Technologiebedingte Herausforderungen für den Datenschutz in Europa

Bericht der ENISA
Ad-Hoc-Arbeitsgruppe zu Datenschutz und Technologie

Juli 2008

Autoren:

Mema Roussopoulos, FORTH (Vorsitzende der Arbeitsgruppe)
Laurent Beslay, EDPS
Caspar Bowden, Microsoft
Giusella Finocchiaro, Universität Bologna
Marit Hansen, ULD Kiel
Marc Langheinrich, ETH Zürich
Gwendal Le Grand, CNIL
Katerina Tsakona, FORTH

Herausgeber:

Marc Langheinrich, ETH Zürich
Mema Roussopoulos, FORTH

Inhaltsverzeichnis

1. Einleitung

Die Privatsphäre und der Schutz personenbezogener Daten gehören heute zu den großen Herausforderungen bei der Entwicklung von Informations- und Kommunikationstechnologie (IKT)-Systemen und -Anwendungen. Das wurde in der Verordnung (EG) Nr. 460/2004 vom März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) klar erkannt (8. Erwägungsgrund). Durch die Zunahme von mobilen Kommunikations- und Wireless-Systemen, von Anwendungen, die auf End-to-end-Internetprotokolle angewiesen sind, um zuverlässig zu funktionieren, sowie durch die Verbreitung von RFID (Funkfrequenz-Identifizierungssystemen) entstehen neue Risiken der illegalen Verarbeitung personenbezogener Daten. Potenzielle Sicherheitslücken, die durch technische und menschliche Schwachstellen entstehen (z. B. aggressive unerwünschte Werbe-E-Mails (Spam), Malware, Phishing), werden für organisierte kriminelle Angriffe genutzt. Die erwartete Ausbreitung von Sensornetzen, die Informationen aus dem Alltag des Einzelnen erfassen, wird die sinnvolle und effektive Anwendung der Grundsätze des Datenschutzes an ihre Grenzen stoßen lassen, wenn nicht angemessene Mittel gefunden werden, um ihre Einhaltung zu garantieren.

Die ENISA-Arbeitsgruppe zu Datenschutz und Technologie wurde eingerichtet, um die durch diese technologischen Entwicklungen entstehenden Probleme und ihre Folgen für den aktuellen Rechtsrahmen der EU zu analysieren. Die Hauptaufgabe der Arbeitsgruppe besteht darin, Maßnahmen zur Bewältigung dieser Probleme vorzuschlagen. In diesem Bericht ermitteln wir die wichtigsten **technologiebedingten Diskrepanzen** zwischen der Datenschutzverordnung und den neuen sozio-ökonomischen Realitäten. Wir betrachten die potenziellen Gefahren und Chancen moderner Technologien und schlagen Prioritäten für Maßnahmen vor, mit denen die gravierendsten Lücken geschlossen werden können.

Die Grundsätze des Datenschutzes werden verständlich und technologieneutral formuliert, es geht aber vor allem darum, zu verstehen, wie diese Grundsätze wirksam auf die Innovationen angewendet werden können, die das in Lissabon formulierte Ziel unterstützen sollen, die Union zum „wettbewerbsfähigsten und dynamischsten wissensbasierten Wirtschaftsraum“ zu machen. **Wenn die Bürger weiterhin darauf vertrauen sollen, dass ihre Grundrechte geschützt werden und dass der EU-Rahmen ihren alltäglichen Erfahrungen Rechnung trägt, müssen sie ihr Recht auf Schutz der Privatsphäre praktisch und sinnvoll ausüben können**. Wir haben Sorge, dass diese Prinzipien zu einer reinen rechtlichen Abstraktion werden könnten und nur theoretisch und in Ausnahmefällen Abhilfe ermöglichen. Eine solche prekäre Situation kann allein durch originelle Ideen und entschlossenes Handeln verhindert werden.

Im folgenden Bericht werden die erkannten Probleme zunächst beschrieben, ihre jeweils spezifischen Merkmale aufgelistet und eine Reihe von Empfehlungen formuliert, die uns geeignet erscheinen, diese Lücken zu schließen. Unsere Analyse berücksichtigt – soweit zutreffend - die Rolle der einschlägigen öffentlichen und privaten Stellen auf europäischer und nationaler Ebene.

2. Zusammenfassung der Empfehlungen

Dieser Abschnitt enthält eine Zusammenfassung der festgestellten Sicherheitslücken und empfohlenen Lösungen. Eine ausführlichere Erörterung findet sich in den Beschreibungen der einzelnen Datenschutzlücken im Hauptteil dieses Berichts.

Datenschutz und digitale Integration

Eine kritische Lücke ist das mangelnde Bewusstsein und Verständnis für Datenschutzfragen bei den einzelnen Nutzern und ihre Unfähigkeit, umsichtig zu handeln. Das könnte die Gesellschaft in „Datenschutz-Bemittelte“ und Datenschutz-Unbemittelte“ spalten. Gerade weil die Informationsgesellschaft das Problem der digitalen Integration in Bezug auf die Informations- und Kommunikationstechnologien (IKT) angehen, d. h. überlegen muss, wie man den Nutzern verstärkt Zugang zu den IKT verschaffen kann, müssen die Bemühungen vor allem darauf gerichtet werden, die Nutzer zu befähigen, ihre persönlichen Daten beim Umgang mit den IKT zu schützen und den Schutz ihrer Privatsphäre wirksam durchzusetzen. Besonders wichtig sind hier nicht nur Gruppen, für die die IKT eine besondere Herausforderung darstellen, wie beispielsweise ältere Menschen oder Menschen mit Behinderungen, sondern auch junge Menschen, bei denen die Schwelle zur IKT-Nutzung niedrig ist.

Wir empfehlen, dass die Kommission Programme zur digitalen Integration in die Wege leitet, bei denen die Menschen mit Beispielszenarien angesprochen werden, die ihrer Lebenssituation entsprechen, etwa in der Schule, im Kindergarten, im Unternehmen oder anderswo. Das erfordert nicht nur die Entwicklung neuer Unterstützungswerkzeuge und Identitätsmanagement-Systeme für Nutzer, sondern auch besseres Informationsmaterial (z. B. Merkblätter zum Datenschutz, Unterrichtsprogramme in den Schulen).

Unterstützungswerkzeuge für Nutzer

Die besten Technologien und Gesetze nützen dem Bürger nichts, wenn er nicht in der Lage ist, im eigenen Interesse Gebrauch davon zu machen. Beispielsweise wurden Sicherheitstechnologien wie Verschlüsselungs- oder Anonymisierungstools bisher von Endnutzern trotz ihrer technischen Ausgereiftheit kaum angenommen. Die für die Datenverarbeitung verantwortlichen Stellen, deren Geschäftsmodell auf der gewinnorientierten Verarbeitung personenbezogener Datenflüsse basiert, haben gegenwärtig nicht genügend Anreize, brauchbare Kontrollschnittstellen für die Betroffenen bereitzustellen.

Wir empfehlen, dass Forschungsagenturen und Wirtschaft Ressourcen für die Entwicklung sinnvoller und benutzerfreundlicher Schnittstellen und

assistentengestützter Anleitungen für die richtige Konfiguration der Systeme und Kontrolle personenbezogener Daten bereitstellen. Um Betroffenen dabei zu helfen, eine klarere Vorstellung von den Zusammenhängen der Datenverarbeitung zu bekommen, sollten sich Mitgliedstaaten, Datenschutzbehörden (Data Protection Authorities, DPA) und Verbraucherverbände stärker um Aufklärung bemühen und ihre Bemühungen nach Möglichkeit auf spezielle Gruppen zuschneiden (z. B. junge Menschen, Eltern).

Online-Dateneinsicht

Ein besonderer Aspekt des EU-Rechtsrahmens zum Datenschutz ist die besondere Stärkung des Rechts des Einzelnen, Auskunft darüber zu erhalten, was Organisationen über ihn wissen – das Recht auf Dateneinsicht. Obwohl die Gründe, aus denen dieses Recht ursprünglich begründet worden ist, vielfältiger und dringlicher geworden sind, hat seine Umsetzung nicht mit anderen Aspekten der Entwicklung der Informationsgesellschaft Schritt gehalten, wodurch eine angemessene und wirksame Ausübung dieses Rechts behindert wird. Bei der Verbesserung der Umsetzung geht es besonders darum, eine zufriedenstellende Authentifizierung der betroffenen Person sicherzustellen, die die Dateneinsicht beantragt.

Wir empfehlen, dass ENISA und die Artikel-29-Datenschutzgruppe eine eingehende Analyse von Maßnahmen zur Überarbeitung des Rechtsrahmens im Hinblick darauf vornehmen, dass die Betroffenen online - im Idealfall kostenlos - möglichst umfassend Einsicht in ihre personenbezogenen Daten im Rahmen der bestehenden Rechtsvorschriften erhalten. Unterstützungswerkzeuge für Nutzer und Identitätsmanagement-Systeme können in einem solchen Rechtsrahmen eine wichtige Rolle spielen.

Identitätsmanagement

Um in der Online-Welt eine klare Rechenschaftspflicht herzustellen, verlangen gängige IKT-Systeme im Allgemeinen von den Nutzern, dass sie ihre wirklichen Namen und weitere persönliche Daten angeben und durch digitale Zertifikate belegen. Häufig ist jedoch eine Angabe des Benutzernamens nicht erforderlich. So genannte „private credentials“ (geschützte Berechtigungsnachweise) oder „minimum disclosure certificates (Mindestoffenlegungs-Zertifikate) bieten Möglichkeiten, die Privatsphäre zu schützen und Autorisierungen zu belegen und gleichzeitig die Identifizierbarkeit und Rechenschaftspflicht des Nutzers zu kontrollieren. Die Verfügbarkeit dieser Technologien hat Auswirkungen auf die Auslegung des Datenminimierungsprinzips und die Bedeutung der Verhältnismäßigkeit, die besagt, dass die Verarbeitung personenbezogener Daten auf das notwendige Maß beschränkt werden sollte.

Wir empfehlen, dass Gesetzgeber und politische Entscheidungsträger auf nationaler und europäischer Ebene die Grundlagen der Rechtmäßigkeit der Verarbeitung personenbezogener Daten vor dem Hintergrund dieser

Technologien neu bewerten. Ferner empfehlen wir, dass Akteure des öffentlichen und privaten Sektors dazu beitragen, die für die Ausstellung und Interoperabilität solcher „Berechtigungsnachweise" erforderliche Infrastruktur aufzubauen, und diese in ihren IKT-Systemen verwenden, wo dies zweckmäßig erscheint.

Offenlegung sicherheitsrelevanter Vorfälle

Ein effizienter Schutz personenbezogener Daten ist nur möglich, wenn Informationen über mögliche Risiken bei der Verarbeitung von Daten für die Sicherheit und den Schutz personenbezogener Daten sowie über sicherheitsrelevante Vorfälle in Bezug auf solche Daten, angemessen und zeitnah mitgeteilt werden.

Wir empfehlen, dass die Europäische Kommission umfassende Rechtsvorschriften zur Meldung von Sicherheitsverstößen erlässt. Damit sollen nicht nur Datenschutzbehörden sondern auch der Einzelne in die Lage versetzt werden, diese Vorfälle besser zu erkennen und darauf zu reagieren. Die Bürger sollen besser verstehen, inwieweit sie von Vorfällen im Zusammenhang mit der Sicherheit und dem Schutz ihrer persönlichen Daten betroffen sind und wie sie angemessen darauf reagieren können. Ferner empfehlen wir, dass Normungsgremien sich mit den Formaten und Protokollen befassen, mit denen IKT-Systeme auf der Nutzerseite bei der Interpretation dieser Meldungen unterstützt werden.

Zertifizierung

Die Schaffung rein wirtschaftlicher Anreize für die Einhaltung der Datenschutzbestimmungen war bislang wenig erfolgreich. Daher sollte auf anderen Wegen versucht werden, die Motivation für die Einhaltung des Datenschutzes zu fördern. Beispielsweise sollten die Mitgliedstaaten Tools für Unternehmen entwickeln, mit denen diese eine Zertifizierung oder Selbstzertifizierung in Bezug auf die Einhaltung der Datenschutzvorschriften durchführen können, wenn sie sich an öffentlichen Ausschreibungen beteiligen. Die Mitgliedstaaten sollten Zertifizierungsprogramme fördern und verfolgen, an denen auch Verbraucherverbände beteiligt werden: Sie sollten Steueranreize für Unternehmen schaffen, die sich an die Bestimmungen halten, und erwägen, ob sie Unternehmen, die eine Datenschutz-Zertifizierung durchführen, bestimmte Meldepflichten erlassen (wie in der am 1. Januar 2008 in Kraft getretenen schweizerischen Verordnung über die Datenschutzzertifizierungen (VDSZ)[1]). Es sollten wirksame Sanktionen (und Entschädigungsregelungen) für Verstöße gegen das Datenschutzrecht vorgesehen werden (z. B. Sanktionen auf Tagessatzbasis oder Schadenersatzpflichten).

Wir empfehlen, dass die Europäische Kommission die Entwicklung von Datenschutz-Zertifizierungsprozessen unterstützt und beispielsweise in

[1] Siehe unter http://www.admin.ch/ch/e/rs/235_13/.

Bezug auf Steuern und andere Bereiche Rechtsvorschriften entwickelt, um Anreize für eine solche Zertifizierung zu bieten. Wir empfehlen außerdem, dass Normungsgremien dazu beitragen, Kriterienwerke für die Datenschutz-Zertifizierung zu standardisieren. Überwachungsinstrumente und beste verfügbare Techniken sind dabei wichtige Bestandteile eines umfassenden Zertifizierungsrahmens.

Überwachungsinstrumente

Für Datenschutzbehörden ist es schwierig, Systeme, mit denen personenbezogene Daten verarbeitet werden, zu kontrollieren und zu prüfen. Auch die Industrie verfügt nicht über angemessene Instrumente, um interne Datenschutzprüfungen durchzuführen. Die modernen Technologien und der aktuelle rechtliche Rahmen bieten nicht die Mittel, mit denen eine leichte Überwachung und Kontrolle der Datenverarbeitung durch die für die Verarbeitung verantwortlichen Stellen (Data controllers) möglich ist. Die Kontrollbefugnisse müssten durch standardisierte Überwachungsinstrumente, die Datenschutzbehörden einen automatisierten Zugriff bzw. eventuell einen Fernzugriff ermöglichen, kontinuierlich und sachgerecht durchgesetzt werden. Außerdem sollten diese Instrumente eine unbestreitbare Rückverfolgbarkeit der Systeme möglich machen. Dadurch könnten die Überwachungsinstrumente zur Verbesserung der Kontrollverfahren und Erleichterung der Analyse von Datenschutzverletzungen beitragen; und schließlich können sie helfen, die Verarbeitung von Daten transparent zu machen und die Nutzer besser darüber zu informieren.

