erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

FIfF-Konferenz 2016

Funktioniert Datenschutz im Unsichtbaren?

Datenschutzgarantien, Transparenz und Intervenierbarkeit in versteckter Informationstechnik

Zusammenfassung des Vortrags von Marit Hansen

Datenschutz bedeutet nicht nur informationelle Selbstbestimmung, sondern dient auch als Korrektiv beim Machtgefälle zwischen Datenverarbeitern und betroffenen Personen. In dem Vortrag geht es um die folgenden Fragen: Kann Datenschutz in versteckter Informationstechnik überhaupt realisiert werden? Bedeutet „Privacy by Default", dass Datenschutz fest eingebaut ist und gar nicht mehr im Blickfeld der Nutzenden stehen müsste? Welche Herausforderungen bestehen angesichts einer für die Betroffenen (und sogar für so manchen Datenverarbeiter) unsichtbaren Funktionalität?

Beim Datenschutz geht es nicht um Daten, sondern um Menschen mit ihren Rechten. Damit ergeben sich bei der Gestaltung von datenschutzfreundlichen Systemen zwei Prüffragen: Welche Auswirkungen hat das System und seine Datenverarbeitung auf Menschen und welche Auswirkungen hat das System und seine Datenverarbeitung auf die Gesellschaft? Die Notwendigkeit des Datenschutzes ergibt sich dabei aus dem Machtgefälle, wichtig ist die Perspektive der Betroffenen. Der Ansatzpunkt des Datenschutzes, um die Menschen zu schützen, sind die personenbezogenen Daten, die durch IT-Systeme verarbeitet werden.

Die klassische Perspektive der IT-Sicherheit sind zwei Personen, die miteinander kommunizieren wollen: häufig Alice und Bob genannt. Bei ihrer Kommunikation werden sie von einer dritten Person – z. B. Eve oder Mallory – bedroht. Der Datenschutz nimmt hier eine neue Sicht ein: Sendet Alice Daten an Bob, so kann auch dieser als Angreifer fungieren, der Datenschutz muss Alice auch vor ihm schützen. Die Datenverarbeitung ist ein potenzieller „Eingreifer", die in Grundrechte (von Alice) eingreift.

Rechtlich wird der Datenschutz durch zwei Grundrechte geschützt, die das Bundesverfassungsgericht aus Artikeln des Grundgesetzes abgeleitet hat: dem Recht auf informationelle Selbstbestimmung und dem sogenannten IT-Grundrecht:

- Datenschutz-Grundrecht 1: „Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen" (informationelle Selbstbestimmung). Aus Anlass der Volkszählung urteilte das Bundesverfassungsgericht am 15. Dezember 1983, dass jeder wissen können soll, wer was über ihn weiß (1 BvR 65/1).

- Datenschutz-Grundrecht 2: „Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme". Zur Online-Durchsuchung urteilte das Bundesverfassungsgericht am 27. Februar 2008, dass es ein Grundrecht gibt auf digitale Intimsphäre und damit präventive staatliche Zugriffe nur bei tatsächlichen Anhaltspunkten einer konkreten Gefahr für ein überragend wichtiges Rechtsgut zulässig sind (1 BvR 37/07, 1 BvR 595/07).

Marit Hansen

Der Datenschutz legt mehrere Grundsätze fest, die bei der Verarbeitung personenbezogener Daten gelten:

- Existenz einer Rechtsgrundlage, in Form einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen

- Zweckbindung
- Erforderlichkeit
- Transparenz
- Betroffenenrechte
- Datensicherheit

Der Datenschutz zielt auf die Sicherheit personenbezogener Daten. Zu den klassischen Schutzzielen der IT-Sicherheit (die durch weitere Schutzziele ergänzt werden können)

- Vertraulichkeit
- Verfügbarkeit
- Integrität

kommen die zusätzlichen Schutzziele des Datenschutzes

- Nicht-Verkettbarkeit
- Intervenierbarkeit
- Transparenz
- Datensparsamkeit

In der heutigen Realität haben wir es mit einigen dominierenden Anbietern zu tun, die in allen Lebenslagen hinter Datenverarbeitungsprozessen stehen können. In Teilen sind diese Anbieter unsichtbar bzw. nicht wahrnehmbar oder unbekannt. Während Anbieter wie PayPal, Apple, Microsoft, Twitter, Amazon, Google, Facebook weithin bekannt sein dürften, sind beispielsweise Anbieter von IT-Infrastruktur wie Akamai möglicherweise vielen Nutzern unbekannt. Es stellen sich Fragen danach, wo und wann die Verarbeitung der Daten stattfindet, wie genau die Datenverarbeitung durchgeführt wird und durch welche Dritten auf die Daten zugegriffen wird.

