Netz blind vertraut, kann sich ohne Not sehr schnell gefährden.

Und was die oben erwähnte Differenzierungsproblematik anbelangt: Vom „Selbstdatenschutz" als Schlagwort und Forderung ist die IT-Sicherheit stets mitgemeint, sie ist eine grundlegende Voraussetzung. Denn wenn personenbezogene Daten bereits ungesichert „herumliegen", dann werden Diskussionen um die Feinheiten des materiellen Datenschutzrechts akademisch.



2 Art. 17 Abs. 1 Richtlinie 95/46/EG.

3 EuGH, Urt. v. 08.04.2014 – C-293/12, C-594/12; vgl. auch *Piltz*, in: Gola, DSGVO, 2. Aufl. 2018, Art. 32 Rn. 6.

4 GDPR Compliance Lowers Data Breach Frequency and Impact Says Report; Bericht zur Cisco-Studie bei BleepingComputer.com; abrufbar unter: www.bleepingcomputer.com/news/security/gdpr-compliance-lowers-data-breach-frequency-and-impact-says-report.

5 Kommentar: In der digitalen Welt muss sich auch jeder selbst schützen, in: Die Welt v. 10.01.2019, abrufbar unter: www.welt.de/debatte/kommentare/article186793708/Frederick-Richter-Fuer-mehr-Selbstschutz-in-der-digitalen-Welt.html.

6 Mehrheit sieht Verantwortung für Datenschutz bei sich selbst; Umfrage von BITKOM und statista vom Januar 2019; abrufbar unter: https://de.statista.com/infografik/16771/umfrage-zur-verantwortung-beim-thema-datenschutz.