Wir empfehlen, dass die Europäische Kommission die Forschung im Bereich Datenschutz-Überwachungsinstrumente im Hinblick auf verlässliche und vertrauenswürdige Prüfverfahren finanziell unterstützt; diese Instrumente sollten dann systematisch von den Datenverarbeitern angewendet werden, um eine kontinuierliche Überwachung des Datenschutzes sicherzustellen; auch die Datenschutzbehörden sollten diese Instrumente verwenden, um ihre Kontrolltätigkeit zu automatisieren.

Beste verfügbare Techniken

Um eine frühzeitige und wirksame Prüfung und Zertifizierung von Systemen für die Erhebung und Verarbeitung von Daten zu ermöglichen, benötigen Industrie und Datenschutzbehörden eine Reihe sektorspezifisch festgelegter „bester verfügbaren Techniken“ (BVT) in Bezug auf Datenschutz und Datensicherheit. Dadurch könnte die Einhaltung der Datenschutzbestimmungen checklistenartig geprüft und ein Basis-Zertifikat erstellt werden, auf das sich weitere Analyse- und Überwachungstools stützen können.

Wir empfehlen, dass die Kommission ein Rechtsinstrument vorschlägt, in dem die geforderten Strukturen und Verfahren für die Ermittlung der BVT festgelegt werden. In diesem Instrument sollte die Einbeziehung aller relevanten Akteure vorgesehen werden, deren Arbeitsergebnisse den

Aufsichtsbehörden und öffentlichen und privaten Organisationen, die diese Systeme umsetzen, als primäre Leitlinien dienen könnten.

Anreize und Sanktionen

Ein allgemeines Defizit besteht darin, dass die für die Verarbeitung der Daten verantwortlichen Stellen nicht wirklich motiviert sind, die Bestimmungen des Datenschutzrechts einzuhalten. Viele Datenschutzbehörden können nur kleinere Verstöße durch die datenverarbeitenden Stellen feststellen, so dass eine unvorschriftsmäßige Verarbeitung von Daten häufig unbemerkt bleibt. Außerdem sind aufgrund der größtenteils geringfügigen Sanktionen kaum wirtschaftliche Anreize für ein datenschutzkonformes Verhalten gegeben.

Wir empfehlen, dass die Europäische Kommission und die Mitgliedstaaten ein System von Anreizen fördern, das mit einem auf den besten verfügbaren Techniken basierenden Zertifizierungsprogramm und wirksamen wirtschaftlichen Sanktionen verbunden ist und mit geeigneten Instrumenten überprüft und beaufsichtigt werden kann.

Welche Daten sind personenbezogen?

Trotz der Anstrengungen, die die Artikel-29-Datenschutzgruppe vor kurzem unternommen hat, um den Begriff „personenbezogene Daten“ zu klären, ist dieser Begriff noch immer umstritten. Selbst in den Fällen, in denen die Industrie davon überzeugt ist, keine personenbezogenen Daten zu verwenden, sollte eine Analyse der Datenschutzrisiken durchgeführt und das entsprechende System so entwickelt werden, damit diese Risiken so gering wie möglich gehalten werden. In einigen Fällen können Daten zu personenbezogenen Daten werden, speziell wenn im Zuge des Fortschritts die technischen Mittel verfügbar werden, die dazu verwendet werden könnten, eine Person zu identifizieren. Daher müssen geeignete Schutzmaßnahmen getroffen werden, um zu verhindern, dass Daten – auch unbeabsichtigt – zu personenbezogenen Daten werden.

Wir empfehlen ENISA, eine Methodik zur Folgenabschätzung für den Datenschutz (Privacy Impact Assessment) zu entwickeln. Der Industrie legen wir nahe, grundsätzlich bei der Festlegung ihrer Strategie zur Sicherung ihrer Daten Folgenabschätzungen für den Datenschutz vorzunehmen. Außerdem empfehlen wir der Industrie angemessene Lösungen zum Schutz individueller Daten zu entwickeln, unabhängig davon, ob diese Daten personenbezogen sind.

Social Sorting

Eine Sortierung von Daten nach sozialen Gesichtpunkten („social sorting“), wie z. B. verhaltensorientiertes Marketing, kann die Privatsphäre von Menschen verletzen, auch wenn die verarbeiteten Daten nicht personenbezogen sind. Die aktuellen gesetzlichen Regelungen sind auf verschiedene Rechtsvorschriften

verteilt und bieten keinen wirksamen Schutz der Privatsphäre in den genannten Bereichen.

Wir empfehlen, dass die Kommission einen umfassenden Rechtsrahmen für jegliche Verarbeitung von Daten über Personen ausarbeitet und verabschiedet, unabhängig davon, ob diese Daten personenbezogen sind oder nicht. Praktisch gesehen könnte das bedeuten, dass ein kompletter Prüfpfad für Datenverarbeitung und Datenquellen sowie mehr Transparenz für die Betroffenen vorgeschrieben wird. Ferner empfehlen wir, dass die für die Datenverarbeitung verantwortlichen Stellen organisatorische und technische Maßnahmen treffen, um sicherzustellen, dass Betroffene ihre Rechte wahrnehmen können.

Privatsphäre, Datenschutz und Raum

Die Informationsgesellschaft stellt uns vor die Aufgabe, personenbezogene Daten der Bürger innerhalb der europäischen Rechtsprechung zu behalten. Durch die Digitalisierung des privaten Bereichs und seiner Grenzen bietet der Begriff des digitalen Territoriums (Digital Territory) die Möglichkeit, die Begriffe Territorium, Eigentum und Raum in digitalen Umgebungen einzuführen. Es sollen Instrumente entwickelt werden, mit denen der Nutzer Nähe und Distanz im digitalen Raum – im legalen und im sozialen Sinne – nach dem Vorbild des Schutzes seiner Privatsphäre in der realen Welt wahren kann.

Wir empfehlen, dass die Artikel-29-Datenschutzgruppe und die Europäische Kommission die Möglichkeit ausloten, den Begriff des Territoriums auf die Informationsgesellschaft anzuwenden und beispielsweise das Recht auf Unverletzlichkeit der Wohnung auf die Online-Welt auszuweiten.

Künftige Arbeit

Einige der festgestellten Defizite beziehen sich auf Gefahren für den Datenschutz durch neue Geschäftsmodelle, die den einzelnen Verbraucher über die Erstellung von Verhaltensprofilen (behavioural profiling) ins Visier nehmen. Die Arbeitsgruppe stellt fest, dass diese Fragen vor kurzem im Kontext von Untersuchungen zum Wettbewerb in den Vereinigten Staaten von Amerika und in der EU aufgeworfen aber nicht beantwortet wurden, und empfiehlt, dass ENISA eingehendere Untersuchungen dieser Fragen unter besonderer Berücksichtigung der Verhaltensökonomie in Auftrag gibt. Die Arbeitsgruppe stellt ferner fest, dass einige Aufsichtsgremien und die Wirtschaft zwar behaupten, geeignete Anreize für eine befriedigende Selbstregulierung seien vorhanden, die vorliegende wissenschaftliche Forschung[2,3] dies aber nur sehr

[2] Siehe unter http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.
[3] Tseng, Jimmy C: An Economic Approach towards Privacy Enforcement, Präsentation auf dem Workshop PRIME/ERIM Privacy for Business, Rotterdam, Dezember 2004. Siehe unter https://www.prime-

unzureichend belegt. Möglicherweise muss darüber nachgedacht werden, ob neue Datenschutzgrundsätze und Marktstrukturen erforderlich sind, um sicherzustellen, dass Wettbewerbskräfte den Schutz der Privatsphäre stärken (statt ihn zu unterminieren). ENISA ist in seiner Rolle als unabhängiger Vermittler der EU-weiten Netz- und Informationsanalyse sehr gut in der Lage, solche Forschung zu fördern und dafür zu sorgen, dass die Schlussfolgerungen daraus in die EU-Politiken einfließen.

Wir empfehlen, dass ENISA weitere Forschungsarbeiten zum Thema Datenschutz und Technologie in Auftrag gibt, um ein fundierteres Verständnis der Problematik zu erlangen. Vorrangig ist dabei eine umfassende Analyse der Marktstruktur von Online-Diensten, die durch Werbung unterstützt werden, und des wirtschaftlichen Einflusses insbesondere von Verhaltensprofilen unter dem besonderen Gesichtspunkt der wirksamen Anwendung der Datenschutzgrundsätze und der Selbstbestimmung der Betroffenen. In dieser Untersuchung sollte eine kritische Evaluierung der potenziellen Wirksamkeit der Selbstregulierung vorgenommen und außerdem untersucht werden, ob Divergenzen bei der Definition des Begriffs der personenbezogenen Daten dazu führen, dass Akteure die unterschiedlichen regulatorischen Bestimmungen in den Mitgliedstaaten ausnutzen.[4,5].

project.eu/events/external/ERIM%20Privacy%20for%20Business%20Workshop/Tseng3.ppt.

[4] Reidenberg, Joel R., Paul M. Schwartz: Data-Protection Law and On-Line Services: Regulatory Responses, Brüssel, 1998, http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/regul_en.pdf.

[5] Bohm, Nicholas, Richard Clayton: Open Letter to the Information Commissioner, Foundation for Information Policy Research, März 2008, http://www.fipr.org/080317icoletter.html.

3. Sylvias Daten: ein Lehrstück

In diesem Kapitel beschreiben wir ein realistisches Nutzer-Szenario, das viele der im vorangehenden Kapitel aufgeführten Defizite und Probleme veranschaulicht, auf die wir im nächsten Kapitel näher eingehen werden.

Sylvia hat in letzter Zeit Datenschutzprobleme. Seit einiger Zeit wird in ihrem bevorzugten Internet-Portal Werbung angezeigt, die beunruhigende Bezüge zu Aspekten ihres Privatlebens hat. Teilweise bezieht sie sich sogar auf ein Krankheitsbild, über das sie im Internet recherchiert hat. Sylvia ist besorgt, denn sie hat darauf geachtet, sich bei ihren Recherchen auf keiner Website einzuloggen und keine persönlichen Daten eingegeben, anhand derer man sie identifizieren könnte. Außerdem findet sie es seltsam, dass sie, wenn sie bestimmte für sie interessante Werbeanzeigen anklickt, weniger günstige Angebote erhält als auf dem Computer einer Freundin. Sie glaubt, dies könnte etwas mit „Cookies" zu tun haben, doch wenn sie versucht, die Funktionsweise verschiedener Arten von Cookies und die Möglichkeiten, sie zu kontrollieren, zu verstehen, findet sie das alles sehr verwirrend. Löscht sie jedoch alle Cookies und deaktiviert ihre Verwendung in ihrem Browser, wird das Surfen auf den meisten ihrer Lieblings-Websites sehr umständlich.

Sie weiß, dass sie nach den Datenschutzgesetzen ihres Landes das Recht hat, zu erfahren, was Organisationen jeder Art über sie wissen, doch wenn sie die Datenschutzerklärungen der Websites anschaut, die sie gern nutzt, ist sie verwirrt, denn dort wird behauptet, dass keine persönlichen Daten erfasst werden, solange sie sich nicht registriert und einloggt. Deshalb weiß sie nicht, wie sie vorgehen soll, um ihren gesetzlichen Anspruch auf Offenlegung dieser Vorgänge geltend zu machen.

Manchmal gibt Sylvia ihre E-Mail-Adresse und Handynummer auf Internetseiten an, die Online-Dienste anbieten, ebenso bei lokalen Geschäften, in denen sie einkauft. Sie stellt fest, dass sie nach dem Besuch anderer Geschäfte manchmal viele E-Mails und SMS mit Werbung für die Art von Produkten erhält, die sie gesucht hat. Sie fragt sich langsam, ob diese Werbung mit den kleinen elektronischen Etiketten zusammenhängen könnte, die sie auf einigen erworbenen Produkten bemerkt hat. Diese Werbung erscheint auch auf dem Web-Browser ihres Handys, wenn sie in der Stadt unterwegs ist, und es ärgert sie, dass sie die Bandbreite, für die sie bezahlt, für das Aufrufen einer Opt-out-Seite verbrauchen muss. Wenn sie sich von diesen Seiten oder Diensten abmeldet, hat sie aber oft den Eindruck, weiterhin ziemlich aufdringliche Werbung von noch mehr Firmen zu bekommen.

Sylvia engagiert sich aktiv für ein umstrittenes politisches Ziel. Ihre Aktivitäten sind zwar legal, doch ihr Freund Michael (der manchmal ihren Computer benutzt) wurde bereits auf dem Weg zu Demonstrationen von der Polizei angehalten und musste bei der Einreise in ein anderes Land viele Fragen

beantworten. Es ist ihr klar, dass es offenbar irgendeine für sie nicht nachvollziehbare Verbindung zwischen ihrem Internetnutzungsverhalten, ihren Wegen durch die Stadt und den von ihr gekauften Produkten gibt. Sie fragt sich, wie lange diese Daten aufbewahrt werden und ob und unter welchen Bedingungen nach dem Recht ihres Landes die Polizei Zugang dazu hat. Manchmal liest sie in den Medien Berichte über solche Gesetze, doch diese sind in Einzelheiten immer widersprüchlich und scheinen fast absichtlich verwirrend zu sein. Auf dem Weg zur nächsten Demonstration wird ihr Auto von der Polizei angehalten, und sie wird zu Farbsprühdosen und Werkzeugen, die sie kürzlich für Reparaturen im Haushalt in einem Baumarkt gekauft (und bar bezahlt) hat befragt. Außerdem will man von ihr wissen, warum sie eine bestimmte politische Website liest. Zu Hause bemerkt sie dann, dass die gekauften Waren mit RFID-Etiketten versehen sind, doch sie hat keine Ahnung, wie die Polizei von der Website wissen konnte.