In der heutigen Realität ist die Datenverarbeitung durch eine komplexe Arbeitsteilung geprägt. Die Endanwender.in, die (vermeintlich) auf eine Webseite zugreift, löst dadurch den Zugriff auf weitere Seiten, häufig sogar hunderte von weiteren Zugriffen aus, die im Hintergrund, also versteckt, stattfinden. Die unsichtbare (und unerwartete) massenhafte Einbindung von Dienstleistern führt zu Sicherheits- und Datenschutzrisiken, es stellt sich die Frage nach der Transparenz der Datenverarbeitung. Selbst wenn der Anwender.in diese Zugriffe im Hintergrund bewusst sind, ist die Praktikabilität von Interventionen angesichts der Menge von Zugriffen zweifelhaft. Zuletzt stellt sich die Frage nach der Verantwortung. Es bleibt festzuhalten, dass es in der heutigen Realität eine massive Marketing-Macht für (unsichtbare) Integration in Angebote gibt. Die Anzahl der Anbieter solcher Dienste ist nicht mehr überschaubar (Quelle: chiefmartec.com Marketing Technology Landscape).

Die Komplexität heutiger Geschäftsprozesse wird häufig in der Cloud verborgen. Neben der (scheinbaren) Vereinfachung ergeben sich dabei neue Fragestellungen: man begibt sich in eine Abhängigkeit von Dienstleistern, die die Cloud-Dienste anbieten, Fremdbestimmbarkeit tritt an die Stelle von Eigenkontrolle und auch hier stellt sich die Frage: „Durch welche Dritten wird auf meine Daten zugegriffen?“

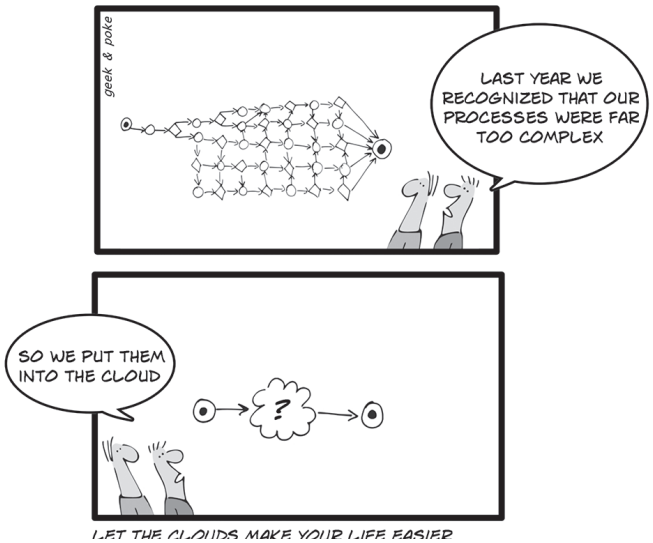
Dazu kommt in der heutigen Realität das „versteckte“ Internet: Internetanbindung zu Hause (im *Smart Home*), im Auto und am Körper (durch *Smart Watches* und Smartphone-Apps). Das Beispiel der Smart-TVs von Samsung ging vor einiger Zeit durch die Medien, wo es in den Bedienungshinweisen heißt:

> *„Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition“ (Samsung Smart TVs Do Not Monitor Living Room Conversations, http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/).*

Samsung trat der Aussage entgegen, dass durch seine Fernsehgeräte die Wohnungen der Nutzer.innen ausgespäht würden.

Die „unsichtbare“ Datenverarbeitung im Smart Home ist auch nicht immer für jeden unsichtbar: Dem „Betreiber“ des Systems, z. B. dem Haushaltsvorstand, Vermieter oder Arbeitgeber sollte bekannt sein, dass im Hintergrund Daten erfasst werden und er ist verpflichtet, Mitnutzer unverzüglich zu warnen. Dies ist nicht neu und gilt schon immer für TK-Anlagen mit Einzelverbindungsnachweis:

> *„[…] Bei Anschlüssen im Haushalt ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass er alle zum Haushalt gehörenden Mitbenutzer des Anschlusses darüber informiert hat und künftige Mitbenutzer unverzüglich darüber informieren wird, dass ihm die Verkehrsdaten zur Erteilung des Nachweises bekannt gegeben werden.*
>
> *Bei Anschlüssen in Betrieben und Behörden ist die Mitteilung nur zulässig, wenn der Teilnehmer in Textform erklärt hat, dass die Mitarbeiter informiert worden sind und künftige Mitarbeiter unverzüglich informiert werden und dass der Betriebsrat oder die Personalvertretung entsprechend den gesetzlichen Vorschriften beteiligt worden ist oder eine solche Beteiligung nicht erforderlich ist. […]“ (§99 Abs. 1 TKG).*