Sie ruft die Hotline der Datenschutzbehörde in ihrem Land an. Es stellt sich heraus, dass die betreffende Website in einem anderen EU-Staat gehostet wird. Man rät ihr, sich an die Datenschutzbehörde in diesem Land zu wenden. Nach einer Reihe von E-Mails an die ausländische Datenschutzbehörde erhält sie eine Antwort von einer Person, die ihre Sprache und ihr Anliegen versteht. Man rät ihr, sich an die Website zu wenden, doch ihre E-Mails werden ignoriert oder mit wenig hilfreichen automatischen Antworten abgespeist. Schließlich schreibt sie einen Brief an die registrierte Kontaktadresse der Website, die auf der Seite selbst nicht aufgeführt ist, die sie aber schließlich über das öffentliche Register der „für die Datenverarbeitung Verantwortlichen" findet. Sie hat jedoch ein Problem: Da sie dieser Website von Anfang nicht ganz getraut hat, hat sie sich unter einem erfundenen Namen registriert. Nach weiterer Korrespondenz mit der Datenschutzbehörde und der Website wird ihrem Wunsch schließlich entsprochen (sie muss jedoch in dem Brief das Passwort für ihr Konto angeben). Sie hat nicht wirklich eingesehen, warum sie ihren echten Namen und ihre Anschrift angeben musste (da sie ja ihren Login-Namen und ihr Passwort angegeben hat), hat aber nach längerer Diskussion mit der Datenschutzbehörde und der Website irgendwann aufgegeben. Nachdem sie mittels internationaler Postanweisung 15 Euro bezahlt hat (die Website akzeptierte keine Online-Zahlung), erhält sie einen Monat später einen ganzen Stapel Ausdrucke, auf denen zwar ihre Nutzung des E-Mail-Dienstes der Website protokolliert, jedoch nichts über „Cookies" oder ihr Surfverhalten zu anderen Zeiten vermerkt ist, in denen sie nicht auf der Seite eingeloggt war. Genau um diese Informationen ging es ihr aber eigentlich (und vor allem darum, auf welchen Wegen diese Informationen möglicherweise an andere Websites oder die Behörden weitergegeben wurden). Sie wendet sich erneut an die Datenschutzbehörde, die ihr mitteilt, nach ihrer Auslegung des nationalen Datenschutzrechts sei die Website nicht verpflichtet, ihr diese Auskünfte zu erteilen. Sylvia ist inzwischen ziemlich enttäuscht darüber, wie kompliziert es ist, ihre Datenschutzrechte wahrzunehmen und dass sie so wenig nützen, wenn es darum geht, etwas über die Fragen zu erfahren, die für den Schutz ihrer Daten online wirklich wichtig

sind. Sie hat eine lange Liste weiterer Unternehmen, an die sie schreiben könnte: die Geschäfte, in denen sie Waren mit elektronischen Etiketten gekauft hat, die anderen Websites, die sie nutzt, und natürlich ihren Internet-Anbieter (Internet Service Provider – ISP), doch das würde eine ganze Menge Geld kosten, und da die meisten Unternehmen behaupten werden, sie „nicht zu kennen" erwartet sie auch nur dieselben unbefriedigenden Ergebnisse. Sie hat jedoch eine Freundin, die Rechtsanwältin und auf Datenschutz spezialisiert ist und sich ihres Falls annimmt. Nach monatelangen geduldigen Recherchen und einer Flut juristischer Korrespondenz kann sie schließlich die „RFID-Identifier" und Cookies ermitteln, die ihrer Meinung nach dafür verantwortlich sind, dass die Polizei ihr auf dem Weg zur Demonstration diese Fragen gestellt hat. Doch die einzigen Unternehmen, die in der Lage waren, der Polizei Rückschlüsse auf ihre echte Identität zu ermöglichen, weigern sich, ihr weitere Auskünfte zu geben. Eine hilfsbereite Firma weist jedoch auf eine Bestimmung im Datenschutzgesetz hin, die sie zu Auskünften nicht verpflichtet sind, wenn es sich um eine „verdächtige Person" handelt.

Sylvia kommt zu dem Schluss, dass sie die Kontrolle über ihre persönlichen Daten völlig verloren hat und ist sogar besorgt, dass sie nach all ihren Bemühungen, auf juristischem Wege ihre Rechte durchzusetzen, als „Unruhestifterin" betrachtet und auf Listen gesetzt werden könnte, die ihr in Zukunft noch mehr Probleme bereiten und vielleicht Schwierigkeiten im Beruf, mit ihrer Krankenkasse und bei Bonitätsprüfungen machen könnten. Sie beschließt, ihre politischen Aktivitäten einzustellen, jegliche Etiketten von den in ihrem Besitz befindlichen Gegenständen zu entfernen, einen neuen Computer zu kaufen, ihren Internet-Anbieter zu wechseln, alle Online-Konten zu schließen und ein Prepaid-Handy zu benutzen, doch sie ist nicht sicher, in welchem Umfang ihre Tätigkeiten immer noch mit ihrer Person in Verbindung gebracht werden können. Sie erzählt ihren Freunden von ihren surrealen Erfahrungen mit der Datenschutz-Bürokratie, doch die glauben ihr nicht so recht und glauben, dass sie langsam etwas wunderlich wird. Schließlich hat Europa ihres Wissens die strengsten Datenschutzgesetze und die meisten Menschen, die Medien und die Politiker scheinen sich um diese Frage keine ernstlichen Sorgen zu machen.

Sylvia erfährt jedoch von einem neuen Software-Paket, das mit einer Reihe beliebter Websites funktioniert, die in Bezug auf den Datenschutz einen guten Ruf haben. Mit diesem Paket kann sie einen kompletten Datenbestand auf ihren Computer herunterladen, der Auskunft über all ihre Interaktionen mit einer Website gibt. Sie ist überrascht, wie detailliert ihr Surfverhalten protokolliert wird, und stellt außerdem fest, dass ein Teil dieser Daten – über Cookies – zu Werbezwecken an andere Unternehmen weitergegeben wurde. Sie wählt einen Internetanbieter, der an diesem Programm teilnimmt und kann so ermitteln, welche „IP-Adresse" sie zu jedem Zeitpunkt hatte. Mit diesen Informationen kann sie auf andere Websites gehen und automatisch abrufen, welche Daten diese über ihre Besuche auf anderen Websites haben (allerdings nur in einigen EU-Ländern, die diese Informationen als „personenbezogene Daten"

anerkennen). Das Softwarepaket verfügt sogar über eine Analysefunktion, mit der sie vergleichen kann, wie lange verschiedene Websites diese Daten über ihr Online-Verhalten aufbewahren und ob dies der jeweiligen Datenschutzerklärung entspricht (dabei stellt sie jedoch fest, dass die Datenschutzerklärungen der meisten Seiten zu unklar sind, um diese Funktion zu nutzen). Außerdem funktioniert das Software-Paket nur bei einer begrenzten Zahl von Websites und einige der Seiten, die sie besonders nützlich findet, beteiligen sich nicht an diesem Download-Dienst. Überraschenderweise beginnen aber einige der innovativsten Websites in den USA, den Download dieser „Attention-Daten" freigeben. Dennoch hat sie gelernt, das Kleingedruckte sehr genau zu lesen, weil ihr klar ist, dass Dritte, die Zugriff auf diese Daten erhalten, daraus Rückschlüsse auf ihre ganz persönlichen Gedanken ziehen könnten.

Ihre Anwältin hat auch gute Nachrichten. Nach mehr als zwei Jahren hat sie ihr Verfahren vor einem vertraulichen „Datentribunal" gewonnen, und die Polizei hat anerkannt, dass nie Anlass bestand, sie als „verdächtige Person" zu betrachten. Endlich kann sie aufdecken, dass die Unternehmen, mit denen sie zu tun hatte, eine Reihe von Daten zu ihrem „elektronischen Leben" gegenüber der Polizei offengelegt haben. Die schlechte Nachricht ist, dass diese Offenlegung nach den geltenden Verfahren erfolgte (sie galten zum damaligen Zeitpunkt angesichts der vorliegenden Informationen und der Umstände als „angemessen"), so dass sie gegen die Polizei und die verschiedenen Unternehmen nichts in der Hand hat, womit sie eine Entschädigung für alle Unannehmlichkeiten und (vorsichtig ausgedrückt) bürokratischen Hürden einfordern könnte, mit denen sie zu kämpfen hatte. Offenbar sind alle „Offiziellen" der Meinung, dass alles richtig gemacht wurde.

Sylvia fragt sich jetzt, warum noch jemand riskieren würde, sich für soziale Veränderungen politisch zu engagieren, wenn das so beunruhigende Folgen haben kann. Sie weiß, dass die Demokratie ein unvollkommenes System ist und das Recht manchmal willkürlich erscheint, doch sie hat den Eindruck, dass das Leben mit den modernen elektronischen Medien von politischem Engagement abschreckt und einem unheimlichen Überwachungsstaat Tür und Tor öffnet. Alles in allem hat sie genug von der Politik (und dem Leben online), doch sie fragt sich, welche Art von Demokratie ihre Kinder erben werden, wenn sich alle so entscheiden. Sie weiß, ohne die Hilfe ihrer Freundin, der Anwältin für Datenschutz (deren Honorar sie sich nicht hätte leisten können), hätte sich nie herausgefunden, was ihr widerfahren war. Vielleicht hätte das Software-Paket für den Abruf und die Verwaltung ihrer personenbezogenen Daten geholfen, wenn sie es früher gefunden hätte, denn es hätte ihr gezeigt, wie stark sie sich durch ihr Online-Verhalten Datenschutzrisiken aussetzt, doch sie hat gelesen, dass das Unternehmen diese Software aus ihrem Programm genommen hat. Offenbar haben sich zu wenige Menschen genug Sorgen um den Schutz ihrer Daten gemacht, dass mit der Software kein Gewinn zu erzielen war, und die großen Websites, die sie wirklich gern besuchte, waren ganz und gar nicht an einer Beteiligung interessiert.

Links

Sehr viel ausführlichere Szenarien finden Sie (in englischer Sprache) bei den SWAMI „Dark Scenarios“ unter http://is.jrc.es/pages/TFS/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf.

4. Datenschutzlücken und Herausforderungen

Im Folgenden sind die zwölf wichtigsten Datenschutzlücken aufgeführt, die die Arbeitsgruppe zwischen der Datenschutzrichtlinie und der Wirklichkeit der Entwicklungen im sozioökonomischen Umfeld festgestellt hat. In den einzelnen Abschnitten wird zunächst die ermittelte Lücke beschrieben; dann folgt eine Liste der Herausforderungen für die technische Forschung und Entwicklung (FuE), den Gesetzgeber und im Kommunikationsbereich.

4.1 Datenschutz und digitale Integration

Ein entscheidendes Defizit ist das mangelnde Bewusstsein und Verständnis für Datenschutzfragen bei den einzelnen Nutzern und ihre Unfähigkeit, umsichtig zu handeln.

Konkrete Sicherheitslücken

Die Bürger sind sich der Datenschutzlücken nicht bewusst bzw. nicht in der Lage, in der gegenwärtigen IKT-Landschaft ihre personenbezogenen Daten zu schützen.

Viele Menschen sind sich der erheblichen Datenschutzprobleme überhaupt nicht bewusst, die aus der Verwendung der neuen Datenerfassungstechnologien, sozialen Netzwerke, allgegenwärtigen Technologien usw. entstehen. Anderen sind bestimmte Formen der Datenverarbeitung nicht geheuer, doch das gesamte Ausmaß der Folgen ihres Handels für den Schutz ihrer personenbezogenen Daten ist ihnen nicht klar. Wieder andere sind sich der Datenschutzprobleme bewusst, wissen aber nicht, was sie tun können, um ihre Privatsphäre zu schützen. Diejenigen, denen der Schutz ihrer Daten wichtig ist, weigern sich oft, an der digitalen Welt teilzunehmen, und können somit nicht vom Nutzen der Informationsgesellschaft profitieren. Wer die Vorteile nutzen will, gibt häufig unter dem Eindruck, keine andere Wahl zu haben, die Bemühungen um den Schutz der Privatsphäre auf.

Rechtsbehelfe sind zeitaufwändig und manchmal unwirksam

Für Nutzer, die wissen, wie sie ihre Privatsphäre schützen können, sind die notwendigen Schritte unter Umständen zu kostspielig oder umständlich. Das gilt auch für Situationen, in denen ihre Datenschutzrechte verletzt wurden. Rechtsbehelfsmaßnahmen sind meist zeitaufwändig, und in manchen Fällen können die Auswirkungen von Datenschutzverletzungen ohnehin nicht rückgängig gemacht werden.

Bewusstsein, Verständnis und die Fähigkeit zum wirksamen Handeln können Faktoren sein, die die Gesellschaft in „Datenschutz-Bemittelte und Datenschutz-Unbemittelte“ spalten.

Die Informationsgesellschaft muss das Problem der „digitalen Integration“ in Bezug auf die IKT bewältigen und die IKT benutzerfreundlicher gestalten. Dass datenschutzrelevante Auswirkungen häufig auf das Verhalten der Nutzer zurückzuführen ist, macht die Aufgabe der digitalen Integration noch dringlicher, wenn es darum geht, die personenbezogenen Daten z. B. von Älteren oder von Menschen mit Behinderungen zu schützen. Die Benutzerfreundlichkeit ist ein wichtiges und noch nicht hinreichend gelöstes Problem bei der Entwicklung von Datenschutzinstrumenten.

Datenschutz-Instrumente sind nicht benutzerfreundlich genug

Besonders groß ist der Bedarf an digitaler Integration auf dem Gebiet des Datenschutzes bei jungen Menschen, d. h, Kindern und Jugendlichen: Bei jungen Menschen ist die Schwelle zur IKT-Nutzung niedrig. Oft lassen sie sich aber besonders leicht von Anbietern, die Spiele oder spielerische Anwendungen anbieten, dazu verleiten, Angaben über ihre Person und möglicherweise auch über Verwandte und Freunde zu machen.

Junge Menschen müssen einbezogen werden

Lösungsvorschläge

Bei der Sensibilisierung der allgemeinen Öffentlichkeit für Datenschutzfragen sind unterschiedliche Ansätze für verschiedene Zielgruppen erforderlich. Kinder müssen z. B. anderes angesprochen werden als ältere Menschen. Humorlose Schulbücher mit erhobenem Zeigefinger sind wenig geeignet, ein verantwortliches Datenschutzverhalten zu vermitteln. Stattdessen müssen die Zielgruppen über Beispiele erreicht werden, die für ihre Lebenssituation relevant sind, sei es in der Schule, im Kindergarten, in einem Unternehmen oder anderen Situationen.

Aufgaben für Forschung und Entwicklung

Bei der Entwicklung von IKT-Systemen jeder Art, die mit der Verarbeitung personenbezogener Daten verbunden sein könnte, sollten ethische Anforderungen und Datenschutzvorkehrungen von Anfang an berücksichtigt werden. IKT-Systeme sollten die Nutzer in die Lage versetzen, ihre Privatsphäre zu schützen und ihre Datenschutzrechte wahrzunehmen, anstatt größere Bevölkerungsgruppen auszuschließen. Die Integration älterer Menschen wird bereits im Rahmen des Projekts SENIOR[6] in Angriff genommen; das Projekt soll eine systematische dialoggestützte Bewertung der sozialen, ethischen und datenschutzbezogenen Probleme vornehmen, die im Kontext IKT und Altern von Belang sind.

Ethische Anforderungen und Datenschutzvorkehrungen in die IKT-Entwicklung einbinden

Die Entwicklung nutzerfreundlicher Unterstützungswerkzeuge wie z. B. „Datenschutz-Assistenten“ – möglicherweise als kostenloses Angebot der Einzelstaaten für ihre Bürger – könnte vorteilhaft sein, um den Nutzern Datenschutzbewusstsein zu vermitteln. So könnte beispielsweise ein „Datenschutz-Assistent“ in Form eines Browser-Plugins die Nutzer vor den Auswirkungen der Eingabe privater Daten auf einer Website warnen (z. B.

Den Nutzern Unterstützungswerkzeuge an die Hand geben

[6] http://seniorproject.eu/.

Geburtsname der Mutter, Kenn-Nr. usw.). Solche Tools könnten auch eingesetzt werden, um angemessene Datenschutz-Standardeinstellungen bei der Konfigurierung von Internetzugangs-Software und Identitäts-Management-Systemen vorzunehmen. Durch die direkte Einbindung solcher automatisierter „Assistenten“ in Standard-IKT-Systeme könnten Nutzer viel über die Auswirkungen ihres Verhaltens auf ihren individuellen Datenschutz lernen.

Aufgaben für den Gesetzgeber

Sowohl die Europäische Datenschutzrichtlinie (Richtlinie 95/46/EG) als auch die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) legen fest, dass die betroffenen Personen das Recht haben, bestimmte Auskünfte zu erhalten. Diese dürfen nicht juristisch verklausuliert, sondern müssen für alle Betroffenen verständlich formuliert sein. Für Online-Dienste hat die Artikel-29-Datenschutzgruppe Stellungnahmen zur Erfüllung dieser rechtmäßigen Anfragen abgegeben, z. B. in den Dokumenten WP 43 und WP 100. Darüber hinaus sind in WP 147 Anforderungen an die Bereitstellung von Informationen für Kinder über sie betreffende Datenschutzfragen beschrieben.

Rechtsvorschriften und Durchsetzungsmaß-nahmen müssen harmonisiert werden.

Diese Empfehlungen werden bisher leider nur selten umgesetzt, und manchmal fehlen selbst grundlegende Informationen. Deshalb müssen die Vorschriften für die Auskunftserteilung gegenüber betroffenen Personen noch verbindlicher und am besten EU-weit harmonisiert festgelegt werden. In der Diskussion sollten außerdem beispielhafte Verfahren für die Benachrichtigung der betroffenen Personen und die Bereitstellung weiterer Informationen hervorgehoben werden. Der Prozess der Information und Sensibilisierung der betroffenen Personen sollte außerdem in Datenschutz-Zertifizierungsprogrammen bewertet werden.

Aufgaben im Kommunikationsbereich

Die Öffentlichkeit muss informiert und geschult werden.

In den Medien sollten regelmäßig Dokumentationen mit visuellen Darstellungen spezifischer Gefahren ausgestrahlt werden. Broschüren sowie audiovisuelle Medien (z. B. in der Art des Materials von „YOU decide“) könnten so auf die potenziellen Gefahren einer allgegenwärtigen Überwachung hinweisen und die Bürger für diese Problematik sensibilisieren. Es sollten Simulationen verfügbar sein, die zeigen, welche Folgen die Preisgabe persönlicher Daten in verschiedenen Zusammenhängen haben kann. Dadurch können die Bürger ein Gefühl dafür entwickeln, welche Risiken langfristig für viele ihrer persönlichen Daten, vor allem für besonders sensible und persönlichkeitsbezogene Daten bestehen. In Schulen kann das Datenschutzbewusstsein der Schüler mit Rollenspielen gefördert werden, in denen beispielsweise der Einfluss deutlich wird, den Daten, die in soziale Netze gestellt wurden, noch Jahre später auf Bewerbungsgespräche haben können.[7]

[7] Solche Aktionen fanden in verschiedenen Schulen am 2. Europäischen Datenschutztag am 28. Januar 2008 statt. Siehe auch online unter:

Wichtig ist auch die tägliche Erziehungsarbeit in der Familie. In der nicht-digitalen Welt existieren bereits verschiedene Ratgeber für den Schutz der Privatsphäre mit Vorschlägen, wie Eltern ihren Kindern z. B. vermitteln können, nein zu sagen, wenn ihre körperliche Privatsphäre verletzt wird, oder dass sie nicht mit Fremden mitgehen dürfen. Die Eltern sollten jedoch auch in die Lage versetzt werden, Kindern beizubringen, wie sie sich in der digitalen Welt schützen können. Es ist aber auch umgekehrt denkbar, dass Kinder ihren Eltern oder Großeltern die Auswirkungen der IKT auf die Privatsphäre erklären und ihnen den Umgang mit Datenschutzinstrumenten beibringen.

Lehrkräfte, Familien, Medien und staatliche Stellen sollten sich im – wahrscheinlich lebenslangen – Bildungs- und Lernprozess aller Bürger engagieren, in dem es darum geht, datenschutzrelevante Informationen (z. B. Datenschutzrichtlinien oder -qualitätssiegel) zu verstehen und richtig mit Datenschutzrisiken umzugehen.

Links

Artikel-29-Datenschutzgruppe: Empfehlung zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union, 5020/01/EN/Final, WP 43, angenommen am 17. Mai 2001, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43de.pdf.

Artikel-29-Datenschutzgruppe: Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, angenommen am 25. November 2004, 11987/04/DE, WP 100, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_de.pdf.

Artikel-29-Datenschutzgruppe: Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen), 00483/08/DE, WP 147, angenommen am 18. Februar 2008, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_de.pdf.

Norwegische Datenaufsicht in Zusammenarbeit mit der norwegischen Direktion für allgemeine und berufliche Bildung und dem norwegischen Technologierat: YOU decide … Thoughts and facts about protecting your personal data *(DU entscheidest … Gedanken und Fakten zum Schutz der persönlichen Daten)*, Januar 2007, http://www.dubestemmer.no/pdf/english-brochure.pdf.

SENIOR – Social Ethical and Privacy Needs in ICT for Older People *(Soziale, ethische und Datenschutzanforderungen in der IKT für ältere Menschen)*, Projekt des 7. Rahmenprogramms, 2008-2009, http://seniorproject.eu/.

---

http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Data_Protection_Day_default.asp.

4.2 Bessere Unterstützungswerkzeuge für Nutzer

Im Idealfall sollten die Bürger „allgegenwärtigen Datenschutz“ genießen, d. h. eine standardmäßige Datenschutzvorrichtung, die ohne Konfigurations- und Verwaltungsaufwand die freie Weitergabe persönlicher Daten erlaubt, aber gleichzeitig durch entsprechende Standardeinstellungen dafür sorgt, dass die Betroffenen den gewünschten Schutz erhalten. Datenschutz und Datensicherheit werden dem Einzelnen wahrscheinlich immer einige Anstrengungen abverlangen. Das liegt daran, dass Datenschutz und Datensicherheit komplexe Konstrukte sind, die stark von der individuellen Situation und dem spezifischen Kontext abhängen, in dem Daten ausgetauscht oder offengelegt werden. Unterstützungswerkzeuge helfen den Nutzern, ihre Privatsphäre zu schützen, indem sie ihnen Mittel zur Überprüfung, Steuerung und Kommunikation an die Hand geben.

Unterstützungswerkzeuge helfen den Nutzern, ihre Daten und Einstellungen zu überprüfen, zu steuern und zu kommunizieren.

Konkrete Sicherheitslücken

Die heutige digitale Welt bietet keine umfassende „Datenschutzsuite“ für Endbenutzer, die ihnen hilft, alle Aspekte des Schutzes ihrer Daten zu verwalten, sondern eine Vielzahl uneinheitlicher Instrumente, die meist nur sehr spezifische Probleme lösen.

Die derzeit verfügbaren Instrumente sind uneinheitlich

Außerdem verlangt die heutige Datenschutztechnologie dem Nutzer viel ab: er muss Identitäten verwalten, Geräte für Standortabfragen verbergen und den Internetverkehr anonymisieren – nicht nur, wenn er vor dem Computer sitzt, sondern den ganzen Tag lang in verschiedensten Situationen von öffentlichen Auftritten und Geschäftsterminen bis zu privaten Treffen.

Die Verbraucher müssen erhebliche Anstrengungen unternehmen, um die Datenschutztechnologie zu nutzen

Das einfache Modell, Hinweise und Wahlmöglichkeiten anzuzeigen, könnte dazu führen, dass die meisten Nutzer sich einfach nicht die Mühe machen und den Datenschutz als elitäres Konzept einigen wenigen Datenschutz-Fundamentalisten überlassen. Selbst diejenigen, die bereit sind, in den Schutz ihrer Daten zu investieren, können entweder durch Tricks dazu gebracht werden, mehr Daten offenzulegen als geplant oder einfach vor der Komplexität der Datenverarbeitung kapitulieren.

Wenn man sie sich selbst überlässt, machen sich viele Menschen möglicherweise nicht die Mühe, ihre Privatsphäre zu schützen

Lösungsvorschläge

Helfen könnten hier besser integrierte und einfacher zu bedienende technologische Werkzeuge, die Interessierten angeboten werden oder in besonderen Situation verfügbar sind, z. B. wenn man Einzelheiten zu einer speziellen Datenerhebung erfahren möchte. Eine Möglichkeit wäre auch eine verbesserte Bildungsstrategie, um den Bürgern zu vermitteln, wie sie ihre Daten wirkungsvoll kontrollieren und verwalten können.

Aufgaben für Forschung und Entwicklung

Unterstützungswerkzeuge sollten leichter zu bedienen sein.

Die Benutzerfreundlichkeit ist bei solchen Hilfsmitteln besonders wichtig, da die Betroffenen sie nicht zur Dateneinsicht nutzen werden, wenn sie kompliziert und/oder teuer (bzw. zeitaufwändig) sind. Solche Instrumente könnten „Datenverfolgungsmechanismen“ einsetzen, um den Nutzern die Überprüfung ihrer eigenen Datenströme zu ermöglichen (wann, wo und zu welchem Zweck werden ihre persönlichen Daten weitergegeben?). Die Systementwickler sollten darin geschult und ausgebildet werden, Instrumente nach Leitlinien für die nutzerfreundliche Konzipierung und Umsetzung sicherer und datenschutzgerechter IKT-Systeme zu gestalten. Um eine korrekte Umsetzung rechtlicher Bestimmungen und Formulierungen in Nutzerschnittstellen sicherzustellen, müssen auch Datenschutzbehörden in diese Arbeit einbezogen werden.

Rechtliche Informationen in technische Protokolle einbinden.

In technische Standards wie z. B. RFID-Kommunikationsprotokolle könnten auch zusätzliche Verweise auf geltende Rechtsvorschriften, die Identität des Datenerhebers oder geplante Nutzungs- und Aufbewahrungsdauer aufgenommen werden.

Aufgaben für den Gesetzgeber

Standardisierte Piktogramme erleichtern das Verständnis rechtlicher Vorgaben

Um Datenschutzrichtlinien zugänglicher und verständlicher zu gestalten, wurden verschiedene Piktogramme vorgeschlagen, um Datenschutzkonzepte auszudrücken, ohne die Nutzer mit möglicherweise verwirrender Rechtssprache zu belasten. Eine Standardisierung dieser Symbole könnte zur Vereinfachung von Hinweisen und Wahlmöglichkeiten beitragen. Die vorliegenden Vorschläge sind jedoch noch nicht auf das europäische Datenschutzrecht ausgerichtet.

Aufgaben im Kommunikationsbereich

Aktive Unterstützung der Nutzer-Erziehung durch Staaten und Datenschutzbehörden

Die Entwicklung von Unterstützungswerkzeugen für Nutzer sollte von den Staaten unterstützt werden. Besonders im Bereich des e-Government (elektronische Behördendienste) und der e-Participation (Bürgerbeteiligung via Internet), wo die Staaten ihre Bürger direkt an der Verarbeitung ihrer Daten beteiligen, sollten sie ihnen beispielhafte Unterstützungswerkzeuge für Sicherheit und Datenschutz bereitstellen und ihren Bürgern beibringen, wie sie zu nutzen sind. Die Datenschutzbehörden sollten entsprechend ausgestattet und beauftragt werden, die Nutzer durch Information und Schulung zu unterstützen, datenschutzgeeignete Konfigurationsdateien oder, wenn möglich, Assistenten zum Download bereitstellen, Anweisungen zum Datenschutz in typischen Konfigurationen geben und einen allgemeinen Helpdesk anbieten. Avatare könnten eine interessante Möglichkeit bieten, Nutzern in leicht zugänglichen bildlichen Darstellungen die Online-Verwaltung von Personen und Teilidentitäten nahezubringen. Diese Aufgaben sind eng verknüpft mit den Lücken und Herausforderungen in den Bereichen Datenschutz und digitale Integration, Anträge auf Online-Dateneinsicht der Betroffenen und Informationen über sicherheitsrelevante Vorfälle.

Links

Beispiele für Icon-Sammlungen zum Datenschutz wurden z. B. von Rundle[8] und Mehldau[9] vorgeschlagen.

Im Rahmen des Projekts PRIME wurden Anforderungen an das Design von Nutzerschnittstellen für Datenschutztools untersucht.[10]

4.3 Das Recht auf Dateneinsicht: Maßnahmen zur wirksamen Umsetzung

Jede betroffene Person hat das Recht auf Dateneinsicht und -berichtigung

Artikel 12 der EU-Datenschutzrichtlinie 95/46/EG garantiert jeder betroffenen Person das Recht auf Dateneinsicht, also das Recht, vom für die Verarbeitung Verantwortlichen die Bestätigung zu erhalten, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Art der Daten und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden. Außerdem hat gemäß Artikel 12 jede betroffene Person das Recht auf Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind.

Die Gründe, aus denen dieses Recht ursprünglich begründet worden ist, sind vielfältiger und dringlicher geworden. Dieses Recht ist nicht nur ein „Sicherheitsnetz“, um in speziellen Fällen Entschädigungsverfahren zu erleichtern, es sollte auch als „Basismechanismus“ für gesellschaftspolitische Transparenz fungieren, um politische Entscheidungsträger zu warnen, wenn der Datenschutz in einem Sektor systemimmanent bedroht ist. Die Eurobarometer-Umfragen in den letzten fünf Jahren haben bestätigt, dass das Recht auf Dateneinsicht kaum bekannt und wenig genutzt wird – aus verständlichen Gründen, denn es ist für betroffene Personen frustrierend, zeitaufwändig und umständlich, bei Bedarf und in brauchbarer Form alle Auskünfte zu erhalten, auf die sie Anspruch haben.

Konkrete Sicherheitslücken

Die Online-Dateneinsicht erleichtert die Ausübung der Datenschutzrechte.