Oliver Widder, CC BY 3.0, http://geek-and-poke.com/something/

Auch die Nutzungsbedingungen von – beispielsweise – WhatsApp verlangen eine Bestätigung, dass Daten nur mit entsprechendem Einverständnis der Betroffenen weitergegeben werden:

> *„Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass Du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können"*
> *(https://www.whatsapp.com/legal/?l=de#terms-of-service).*

Doch nicht nur der Datenabfluss kann kritisch sein, auch die Fremdbeeinflussung, z. B. das Stilllegen von Fahrzeugen bei nicht rechtzeitig bezahlten Raten (während der Fahrt auf der Autobahn: „*Terrified driver almost crashes when loan company hit ‚kill switch' for missing repayments*", Mirror, *http://www.mirror.co.uk/news/technology-science/terrified-driver-crashes-car-loan-4325955*) oder die Fremdbeeinflussung des Weges bei Navigationsgeräten. Auch Sicherheitsbehörden träumen von solchen Möglichkeiten: „*I want to remotely disable Londoner's cars, says Met's top cop*" (The Register, *http://www.theregister.co.uk/2016/09/22/met_police_commissioner_i_want_remotely_kill_car_electronics/*).

Gerade bei Smart Homes wird man sich auch neue Gedanken über das Human Computer Interface (HCI) machen müssen – auch im Hinblick auf Datenschutzfunktionen. Die Komplexität dieser Systeme sollte verringert werden, auch die „historisch gewachsene".

In der Praxis der Entwicklung zeigt sich allerdings häufig, dass für den Fortschritt andere Prioritäten gesetzt werden. Das World Wide Web wurde ohne Berücksichtigung der Sicherheit entwickelt; dieses Vorgehen wird von Tim Berners-Lee verteidigt: Zielsetzung bei der Entwicklung war „ … *a platform that developers would find familiar and easy to use. Baking in security at that point might have worked against that goal …* " (The Register, http://www.theregister.co.uk/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/). Einen anderen Standpunkt hat heute Vint Cerf: „ … *Vint Cerf … regretted not building in security to basic internet protocols.*" Fest steht, dass Sicherheit (und Datenschutz) bei der Entwicklung als nachrangig eingestuft wurden.

Der Ansatz, ein Verständnis der Sicherheit von Systemen durch Reverse Engineering zu erzielen, ist in der Praxis mit Problemen behaftet: er ist nur für wenige Experten realistisch, es gibt dafür rechtliche Einschränkungen und auch dadurch sind die Systeme nicht vollständig verstehbar. Viktor Mayer-Schönberger erwartet: „Wir glauben, dass sich eine eigene Kaste von Experten entwickeln wird, die Algorithmiker" (Zeit Online 2013/09). Diese sollen die Systeme durchschauen. Die Forderung nach Open Source reicht dafür aber nicht!

Die neue gesetzliche Grundlage für den Datenschutz ist die Europäische Datenschutz-Grundverordnung mit den Prinzipien

- Marktortprinzip (Art. 3 – d. h. auch für außereuropäische Player mit Datenverarbeitung in der EU)

- Signifikante Sanktionen (Art. 83, 84)

- Insbesondere:
  1. Adäquater Umgang mit Risiken (Art. 24, 25, 32, 35, 36)
  2. Datenschutz durch Technikgestaltung (Art. 25, Sicherheit: Art. 32)
  3. Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25)
  4. Transparenz für die betroffenen Personen (Art. 5, 12–15, 19, 22, 30, 33)
  5. Intervenierbarkeit für die betroffenen Personen (Art. 5, 7, 8, 16–18, 20, 21)
  6. Verantwortung des für die Verarbeitung Verantwortlichen (Art. 6 II, 24)

- Adressat ist dabei der Datenverarbeiter (Betreiber, Auftragnehmer, u. U. auch Privatpersonen; nicht unmittelbar Hersteller)

Ziel der Verordnung ist der Schutz der Rechte und Freiheiten natürlicher Personen.

Ein wesentlicher Aspekt ist die Transparenz, also die Verständlichkeit der Datenverarbeitung. Die Verordnung schreibt dafür eigentlich den Grundsatz der fairen und transparenten Datenverarbeitung vor. Es sind aber Ausnahmen möglich: Im Ermessen des Verantwortlichen kann die Information der Betroffenen unterbleiben, wenn „die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde" (Art. 14 Abs. 5 lit. b DS-GVO). Dies wirft die Frage nach Anwendungen auf, die Big-Data-Techniken nutzen oder nach Anwendungen des Ubiquitous Computing. Zu fragen ist auch, wie die Informationen über die Datennutzung zum Betroffenen gelangen sollen.