Die Dateneinsicht ist zum „Aschenputtel“ unter den Menschenrechten geworden. Wenn es um die Informationsgesellschaft geht, ist viel von der Leistungsfähigkeit der Unternehmen, der Innovation und der Bequemlichkeit für die Bürger die Rede. Wenn die Bürger jedoch verfolgen wollen, welche Daten von ihnen gespeichert werden, und verstehen möchten, wie daraus Rückschlüsse

[8] http://identityproject.lse.ac.uk/mary.pdf.
[9] http://asset.netzpolitik.org/wp-upload/data-privacy-icons-v01.pdf.
[10] https://www.prime-project.eu/prime_products/reports/.

gezogen werden, die sich auf ihre Behandlung auswirken, müssen sie einen formalrechtlichen Hindernislauf bewältigen, der aus der Feder von Dickens oder Kafka stammen könnte. Hier klafft eine große Lücke. Es fehlen einfachere Möglichkeiten für Bürger zur Ausübung ihrer Datenschutzrechte, besonders über die Online-Dateneinsicht, mit denen sich diese Schwelle deutlich senken ließe. Doch selbst bei Online-Diensten erhalten die Nutzer meist keine Einsicht in all ihre persönlichen Daten, einschließlich derjenigen, die in Log-Dateien gespeichert oder durch Erstellen von Profilen, Scoring oder Data-Mining-Systeme verarbeitet werden.

Bei der Verbesserung der Umsetzung geht es besonders darum, eine zufriedenstellende Authentifizierung der betroffenen Person sicherzustellen, die die Dateneinsicht beantragt. Hat der Authentifizierungsprozess Mängel, öffnet er die größte Datenschutzlücke überhaupt – „automatisch generierte“ Anfragen. Das ideale Werkzeug für die Authentifizierung zur Dateneinsicht ist jedoch verfügbar und bequem zu nutzen: „nutzerzentrierte“ Identitätsmanagement-Systeme, die dem Nutzer erlauben, Online-Beziehungen mit verschiedenen unverbundenen datenverarbeitenden Stellen zu verwalten, mit sicheren gegenseitigen Authentifizierungsmechanismen für alle Seiten.

Außerdem fehlt es an Verfahren zur Einsicht in pseudonyme Daten, die in der Online-Welt besonders relevant ist, in der eine Person viele Kennungen haben kann.

Die Online-Dateneinsicht sollte in datensparsamer Form möglich sein

Lösungsvorschläge

Die Bürger sollten bei der Ausübung ihrer Datenschutzrechte, insbesondere in der Online-Welt, wirksamer unterstützt werden. Datenverarbeitende Stellen sollten Dateneinsicht gewähren, wo immer dies möglich ist.

Aufgaben für Forschung und Entwicklung

Damit die Nutzer ihre Datenschutzrechte unkompliziert wahrnehmen können, sind verständliche Nutzerschnittstellen notwendig. Datenverarbeitende Stellen sollten die Dateneinsicht nicht auf die Masterdaten ihrer Kunden beschränken. Der Online-Lesezugriff ist normalerweise nicht problematisch, sofern der Nutzer ordnungsgemäß authentifiziert wurde und die angefragten personenbezogenen Daten getrennt von anderen geschützten Informationen angezeigt werden können, doch die Berichtigung oder Löschung ist oft weniger leicht umzusetzen, vor allem, wenn dies im Widerspruch zu anderen Zielen steht. So sollten Nutzer beispielsweise nicht in der Lage sein, Prüfpfade oder digitale Beweismittel zu ändern. Vor allem die folgenden Möglichkeiten sollten erforscht werden:

Datenverarbeitende Stellen sollten nutzerfreundliches Design für die Dateneinsicht bieten

- Strukturierung der Systeme der datenverarbeitenden Stellen zur Minimierung der Auswirkungen von Ausnahmen (z. B. Daten, die sich ausschließlich auf die betroffene Person beziehen und keine anderen Ausnahmen aktivieren)

- strategische Optionen zur schrittweisen Verpflichtung datenverarbeitender Stellen, die Online-Identitäts-Beziehungen mit Nutzern unterhalten, Anträgen auf Online-Dateneinsicht sicher und im größtmöglichen praktikablen Umfang zu entsprechen.

Werkzeuge für Nutzer, die die Ausübung von Datenschutzrechten erleichtern

Außerdem könnten den Nutzern Werkzeuge an die Hand gegeben werden, die ihnen helfen, Anträge an die datenverarbeitenden Stellen zu stellen oder – bei Bedarf – bei der Aufsichtsbehörde Beschwerde einzulegen. Solche Werkzeuge können von den Funktionalitäten eines nutzergesteuerten Identitätsmanagements und maschinenlesbarer Datenschutzrichtlinien profitieren. Wichtig sind folgende Faktoren:

- Beseitigung von Barrieren für die Inanspruchnahme des Rechts auf Dateneinsicht, die der Situation des Online-Zugangs nicht angemessen sind.
- „Meta-Datenschutz"-Maßnahmen, die notwendig sind, um den Nutzer vor Einmischung oder Überwachung oder Diskriminierung im Zusammenhang mit der Wahrnehmung des Rechts auf Dateneinsicht zu schützen, und
- Verfahren zur Wahrnehmung des Rechts auf Dateneinsicht gegenüber „indirekten" datenverarbeitenden Stellen (z. B. Stellen, die Daten speichern, die nur mittels einer pseudonymen Kennung zu Einzelpersonen zurückverfolgt werden können).

Datensparende Verfahren zur Einsicht in eigene Daten

Das Recht auf Einsicht in personenbezogene Daten erfordert einen irgendwie gearteten Identitätsnachweis, damit die Daten nicht an unberechtigte Personen weitergegeben werden. Wenn ein Nutzer unter einem Pseudonym Daten eingegeben hat, muss der Nachweis erbracht werden, dass der Antrag tatsächlich von der Person kommt, die hinter diesem Pseudonym steht. Das erfordert angemessene – datensparende – Authentifizierungsmechanismen, u. a.

- sichere gegenseitige Authentifizierung des Nutzers und der datenverarbeitenden Stelle durch nutzerzentrierte Identitätsmanagement-Technologien, die für die Stellung und Erfüllung von Anträgen auf Online-Dateneinsicht angemessen sind, und
- ein höheres Authentifizierungsniveau, damit der Nutzer die Aktivierung der Online-Dateneinsicht bei einer bestimmten datenverarbeitenden Stelle eindeutig genehmigen kann.

Aufgaben für den Gesetzgeber

Online-Dateneinsicht gesetzlich vorschreiben

Für Anbieter, die personenbezogene Daten im Internet oder anderen Online-Szenarien verarbeiten, sollte die Gewährung von Online-Dateneinsicht und anderen Formen der Wahrnehmung von Datenschutzrechten so weit wie möglich gesetzlich vorgeschrieben sein.

Angemessene Pseudonyme für datensparsamen Zugang fordern

Darüber hinaus muss diskutiert werden, ob Pseudonyme, die keinen Nachweis der Nutzeridentität in datensparsamer Form liefern (zumindest ohne die Notwendigkeit, die bürgerliche Identität offenzulegen), in der Datenverarbeitung zugelassen werden sollten, da in einem solchen Fall die Nutzer ihre Datenschutzrechte nicht wahrnehmen können. Dazu könnte auch Folgendes erforderlich sein:

- Optionen für zusätzliche rechtliche Schutzmechanismen gegen erzwungene Dateneinsicht der betroffenen Person und
- ein behördlicher Rahmen zur Bewertung der Angemessenheit von Sicherheitsmaßnahmen zum Schutz von Online-Zugangsmechanismen und Verfahren.

Aufgaben im Kommunikationsbereich

Information der Bürger über ihre Datenschutzrechte

Die Nutzer sollten ebenso wie die datenverarbeitenden Stellen auf die Datenschutzrechte der Nutzer und die Möglichkeit, sie wahrzunehmen, aufmerksam gemacht werden.

Links

Im Rahmen des Projekts PRIME – Privacy and Identity Management for Europe *(Datenschutz und Identitätsmanagement für Europa)*[11] im 6. Rahmenprogramm wurden Möglichkeiten der Integration der Online-Dateneinsicht in ein nutzergesteuertes Identitätsmanagement-System vorgeschlagen.

In manchen Ländern erhalten die Nutzer Online-Einsicht in ihre personenbezogenen Daten in der nationalen Registerdatei, einschließlich der Logdatei mit den Zugriffen auf ihre Daten, z. B. in Belgien („mijndossier/mondossier“) und Norwegen („minside“).

Eurobaromenter-Umfragen zum Datenschutz:

- Data Protection, Opinion Poll *(Umfrage Datenschutz)*, Spezial Eurobarometer Nr. 196, Umfragewelle 60.0 – Europäische Meinungsumfragegruppe EWIV, Umfrage in Auftrag gegeben von der Generaldirektion Binnenmarkt, Referat E4 – Medien und Datenschutz, Dezember 2003, http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_data_protection.pdf.

- Data Protection in the European Union – Citizens' perceptions, *(Datenschutz in der Europäischen Union: die Sicht der Bürger)*, Analysebericht, Flash Eurobarometer No. 225, Umfrage der Gallup Organization Ungarn im Auftrag der Generaldirektion Justiz, Freiheit und Sicherheit, Februar 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[11] https://www.prime-project.eu/

4.4 Identitätsmanagement zur Kontexttrennung

Die Zweckbindung ist in Europa ein wichtiger Rechtsgrundsatz

Es ist allgemein bekannt, dass die Ansammlung personenbezogener Daten zu gravierenden Datenschutzproblemen führen kann. Die in der Europäischen Datenschutzrichtlinie festgelegte Zweckbindung zielt darauf ab, die Erhebung und Verwendung von Daten auf vorab festgelegte Zwecke zu beschränken: „Die Mitgliedstaaten sehen vor, dass personenbezogene Daten …(b) für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. …c) den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen …“ (Artikel 6 Absatz 1 der Europäischen Datenschutzrichtlinie).

Kontextübergreifende Ansammlung personenbezogener Daten gefährdet die Privatsphäre der Bürger

In Europa gibt es jedoch eine Tendenz zur Aufweichung dieses Grundsatzes, so dass verfügbare personenbezogene Daten oft auch für andere Zwecke genutzt werden können, selbst wenn dies in den Rechtsetzungsprozessen ausgeschlossen wurde. Z. B. wird darüber diskutiert, Mautdaten für die Strafverfolgung oder Daten aus der Vorratsspeicherung im Telekommunikationswesen für Marketing-Zwecke zu nutzen. Dieser Trend wird durch mehr und mehr eindeutige Kennungen verstärkt, die als so genannte „Personenkennzeichen“ fungieren können. Diese Kennungen können normalerweise in verschiedenen Anwendungskontexten (z. B. verschiedenen Behörden oder Aktivitäten bei der Internetnutzung) erscheinen und die dahinter stehend Person eindeutig identifizieren. Dadurch, dass personenbezogene Daten in verschiedenen Zusammenhängen erscheinen, werden eine kontextübergreifende Verlinkung und damit auch zunehmend detaillierte Profile möglich. Das wird auch von Datenschutzexperten außerhalb Europas anerkannt, z. B. Nissenbaum, für den es beim Datenschutz um „kontextuelle Integrität“ geht.

Konkrete Sicherheitslücken

Das Problem: wachsende Verfügbarkeit verknüpfbarer personenbezogener Daten

Die zunehmende digitale Verfügbarkeit personenbezogener Daten, die zudem immer besser verknüpft werden können, ist ein großes Problem. Selbst wenn die Daten ursprünglich anonym sind, können sie mit einem Profil verknüpft werden, das genug Informationen zur Identifizierung des Nutzers enthalten kann. Die wachsende Verknüpfbarkeit wird vor allem durch die wiederholte Verwendung eindeutiger Kennungen verursacht, die oft durch IKT-Systeme eingeführt werden, z. B. IP-Adressen, Cookies oder Indexnummern in Datenbanken, aber auch schon die Angabe des Namens reicht in vielen Fällen aus, damit Suchmaschinen gesammelte Informationen zusammenstellen können.

Die Durchsetzung der Zweckbindung ist schwierig

Die Zweckbindung ist schwer umzusetzen, sofern die Daten nicht bereits für eine kontextspezifische [12] Nutzung vorbereitet sind. Die Anwendung des Grundsatzes der Datensparsamkeit unterstützt den Zweckbindungsgrundsatz sehr wirksam. Für die Beschränkung der Datennutzung auf einen bestimmten Kontext gibt es verschiedene Möglichkeiten, z. B. sektorspezifische Kennungen bei elektronischen Behördendiensten (z. B. „Bürgerkarte“ in Österreich), unterschiedliche Pseudonyme für verschiedene Websites, die Pseudonymisierung personenbezogener Daten in Datenbanken oder so genannte „private credentials“ (geschützte Berechtigungsnachweise) oder „minimal disclosure certificates“ (Mindestoffenlegungs-Zertifikate). Solche „Credentials“ bieten datenschutzfreundliche Möglichkeiten, die Zugangsberechtigung nachzuweisen und damit die Rechenschaftspflicht zu gewährleisten, und stellen gleichzeitig die Anonymität des Nutzers sicher, der nur bei Verstößen identifiziert werden kann. Dadurch wird die Rechenschaftspflicht in der Online-Welt sichergestellt, ohne dass die Nutzer allen Interaktionspartnern ihren echten Namen und weitere persönliche Informationen mitteilen müssen.

Unzureichende Verbreitung technischer Lösungen

Auch wenn all diese Lösungen als Elemente eines nutzerzentrierten Identitätsmanagements diskutiert werden und in den letzten Jahren zu ausgereiften Systemen entwickelt wurden, sind diese Konzepte – insbesondere die komplexeren Ansätze für „private credentials“ – wenig bekannt und werden von Anwendungsentwicklern selten in ihren IKT-Systemen eingesetzt. Auch eine gesellschaftliche Diskussion über die wünschenswerten Voraussetzungen für eine Verknüpfbarkeit oder Unverknüpfbarkeit ist noch kaum entwickelt, da viele Beteiligte diese wichtige Herausforderung noch nicht erkannt haben und noch keine Lösungsmöglichkeiten sehen.

Lösungsvorschläge

Aufgaben für Forschung und Entwicklung

Bessere Umsetzung nötig

Auch wenn die Konzepte für Kontexttrennung und nutzerzentriertes Identitätsmanagement im letzten Jahr weiter optimiert wurden, ist ihre Integration, Interoperabilität und Benutzerfreundlichkeit immer noch verbesserungsbedürftig.

Aufbau einer Infrastruktur für „private credentials“ nötig

Außerdem empfehlen wir, dass Verwaltung und Industrie zum Aufbau der notwendigen Infrastruktur für die Ausstellung von „private credentials“ beitragen und sie in ihren IKT-Systemen an angemessener Stelle einsetzen.

[12] Die Frage, wie feinmaschig das Konzept der „konzeptspezifischen Nutzung“ sein sollte, lassen wir an dieser Stelle offen. In manchen Zusammenhängen kann jede Transaktion einen eigenen Kontext darstellen, in anderen kann eine gröbere Perspektive angemessen sein. Der Begriff der Zweckbestimmung könnte ein Meilenstein für die Kontext-Diskussion sein, doch auch hier besteht noch rechtlicher Klärungsbedarf.