Marit Hansen

Marit Hansen ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz (ULD). Davor war die Diplom-Informatikerin sieben Jahre lang stellvertretende Landesbeauftragte für Datenschutz. Im ULD hat sie den Bereich der Projekte für technischen Datenschutz und das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) aufgebaut. Seit 1995 arbeitet sie zu Themen des Datenschutzes und der Informationssicherheit. Ihr Schwerpunkt liegt auf der grundrechtskonformen Gestaltung von Systemen, insbesondere durch Privacy by Design und Privacy by Default.

Für mehr Transparenz gibt es bereits Vorschläge: Nutzung einer klaren und einfachen Sprache für die Information der Betroffenen, Aufbau der Datenschutz-Policies in mehreren Ebenen (*layered policies*), durch standardisierte Bildsymbole (vgl. Art. 12 Abs. 7 DS-GVO) und in maschinenlesbarer Form. Auch für die Unterstützung der Selbstbestimmung gibt es Vorschläge:

- Datensparsamkeit und Privacy by Design als Grundprinzip [stark unter Beschuss von Politik und Wirtschaft, Gegenbegriffe: Datenreichtum, Datensouveränität]
- Binden der akzeptierten Verarbeitungsregeln an die Daten (z. B. Sticky Policies) [dabei sind aber Seiteneffekte zu beachten]
- Assistenten Technik/Menschen/Organisationen [das erfordert ein Vertrauensmodell!]
- Adäquate HCI

Art. 25 der EU-Datenschutz-Grundverordnung fordert Datenschutz by Design & by Default. Diese Forderung richtet sich primär an Datenverarbeiter (auch im Auftrag) und (nur indirekt) an die Hersteller von IT-Systemen. Ziel dabei ist die Gestaltung von Systemen und Diensten von Anfang an über den gesamten Lebenszyklus: Diese müssen datensparsam und mit möglichst datenschutzfreundlichen Voreinstellungen versehen sein:

> *„(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.*
>
> *(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen" (Art. 25 EU-DSGVO).*

Erwägungsgrund 78 der Verordnung fordert zu Datenschutz by Design & by Default Folgendes:

- Nachweis durch interne Strategien und technische und organisatorische Maßnahmen, u. a.:
  1. Datenminimierung
  2. schnellstmögliche Pseudonymisierung
  3. Transparenz in Bezug auf Funktionen und Verarbeitung
  4. Ermöglichung der Überwachung der Verarbeitung durch den Betroffenen
  5. Ermöglichung für Sicherheitsfunktionen *on top* durch Verantwortlichen
- Hersteller sollten zur Berücksichtigung des Rechts auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen ermutigt werden.
- Die Grundsätze sollten in öffentlichen Ausschreibungen berücksichtigt werden.

Zusätzlich zum Datenschutz sind die Grundsätze des Verbraucherschutzes zu beachten: Anforderung an eine gültige Einwilligung nach Datenschutzrecht ist, dass sie bewusst, informiert und freiwillig gegeben wird. Eine AGB-Vertragsklausel kann eingeschränkt gültig oder unwirksam sein, weil die AGB-Bestimmung unklar ist, die AGB-Bestimmung überraschend ist oder die AGB-Bestimmung den Kunden unangemessen benachteiligt. Frage ist: Wieviel ist dem Betroffenen zuzumuten?

Fazit

Informationelle Selbstbestimmung ist schon immer mehr Ziel als Realität. Bei versteckter Informationstechnik ist eine Selbstbestimmung im Einzelfall praktisch nicht möglich. Feingranulare Abfragen oder Konfigurationen sind zeitintensiv und anspruchsvoll, für die meisten unzumutbar. Die Umsetzung muss auf eine Weise geschehen, die analog zur Einwilligung in die Organspende oder zur Patientenverfügung ist.

Garantien durch eingebauten Datenschutz sind aber möglich: beispielsweise durch Privacy by design & by default. Der Default ist aber häufig nur der Startpunkt, von dem danach wieder abgewichen werden kann. Das Maß des technisch umgesetzten Datenschutzes hängt in der Praxis auch von der Anwendungssituation ab – *One size fits all* ist in vielen Bereichen nicht realistisch.

Die Realität der heutigen Informationstechnik und Informationsgesellschaft ist vom Datenschutz-Optimum – und sogar vom Akzeptablen – weit entfernt. Lösungen müssen sichtbarer werden, für Hersteller, Betreiber, Nutzer und Datenschutzbehörden; auch über die Community-Grenzen hinaus. Die Diskussion von Seiteneffekten und Technikfolgen ist nötig. Und zuletzt: Datenschützer.innen müssen sichtbarer werden.