Erforscht werden sollte auch die Messung der Verknüpfbarkeit und Unverknüpfbarkeit. Das ist sowohl für die Entwicklung von IKT-Systemen als auch für die Kontrolle des Nutzers selbst über seine Privatsphäre wichtig. Insbesondere für die langfristige Wahrung der Privatsphäre ist noch nicht geklärt, wie der Datenschutz gewährleistet werden kann.

Messung der Verknüpfbarkeit erforderlich

Aufgaben für den Gesetzgeber

Die Verfügbarkeit von Technologien für die Kontexttrennung wirkt sich auf die Auslegung des Grundsatzes der Datensparsamkeit aus, der besagt, dass personenbezogene Daten so wenig wie möglich verarbeitet werden sollten. Wir empfehlen, dass Gesetzgeber und politische Entscheidungsträger auf nationaler und europäischer Ebene die aktuelle Rechtslage in Bezug auf „private credentials“ evaluieren.

Evaluierung der aktuellen Rechtslage in Bezug auf „private credentials“

Aufgaben im Kommunikationsbereich

Wir schlagen vor, dass die erwünschten Voraussetzungen für eine (Un-) Verknüpfbarkeit und die möglichen rechtlichen, organisatorischen und technologischen Auswirkungen ins Blickfeld der politischen Entscheidungsträger, Datenschutzbeauftragten und Nutzer gerückt werden. Besonders wichtig ist dies bei eher wenig intuitiven Konzepten wie den „private credentials“.

Eine öffentliche Diskussion über die (Un-)Verknüpfbarkeit anstoßen

Links

Brands, Stefan A.: Rethinking Public Key Infrastructures and Digital Certificates, MIT Press, 2000.

Camenisch, Jan, Anna Lysyanskaya: Efficient Nontransferable Anonymous Multishow Credential System with Optional Anonymity Revocation, Research Report RZ 3295, no. 93341, IBM Research, November 2000.

Chaum, David: Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Comm. ACM, Bd. 28, Nr. 10, Oct. 1985, S. 1030-1044.

Clauß, Sebastian, Marit Köhntopp: Identity management and its support of multilateral security, Computer Networks 37(2): 205-219 (2001).

Jøsang, Audun, Simon Pope: User Centric Identity Management, Proceedings of AusCERT, Gold Coast, Mai 2005.

Nissenbaum, Helen: Privacy as Contextual Integrity, Washington Law Review, Bd. 79, Nr. 1, 2004.

PRIME White Paper – Privacy and Identity Management for Europe V3, https://www.prime-project.eu/prime_products/whitepaper/.

4.5 Meldung sicherheitsrelevanter Vorfälle

Ein Schutz der eigenen Privatsphäre ist nur möglich, wenn man über ausreichende Informationen zur geplanten Datenverarbeitung, den damit verbundenen Risiken für die Sicherheit und den Schutz personenbezogener Daten und über sicherheitsrelevante Vorfälle in Bezug auf die eigenen Daten verfügt.

Konkrete Sicherheitslücken

Keine Verpflichtung zur Information der Betroffenen bei Verstößen gegen Datensicherheits- und Datenschutzbestimmungen.

Im Rahmen der gültigen europäischen Datenschutzbestimmungen sind Datenhalter nicht dazu verpflichtet, Betroffene über Vorfälle im Zusammenhang mit Sicherheit und Schutz persönlicher Daten zu informieren. Gemäß Artikel 4 der Richtlinie 2002/58 [13] entsteht eine Verpflichtung der Datenhalter zur Einschränkung möglicher Risiken durch Sicherheitsmaßnahmen und zur Information der Nutzer über diese Risiken nur, bevor ein sicherheitsrelevanter Vorfall eintritt; nach dem Auftreten eines solchen Vorfalles besteht hingegen keine Meldepflicht.

Der Gesetzgeber mag der Ansicht sein, dass der rechtliche Rahmen durch den Wettbewerb auf dem Markt und entsprechende Selbstregulierungsprozesse, in deren Rahmen technische und organisatorische Vorkehrungen zur richtigen Handhabung von sicherheitsrelevanten Vorfällen eingeführt werden, ergänzt wird. Angesichts diverser kritischer und charakteristischer Vorfälle erscheinen diese Anreize jedoch nicht auszureichen, um die Notwendigkeit einer Information des Endnutzers bei Sicherheitsverstößen sowie einer proaktiven Milderung der negativen Auswirkungen solcher Verstöße zu verankern.

Das teilweise oder sogar vollständige Fehlen von Meldungen über sicherheitsrelevante Vorfälle erschwert außerdem die Realisierung von Schutzmaßnahmen, wie sie von der heutigen Gesetzgebung gefordert werden.

Eine weitere direkte Folge dieses Mangels an Informationen über Sicherheitsvorfälle sind unzuverlässige Zahlen und Statistiken, die somit ungeeignet sind, zu mehr Transparenz und Vertrauensbildung beizutragen.

Selbst wenn ein Sicherheitsverstoß bekannt wird, wissen die Bürger in der Regel nicht, auf welche Art sie selbst betroffen sein könnten noch wie sie angemessen reagieren sollten.

[13] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Lösungsvorschläge

Aufgaben für Forschung und Entwicklung

„Security Feeds“ als Standard-Berichtsformat

Auf der Grundlage von Newsfeeds, mit denen z. B. Computernotfallteams sicherheitsrelevante Schwachstellen melden, wurde der Prototyp eines „Security Feed“ getestet, der Informationen zu Datensicherheits- und Datenschutzrisiken und -vorfällen in einem strukturierten XML-Format über einen RSS-Feed überträgt; die Informationen werden dann vom Identitätsmanagement-System des Projekts PRIME – Privacy and Identity Management for Europe (Datenschutz- und Identitätsmanagement für Europa) ausgewertet. Dieses Konzept umfasst alle derzeit eingesetzten Instrumente und Lösungen, wie zum Beispiel Protokolle, Anwendungen, Verschlüsselungsalgorithmen sowie die Identitätsmanagement-Software selbst. Insbesondere erhält der Nutzer Informationen zu Risiken, die seine Privatsphäre betreffen, d. h. Möglichkeiten des unerlaubten Zugriffs auf personenbezogene Daten, und wird über die Folgen, z. B. Handlungsoptionen, aufgeklärt.

Aufgaben für den Gesetzgeber

Datenhalter müssen gesetzlich zur Auskunft bei Sicherheitsverstößen verpflichtet werden.

Die für die Datenverarbeitung verantwortlichen Stellen sollten gesetzlich verpflichtet werden, Betroffene individuell oder über Rundfunk und Fernsehen über Vorfälle zu informieren – ähnlich wie in den Gesetzen zur Notifizierung von Sicherheitsvorfällen (Security Breach Notification Acts), die in vielen amerikanischen Bundesstaaten gelten.

Im November 2007 legte die Europäische Kommission einen Vorschlag[14] zur Revision der Richtlinie 2002/58 vor und führte eine Meldepflicht bei Sicherheitsverstößen ein.

Auch andere Vorfälle sind relevant

Festzustellen ist, dass sich die Diskussion in der Regel ausschließlich auf sicherheitsrelevante Vorfälle beschränkt, z. B. Angriffe durch Hacker oder Datenverlust. Es gibt jedoch auch andere datenschutzrelevante Ereignisse wie etwa Unternehmensfusionen, bei denen Datenbanken zusammengelegt werden oder die Auslagerung der Verarbeitung personenbezogener Daten in ein anderes Land. Auch solche Informationen können für den Schutz der Privatsphäre des Einzelnen relevant sein.

[14] Vorschlag vom 13. November 2007 für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Aufgaben im Kommunikationsbereich

Mitteilungen über sicherheitsrelevante Vorfälle versetzen den Bürger in die Lage, seine persönlichen Daten zu schützen

Die Bürger sollten auf verständliche Weise über Vorfälle informiert werden, die die Sicherheit und den Schutz von personenbezogenen Daten betreffen könnten. Ebenso sollte der Einzelne in jedem Fall Beratung erhalten, welche Maßnahmen er ergreifen kann, um unerwünschte Auswirkungen auf seine Privatsphäre zu minimieren. Diese Informationen erhöhen die Transparenz der Verarbeitung personenbezogener Daten und dienen dem Einzelnen als Grundlage für die Steuerung seiner Privatsphäre.

Genauere und umfassendere Berichte über Sicherheitsverstöße würden die Möglichkeit eröffnen, die Entwicklung zuverlässiger Sicherheitsvorkehrungen nach entsprechenden Vorfällen sowie gezielter Ausgleichsmaßnahmen zur Kontrolle des Restrisikos zu fördern.

Mehrere Kanäle zur Meldung von Informationen über sicherheitsrelevante Vorfälle

Nicht nur die Datenhalter selbst, auch andere Akteure wie Zeitungen, Datenschutzbehörden, Verbraucherschutzorganisationen oder Fachkollegen könnten Informationen über Risiken für Datensicherheit und Datenschutz bzw. einschlägige Vorfälle verbreiten. Die Informationen könnten in einem digitalen Standardformat übermittelt werden, welches die Auswertung durch die Computer der Nutzer erleichtert. Vor allem die Kombination mit benutzergesteuerten Identitätsmanagement-Systemen lässt hier Synergien entstehen.

Links

Security Breach Notification Laws: Views from Chief Security Officers A Study Conducted for the Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law, Dezember 2007, http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf.

Hansen, Marit, Jan Schallaböck: Extending Policy Negotiation in User-Controlled Identity Management by Privacy & Security Information Services, Position Paper Submission to the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, http://www.w3.org/2006/07/privacy-ws/papers/18-hansen-user-controlled-idm/.

Hansen, Marit: Marrying Transparency Tools With User-Controlled Identity Management. In: Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, Leonardo Martucci (Hrsg.): The Future of Identity in the Information Society, Proceedings of the Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society, August 2007; IFIP International Federation for Information Processing, Band 262; Springer; 2008, S. 199-220.

Hogan & Hartson Analysys: Preparing the Next Steps in Regulation of Electronic Communications – A Contribution to the Review of the Electronic Communications Regulatory Framework.

http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/next_steps/regul_of_ecomm_july2006_final.pdf.

Nageler, Antje: Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem. Diplomarbeit, Christian-Albrechts-Universität zu Kiel, Mai 2006.

4.6 Leitlinien für Zertifizierungsprogramme

Zertifizierungen können helfen, die Einhaltung von Datenschutzstandards nachzuweisen

Eines der größten Probleme der heutigen Informationsgesellschaft ist der Mangel an Transparenz von IKT-Produkten und -dienstleistungen hinsichtlich der Einhaltung von Datensicherheits- und Datenschutzstandards. Für Nutzer ebenso wie für Datenhalter und Datenschutzbehörden ist dies eine der wichtigsten Herausforderungen im Zusammenhang mit IKT-Systemen. Zertifizierungsprogramme sollten sicherstellen, dass ein Produkt oder eine Dienstleistung im Einklang mit den europäischen Rechtsvorschriften zum Datenschutz entwickelt wurde und angewendet werden kann.

Konkrete Sicherheitslücken

Noch gibt es keine Datenschutzzertifizierung

Die Verfügbarkeit zuverlässiger IKT-Lösungen im Allgemeinen und technologischer Anwendungen mit verbessertem Datenschutz im Besonderen liegt im Interesse aller Akteure in der EU. Daher sollte die Aufmerksamkeit auf die Entwicklung von Möglichkeiten und Kriterien zur harmonisierten Verbreitung zuverlässiger und datenschutzkonformer Zertifizierungsprogramme in allen Mitgliedstaaten gerichtet werden.

Zertifizierung gewährleistet effizienten Datenschutz

In diesem Abschnitt sollen diesbezügliche Lücken mit den jeweiligen Abhilfemaßnahmen sowie die angestrebten Auswirkungen/Vorteile erläutert werden. Dazu gehören Wettbewerbsvorteile, größeres Vertrauen zu zertifizierten Produkten, eine Steigerung des öffentlichen Vertrauens und Bewusstseins, die Förderung eines „eingebauten“ anstelle eines nachträglich hinzugefügten Datenschutzes und die homogene, und damit effektivere, Anwendung von Datenschutzregeln für alle Akteure der Informationsgesellschaft (betroffene Personen, Datenhalter, Datenschutzbehörden, IKT-Entwickler, Anbieter, Hersteller, Mitgliedstaaten usw.).

Es sollte ein Mindestmaß an Schutz persönlicher Daten definiert werden

In unseren Augen entscheidend ist, dass (a) solche Zertifizierungsprogramme letztendlich gewährleisten sollten, dass ein Produkt ein gewisses (Mindest-)Maß an Datenschutz garantiert, dass (b) zu diesem Zweck eine entsprechende Methodik entwickelt sowie die Akzeptanz solcher Zertifizierungssysteme gefördert werden muss und dass (c) die zur Beurteilung der Datenschutzkonformität eingesetzten Kriterienwerke, Zertifizierungskriterien und -bedingungen von geeigneten Stellen standardisiert werden müssen.

Lösungsvorschläge

Es müssen Anreize für eine Zertifizierung geschaffen werden

Die Mitgliedstaaten sollten Zertifizierungsprogramme fördern und verfolgen, an denen auch Verbraucherverbände beteiligt werden. Dabei sollten die Mitgliedstaaten Steueranreize für Unternehmen schaffen, die sich an die Bestimmungen halten, und erwägen, ob sie Unternehmen, die eine Datenschutz-Zertifizierung durchführen, bestimmte Meldepflichten erlassen.

Im Anschluss an Überlegungen, ob ein solches Zertifizierungssystem obligatorisch sein sollte oder nicht, wer die Einführung solcher Systeme befürworten sollte und wie ein allgemeiner Konsens hinsichtlich der erforderlichen Datenschutzanforderungen auf transparente Weise zu erreichen ist, sollten neue Lösungen zur Förderung der Datenschutzkonformität untersucht werden. So sollten die Mitgliedstaaten z. B. Instrumente für Unternehmen entwickeln, mit denen diese eine Zertifizierung oder Selbstzertifizierung in Bezug auf die Einhaltung der Datenschutzvorschriften durchführen können, wenn sie sich an öffentlichen Ausschreibungen beteiligen.

Es gibt bereits Erfahrungen mit Zertifizierungsprogrammen

Geeignete Ideen lassen sich aus den Erkenntnissen ähnlicher Forschungsprojekte (z. B. EuroPriSe [15]) und anderer Länder (z. B. der Schweiz [16]), die Zertifizierungsprogramme entwickelt haben, ableiten sowie aus Erfahrungen mit zugelassenen elektronischen Signaturen, Verschlüsselungstechnologien und deren jeweiligen Rechtsrahmen.

Schlüsselmerkmale eines Datenschutz-Zertifizierungsprogramms

Unserer Ansicht nach sollte ein Zertifizierungsprogramm folgende Schlüsselmerkmale aufweisen: Interessenten, die in der Öffentlichkeit als akkreditierte Datenschutz- und Datensicherheits-Zertifizierer auftreten möchten, sollten zu diesem Zweck von bestimmen unabhängigen (dritten) Stellen, die bereits als Akkreditierungsbehörden etabliert sind, (in Zusammenarbeit mit den Datenschutzbehörden) zertifiziert werden. Diese Zertifizierung sollte dann stattfinden, wenn die Interessenten die jeweiligen technischen und gesetzlichen Anforderungen erfüllen („eingebauter“ Datenschutz, beste verfügbare Techniken, Mindestmaß an Datenschutzprinzipien), wie sie in den jeweiligen von den Datenschutzbehörden in Zusammenarbeit mit der Artikel-29-Datenschutzgruppe und der Europäischen Kommission herausgegebenen Regelwerken aufgeführt sind. Das Zertifikat sollte eine begrenzte Gültigkeitsdauer von etwa zwei bis drei Jahren haben, wobei jährliche Konformitätsprüfungen während dieses Zeitraums vorgesehen werden sollten. Bei Verstößen, Missbrauch, Falschangaben oder widerrechtlicher Verwendung

[15] Siehe unter http://www.european-privacy-seal.eu/.

[16] Siehe Verordnung über die Datenschutzzertifizierungen - Ordonnance sur les certifications en matiere de protection des données (VDSZ-OCPD) vom 28. September 2007 des Schweizerischen Bundesrats sowie das Bundesgesetz über den Datenschutz der Bundesversammlung der Schweizerischen Eidgenossenschaft (Loi federale sur la protection des données - LPD) vom 19. Juni 1992 (Etat le 1er Janvier 2008. Siehe unter: http://www.admin.ch/ch/e/rs/235_13/index.html.

des Zertifikats sollten Strafen und Geldbußen verhängt und natürlich das Zertifikat entzogen werden. Es müssen daher auf Kommissionsebene weitere legislative Schritte in diese Richtung unternommen werden, um eine harmonisierte Einführung und Anwendung innerhalb der Europäischen Union zu unterstützen. Vor allem sollten Kontrollen und die Haftung der Prüfer und der Inhaber von Zertifikaten festgelegt werden.

Notwendigkeit einer internationalen Standardisierung

Schließlich sollten die Kriterienwerke für die Zertifizierung auf internationaler Ebene standardisiert werden, um eine Harmonisierung und Transparenz der verwendeten Methoden und der geprüften Kriterien zu erreichen. Diese Kataloge sollen die Kriterien enthalten, die im Rahmen der Bewertung von IKT-Produkten und -Dienstleistungen für die Überprüfung heranzuziehen sind. Sie sollen den Prüfern als Leitfaden für die Durchführung einer solchen Bewertung dienen.

4.7 Überwachungsinstrumente

Zur Durchführung interner Datenschutzprüfungen werden geeignete Werkzeuge benötigt

Unternehmen, die personenbezogene Daten verarbeiten, müssen ihre Datenschutzgrundsätze festlegen und sicherstellen, dass diese in ihrem Umfeld auch eingehalten werden. Aufgrund der vielen Parameter, die dabei berücksichtigt werden müssen, sind diese Datenschutzgrundsätze meist sehr komplex. Sobald die Datenschutzgrundsätze aufgestellt sind, sollten skalierbare automatisierte Lösungen eingesetzt werden, mit denen ihre Einhaltung regelmäßig überprüft wird. Doch fehlt es der Industrie hierzu an geeigneten Überwachungs- und Managementinstrumenten für interne Datenschutzprüfungen.

Solche Instrumente sind auch für die Aufsichtsbehörden nützlich

Darüber hinaus sind die Datenschutzbehörden immer wieder mit Schwierigkeiten konfrontiert, wenn sie Kontrollen durchführen und die Speicherung, Verarbeitung und Verwendung personenbezogener Daten prüfen wollen. Der EU-Rechtsrahmen enthält genaue Bestimmungen hinsichtlich der Pflichten und Sicherheitsmaßnahmen, die die für die Datenverarbeitung Verantwortlichen (data controllers) erfüllen und umsetzen müssen[17], nennt jedoch keine konkreten Überwachungsinstrumente bzw. enthält keine Vorgaben, dass solche Instrumente zur Unterstützung der Arbeit der Aufsichtsbehörden zu entwickeln sind.

Konkrete Sicherheitslücken

Datenschutz-Prüfungen sind ressourcenintensiv

Die meisten IKT-Systeme zur Verarbeitung personenbezogener Daten sind gewöhnlich nicht so ausgelegt, dass Prüfungen oder auch nur Selbstkontrollen leicht durchgeführt werden können. Für die Prüfungen sind jeweils maßgeschneiderte Lösungen notwendig, die zusätzliche Ressourcen erfordern.

[17] Siehe Artikel 17 der Richtlinie 95/46/EG.

Dazu gehört die Fähigkeit zu prüfen, ob eine physische Datenschutzvorrichtung die hohen Datenschutzanforderungen erfüllt. Folglich müssen dedizierte Metriken für den Datenschutz erwogen werden, was bestimmte Mittel einschließt, mit denen die anspruchsvollen Spezifikationen für die Konfigurationen innerhalb der betreffenden Informationssysteme erstellt werden können.

Angesichts des enormen Umfangs der zu überprüfenden Datenerfassungstätigkeit müssen für verlässliche automatisierte Prüfungen zudem unbedingt standardisierte und verbindliche Aufzeichnungstechniken entwickelt werden.

Überwachungsinstrumente sind für Industrie, Datenschützer und Anwender gleichermaßen nützlich

Es könnte sinnvoll sein, diese Überwachungsinstrumente auch den Datenschutzbehörden zur Verfügung zu stellen, damit sie ihre Kontrollbefugnisse kontinuierlich und möglicherweise auch per Fernzugang wahrnehmen können. Auch der Endnutzer sollte technisch in der Lage sein, automatische Rückmeldungen über die Verarbeitung seiner personenbezogenen Daten zu empfangen.

Lösungsvorschläge

Aufgaben für Forschung und Entwicklung

„Zugriffsschutzrichtlinien als „sticky policies“

Datenschutzbestimmungen könnten auf die übertragenen Daten angewendet werden (z. B. als „Sticky Policies“, die an die Daten angeheftet werden), und die datenverarbeitende Stelle wäre dann verpflichtet, diese Grundsätze zu befolgen. Aus Gründen der Transparenz müssten dann nicht nur – wie heute schon gesetzlich vorgeschrieben – die Empfänger in Gruppen zusammengefasst, sondern jeder einzelne reale Empfänger genau dokumentiert werden.

Technische und rechtliche Datenschutzanforderungen über Prüfpfade synchronisieren

Durch effiziente automatisierte Überprüfungsinstrumente für die Datenschutzpraxis ließen sich Regelungen leichter durchsetzen. Prüfpfade könnten proaktiv in die Systeme eingebaut werden, um im Nachhinein Rückschlüsse auf die technische Lösung zur Umsetzung des Datenschutzes zu ermöglichen und zu prüfen, ob diese Lösung angemessen hohen Datenschutzanforderungen entspricht.

Forschungs- und Entwicklungsarbeiten zur Bereitstellung von mehr automatisierten Instrumenten für Kontrollen, Rückverfolgbarkeit und Prüfmaßnahmen sollten unterstützt werden. Eine andere Möglichkeit wäre, diese Tätigkeiten auszulagern und akkreditierte (private) Stellen damit zu beauftragen, die auch qualifiziert sind, datenschutzkonform arbeitenden Organisationen entsprechende Zertifikate auszustellen (wie z. B. beim Zertifizierungsprogramm im schweizerischen Kanton Genf).

Festgelegte Kriterienkataloge vereinfachen die Prüfung

Sowohl interne Auditoren (zum Beispiel die Audit-Abteilung) als auch externe Prüfer (z. B. die zuständige Datenschutzbehörde) könnten von festgelegten (und möglicherweise standardisierten) Prüfkriterien für IKT-Systeme und

Datenverarbeitungsabläufe profitieren. Darüber hinaus sollten die für die Prüfung verwendeten Testverfahren alle relevanten Fälle abdecken. Für eine Langzeit-Überwachung könnte man auch bestimmte Blinddaten einfügen und dann sehen, ob diese Daten durchsickern und später außerhalb des IKT-Systems auftauchen. Man müsste dann aber auch sehr gut aufpassen, dass diese Testdaten nicht selbst zu einer unkontrollierten digitalen Identität werden, die missbraucht werden kann.

Aufgaben für den Gesetzgeber

Prüfpfade auf dem gesamten Datenpfad vorschreiben

Es wäre denkbar gesetzlich vorzuschreiben, dass die Verarbeitung personenbezogener Daten nur erlaubt ist, wenn die Daten aus einer zuverlässigen Quelle stammen, bei der alle Datenübertragungen dokumentiert werden müssen.

Fernzugang für Datenschutzbehörden

Zur Überprüfung der Übereinstimmung der Systeme mit den Meldungen und zur Erleichterung der Prüfungen könnte auch ein ständiger Fernzugang der Datenschutzbehörden zu begrenzten Merkmalen der datenverarbeitenden Stellen erwogen werden.

Aufgaben im Kommunikationsbereich

Interne Kontrolle durch Selbstprüfungen

Berichte über Selbstprüfungen würden außerdem die Effizienz der Arbeit der Überwachungsbehörden unterstützen; letztere wären dann nämlich in der Lage, die größten Schwachstellen zu ermitteln und sich bei ihrem eigenen Prüfverfahren auf diese zu konzentrieren.

4.8 Beste verfügbare Techniken

BVT sind eine spezifische Kombination aus Technologien, Protokollen und Standards

Datenschutz und Datensicherheit sind komplexe Probleme, für die es kaum eine allgemeine technische Patentlösung geben wird. Vielmehr erfordern unterschiedliche Anwendungsbereiche eine jeweils unterschiedliche technische Unterstützung im Hinblick auf den Schutz der Privatsphäre der Bürger. Eine technische Unterstützung dieser Art muss sorgfältig durch einen Rechtsrahmen und Leitlinien für die Praxis ergänzt werden, die speziell auf eine bestimmten Anwendungsbereich oder ausgewählte operative Grundsätze ausgerichtet sind. Diese bestimmte Kombination von Technologien, Protokollen, Normen, Verfahren usw., mit der ein angemessener Datenschutz in einem bestimmten Bereich gewährleistet werden kann, lässt sich als „beste verfügbare Techniken“ (BVT) bezeichnen.

Konkrete Sicherheitslücken

BVT für Datenschutz und Datensicherheit müssen festgelegt und harmonisiert werden

Es besteht - auf europäischer Ebene – eine Lücke im Hinblick auf die Festlegung und Harmonisierung der besten verfügbaren Techniken (BVT) in verschiedenen Bereichen und den Umfang ihrer Anwendung durch für die Datenverarbeitung

verantwortliche Stellen und Auftragsverarbeiter.

Beispiel: Schutz von Aufenthaltsinformationen

Die aktuelle Diskussion um die Techniken zum Schutz von Aufenthaltsinformationen veranschaulicht diese Lücke. Viele der zur Zeit zum Schutz von Aufenthaltsinformationen vorgeschlagenen Ansätze versuchen, Informationen zum Aufenthaltsort so zu verschleiern, dass in einem bestimmten Gebiet mindestens *k-1* weitere Nutzer zum entsprechenden Zeitpunkt dieselbe Ortsinformation haben. Dieses Prinzip wird „k-Anonymität“ genannt. Diese Methode ist zwar effizient, aber man muss sich trotzdem eingehender mit der praktischen Anwendung solcher Methoden befassen. Wie kann ein Nutzer beispielsweise eine auf dem Prinzip der *k-Anonymität* beruhende Verschleierungstechnik anwenden? Wie könnte man beurteilen, welcher *k*-Wert angemessen ist oder wann das System ein- bzw. ausgeschaltet werden muss? Wie könnte ein ausgewogenes Verhältnis zwischen Genauigkeit der Aufenthaltsinformationen und Schutz der Aufenthaltsinformationen hergestellt werden? Oder sollte man einfach ein Modell wählen, bei dem ein vertrauenswürdiger Dienstleister, z. B. der Mobiltelefon-Anbieter, alle Daten zentral verwaltet, und statistische Datenbanken und andere Werkzeuge nutzen, um Anwenderprofile zu schützen? Unterschiedliche Anwendungs-Szenarien könnten unterschiedliche Lösungen erfordern.

Lösungsvorschläge

Bei der Definition bester verfügbarer Techniken im Bereich des Datenschutzes geht es sowohl darum, die geeigneten Techniken zu ermitteln, als auch darum, Verfahren zur Harmonisierung dieser Techniken in den EU-Mitgliedstaaten festzulegen.

Aufgaben für Forschung und Entwicklung

Technologien und Vorgehensweisen ermitteln und zusammenstellen

In einem ersten Schritt müssten die einschlägigen Anwendungen ermittelt werden, insbesondere im Bereich der neueren technologischen Entwicklungen (wie z. B. RFID, standortbezogene Dienste und Biometrie). Diese sollten dann nach ihren jeweiligen Informationsflussmodellen, d. h. ihren besonderen Datenverarbeitungsmethoden und ihrem Informationsbedarf spezifischer kategorisiert werden.

Geeignete Techniken für spezifische Anwendungsbereiche finden

Sobald allgemeine Anwendungstypen ermittelt worden sind, können die aktuellen Technologien und Verfahren erhoben und festgelegte beste verfügbare Techniken für die jeweiligen Anwendungen definiert werden. Wie bereits weiter oben erwähnt, sind wirtschaftliche und technische Machbarkeit wichtige Faktoren bei einer solchen Bewertung.

Aufgaben für den Gesetzgeber

Datenschutzbehörden einbeziehen und Durchsetzungsmodelle festlegen

Die Datenschutzbehörden müssen in dieses Verfahren zur Ermittlung und Auflistung der besten verfügbaren Techniken für Datenschutz und Datensicherheit einbezogen werden. Es muss festgelegt werden, wie

Datenschutzbehörden die Anwendung der besten verfügbaren Techniken durchsetzen können und sollten, insbesondere wenn Technologien zwar vorhanden, aber nicht Teil standardardisierter Systeme sind (z. B. sicheres Löschen mit Hilfe von Wiping Tools, die kein Bestandteil von Standardbetriebssystemen sind) oder wenn ihre Anwendung entweder die Zusammenarbeit mehrerer Parteien oder eine zusätzliche Infrastruktur erfordert (z. B. können Anonymisierungssysteme, die personenbezogene Daten schützen sollen, bevor sie für eine datenverarbeitende Stelle sichtbar sind, nicht von dieser selbst betrieben werden, sondern nur durch zusätzliche unabhängige Anbieter).

Zukünftige Verknüpfungen von Technologien voraussehen

Zu beachten ist, dass bei den verschiedenen Lösungen die Risiken in Betracht gezogen werden müssen, die durch die Kombination mehrerer vorhandener Technologien entstehen. Diese Risiken müssen vorausgesehen, analysiert und quantifiziert werden. Erhebliche Risiken entstehen zum Beispiel bei der Verknüpfung von Gesichtserkennungsbiometrik mit Videoüberwachungs-Systemen oder von standortbezogenen Diensten, die über kartographische Informationen verfügen. Bei der Festlegung der Verfahrensweisen im Hinblick auf eine spezifische Technologie sollten zukünftige Nutzungen daher soweit wie möglich abgeschätzt werden, so dass in jeder Phase der jeweiligen Technologieentwicklung geeignete Sicherungsmaßnahmen vorgesehen werden können.

Aufgaben im Kommunikationsbereich

Ein öffentlicher Prozess

Die Liste der ermittelten besten verfügbaren Techniken (BVT) für wichtige Anwendungsmodelle und deren Merkmale müssen öffentlich gemacht werden, damit alle für die Datenverarbeitung verantwortliche Stelle und die Auftragsverarbeiter davon Kenntnis erlangen können. Beispielhafte Verfahren können die Verwendung der BVT veranschaulichen.

Links

BVT wurden im Umweltbereich in der IPPC-Richtlinie 96/61/EC[18] erfolgreich festgelegt.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat kürzlich ein Projekt gestartet, das als Beispiel für den Einsatz von BVTs in RFID-Anwendungen[19] dienen könnte.

[18] http://ec.europa.eu/environment/air/legis.htm#stationary.

[19] http://www.bsi.de/presse/pressinf/071207_RFID.htm.

4.9 Wirksame Anreize und Sanktionen

Datenschutzbestimmungen werden häufig nicht eingehalten

Das Datenschutzrecht ist relativ eigentlich schon recht alt. In der heutigen Welt der Datenverarbeitung ist es jedoch an der Tagesordnung, dass IKT-Komponenten und Organisationsstrukturen die Datenschutzbestimmungen nicht erfüllen. In den letzten Jahrzehnten konnte man beobachten, dass datenschutzfreundliche Technologien nicht in nennenswertem Umfang entstehen, wenn man sich allein auf die Regulierungskräfte des freien Marktes verlässt.

Konkrete Sicherheitslücken

Es fehlt an Motivation und Anreizen

Eine allgemeine Lücke besteht darin, dass die für die Verarbeitung der Daten verantwortlichen Stellen nicht wirklich motiviert sind, die Bestimmungen des Datenschutzrechts einzuhalten. Eng mit diesem Defizit verbunden ist die fehlende Motivation, datenschutzfreundliche Technologien einzusetzen, wodurch letztlich auch die technische Entwicklung angekurbelt würde.

Fehlende Instrumente erschweren die Kontrolle durch die Datenschutzbehörden

Im Allgemeinen können Sanktionen nur verhängt werden, wenn der zuständigen Aufsichtsbehörde oder einem Gericht ein Verstoß gegen das Datenschutzgesetz bekannt wird. Gegenwärtig kontrollieren die Datenschutzbehörden nur wenige der für die Datenverarbeitung Verantwortlichen, was dazu führt, dass datenschutzrechtlich relevante Verstöße bei der Datenverarbeitung häufig unbemerkt bleiben.

Die heute üblichen Sanktionen halten kaum zur Einhaltung der Datenschutz-bestimmungen an

Die häufig leichten Sanktionen können kaum dazu anhalten, die Datenschutzbestimmungen zu befolgen. So können für die Datenverarbeitung verantwortliche Stellen in einigen Rechtsprechungen nur einmal mit einem Bußgeld belegt werden – auch wenn sie danach ihre Datenverarbeitung nicht umstellen. In mehreren Fällen haben Gerichte verhängte Bußgelder wieder aufgehoben, um zu vermeiden, im Fall eines Diskriminierungsvorwurfs auch alle Konkurrenten der beschuldigten verantwortlichen Stelle kontrollieren zu müssen.

Lösungsvorschläge

Einhaltung der Datenschutzbestimmungen durch Belohnung oder Bestrafung

Um die für die Datenverarbeitung verantwortlichen Stellen darin zu bestärken, die persönlichen Daten der Betroffenen besser zu schützen, sind zwei generelle Lösungen denkbar:

1. *Anreize* schaffen, mit denen die für die Datenverarbeitung verantwortlichen Stellen belohnt werden
2. *Sanktionen* vorsehen, mit denen die für die Datenverarbeitung verantwortlichen Stellen bestraft werden

Unterschiedliche Wirksamkeit von Sanktionen im privatwirtschaftlichen und öffentlichen Sektor

Was als Anreiz oder Sanktion tatsächlich wirkt, hängt von der für die Datenverarbeitung verantwortlichen Stelle im Einzelnen ab. Für Unternehmen stehen wirtschaftliche Faktoren an vorderster Stelle. Das bedeutet unter anderem, dass ein Bußgeld für datenschutzrechtliche Verstöße für das Unternehmen deutlich spürbar sein muss – der nicht regelkonforme Umgang mit personenbezogenen Daten darf sich für das Unternehmen nicht auszahlen. Bei behördlichen Verarbeitungsprozessen *müssen* die Datenschutzbestimmungen eingehalten werden – andernfalls müssten die Aufsichtsbehörden sofort intervenieren.

Aufgaben für Forschung und Entwicklung

Standardisierte Prüfinstrumente zur Kontrolle der Einhaltung der Datenschutzbestimmungen

Der Mangel an automatisierten Prüfinstrumenten bewirkt, dass Verstöße kaum geahndet werden. Solche Instrumente erfordern einen Standardisierungs- und Zertifizierungsprozess, bei dem in Zusammenarbeit mit den Datenschutzbehörden die für einen entsprechenden Prüfpfad erforderlichen Informationen ermittelt werden.

Aufgaben für den Gesetzgeber

Zertifizierungspflicht oder Nachweis der Verwendung von Datenschutztechnologie

Bei der Vergabe öffentlicher Aufträge könnte der Nachweis der Verwendung datenschutzfreundlicher Technologie oder eine Zertifizierung bzw. Selbstzertifizierung vorgeschrieben werden. Bestimmte technische Maßnahmen könnten, wie bereits in einigen Rechtsprechungen geschehen, als obligatorisch eingestuft werden; welche Maßnahmen am besten geeignet sind, bliebe noch festzulegen.

Wirksame und wirtschaftlich spürbare Sanktionen

Wirksame Sanktionen könnten dazu beitragen, die für die Datenverarbeitung verantwortlichen Stellen davon zu überzeugen, datenschutzkonforme Systeme zu verwenden. Sanktionen sollten nicht auf administrative Sanktionen beschränkt sein (in einigen Ländern gibt es auch strafrechtliche Sanktionen), sondern auch eine Haftungspflicht umfassen. In diesem Fall fiele den Verbraucherverbänden eine wichtige Rolle zu.

In einigen Mitgliedstaaten funktionieren die Sanktionssysteme jedoch nicht effektiv. Sie müssten durch wirksame Prüfverfahren unterstützt werden. Andererseits sollten aber auch Anreize, beispielsweise steuerliche Vorteile, geschaffen werden. Das ist aber nur sinnvoll, wenn daran ein Zertifizierungssystem gekoppelt wird.

Wir empfehlen, dass die Europäische Kommission und die Mitgliedstaaten ein an Zertifizierung und wirksame finanzielle Sanktionen geknüpftes System von Anreizen unterstützen.

Aufgaben im Kommunikationsbereich

Informationskampagnen für Verbraucher

Die Einhaltung der Datenschutzbestimmungen oder der (nachweisliche) Einsatz datenschutzfreundlicher Technologie können ein wichtiges Verkaufsargument für die Datenverarbeiter sein. Das würde sich auch positiv auf den Ruf des

Unternehmens und damit auf die Gewinnung und Bindung von Kunden auswirken. Informationskampagnen können eine Nachfrage des Marktes nach datenschutzkonformen Systemen auslösen, insbesondere wenn es für die Verbraucher möglich ist, ihre Forderungen ohne großen Aufwand einzubringen. Datensparsamkeit bedeutet geringeres Missbrauchsrisiko und fördert den guten Ruf der für die Verarbeitung der Daten verantwortlichen Stelle.

Die Vorteile anonymer Daten deutlich machen

Die verantwortlichen Stellen könnten davon überzeugt werden, dass die Organisation der Datenverarbeitung unter Datenschutzgesichtspunkten, insbesondere nach dem Grundsatz der Datenminimierung häufig kostengünstiger ist, als wenn man neben Speichermedien auch für geeignete Sicherheitseinrichtungen, Dokumentation sowie für den Zugang der Betroffenen zu ihren Daten oder zu Rechtsbehelfen Sorge tragen muss.

Links

Ross Anderson unterhält eine Seite zu „Economics and Security Resource“ („Ökonomie und IT-Sicherheit“) auf seiner Website[20], Alessandro Acquisti eine ähnlich gelagerte Site zur Ökonomie des Datenschutzes.[21]

4.10 Welche Daten sind personenbezogen?

Der Begriff personenbezogene Daten deckt alle Informationen ab, die auf eine einzelne Person bezogen werden können

Gemäß der Richtlinie 95/46/EG sind unter personenbezogenen Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person“) zu verstehen. Dieser Begriff ist weit gefasst, da er alle Informationen abdeckt, die mit einer Person verbunden werden können. Tatsächlich können verschiedene Daten zusammengeführt werden und dann Rückschlüsse auf die Identität einer Person ermöglichen (z. B. durch soziale Netze, die Verfolgung von RFID-Etiketten, die Kombination von Suchanfragen auf Suchmaschinen usw.). Europäische Gesetzgeber haben den Begriff der personenbezogenen Daten zwar weit gefasst, aber er hat durchaus seine Grenzen. Der Geltungsbereich der Datenschutzbestimmungen darf nicht überstrapaziert, der Begriff der personenbezogenen Daten aber auch nicht unangemessen eingeschränkt werden. Da die Grenzen zwischen personenbezogenen und nicht personenbezogenen Daten manchmal jedoch verwischen, wurden Versuche unternommen, den Begriff eindeutig zu fassen, wie beispielsweise in der Stellungnahme der Artikel-29-Datenschutzgruppe zum Begriff der personenbezogenen Daten.

[20] Siehe unter: http://www.cl.cam.ac.uk/~rja14/econsec.html.
[21] Siehe unter http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.

Konkrete Sicherheitslücken

Es ist nicht immer eindeutig, ob Daten personenbezogen sind

Trotz der Anstrengungen, die die Artikel-29-Datenschutzgruppe vor kurzem unternommen hat, um den Begriff der personenbezogenen Daten zu klären, ist der Begriff häufig umstritten. Das ist insofern problematisch, als für Daten, die nicht als personenbezogen betrachtet werden, möglicherweise keine ausreichenden Sicherheitsmaßnahmen getroffen werden um sicherzustellen, dass sie nicht zu personenbezogenen Daten werden.

Beispiel: RFID-Etiketten im Einzelhandel werden nicht deaktiviert, auch wenn das Etikett keine Funktion außerhalb des Geschäfts hat

Darüber hinaus sind die Auffassungen, was als hinnehmbares Eindringen in die Privatsphäre angesehen wird, und das, was die Nutzer als personenbezogene Daten ansehen, dynamische Konzepte. Die RFID-Technologie findet sich heute in vielen Anwendungen wieder (z. B. Einzelhandel, digitale Identität auf Ausweispapieren und Autoschlüsseln, mobiles Bezahlen usw.). Diese Technologie birgt viele Sicherheitsrisiken, da sie eine quasi unbegrenzte Nutzerüberwachung und Datenerhebung ermöglicht, ohne dass die betroffene Person etwas davon bemerkt. Mit dieser Technologie kann eine natürliche Person identifiziert werden, wenn ihr Name oder ihre biometrischen Daten im Etikett gespeichert sind. Außerdem ist es möglich, die Tätigkeiten einer Person, die Gegenstände mit sich führt, die ein RFID-Etikett tragen (das einen unverwechselbaren Code enthält) aufzuzeichnen und zurückzuverfolgen sowie ein Personenprofil zu erstellen. Im Einzelhandel werden solche Etiketten, die in der Regel keine personenbezogenen Daten enthalten und rein logistischen Zwecken dienen, an der Kasse normalerweise nicht deaktiviert, so dass der Käufer aktive elektronische Etiketten mit sich trägt, die dazu verwendet werden könnten, aufzuzeichnen, wo er sich bewegt.

Durch den Einfluss sozialer Faktoren, erwarteter Sicherheitsanforderungen und technischer Verbesserungen ändern sich im Laufe der Zeit die Auffassungen darüber, wie weit ein Eindringen in die Privatsphäre hinnehmbar ist und welche Daten die Nutzer als personenbezogene Daten ansehen. Soziale Faktoren spielen bei den Reaktionen auf datenschutzbedenkliche Technologien eine Rolle, da die Auffassung von Privatsphäre subjektiv ist und von Alter, Bildung und Umfeld beeinflusst wird. Auch hinsichtlich der erwarteten Sicherheitsanforderungen gibt es Unterschiede: Erfahrene Nutzer möchten ihre Systeme möglicherweise selbst bis ins Detail konfigurieren, während die Mehrheit wahrscheinlich einfache, leicht verständliche und datenschutzkonforme Standardeinstellungen bevorzugt. Daten, die heute als nicht personenbezogene Daten gelten (da sie nur mit sehr aufwändigen Mitteln auf eine Person bezogen werden könnten) können im Zuge des technologischen Fortschritts zu personenbezogenen Daten werden.

Lösungsvorschläge

Aufgaben für Forschung und Entwicklung

Entwicklung geeigneter technischer Sicherheitsvorrichtungen auch für Daten, die nicht zu personenbezogenen Daten werden sollen

Um die mit der Datenverarbeitung verbundenen Risiken für den Datenschutz zu bewerten, müssen Methoden zur Folgenabschätzung entwickelt und angewendet werden. Wie ausgedehnt die Analyse durchzuführen ist, sollte davon abhängig gemacht werden, wie sensibel die Verarbeitung und die betroffenen Daten sind.

Es sollten Sicherheitsvorrichtungen entwickelt werden, mit denen individuelle Daten, unabhängig davon, ob es sich dabei um personenbezogene Daten handelt oder nicht, angemessen geschützt werden. Dadurch werden Befugnisse und Kontrolle der Nutzer eindeutig gestärkt.

Bei der Entwicklung solcher Systeme und der Festlegung von Vorschriften sollte künftigen technischen Mitteln und Entwicklungen angemessen Rechnung getragen werden, beispielsweise der Möglichkeit, dass nicht personenbezogene Daten im Zuge der technologischen Entwicklung durchaus zu personenbezogenen Daten werden können.

Die sozialen Auswirkungen der neuen Technologien sollten systematisch und wissenschaftlich bewertet und der Nutzen der Technologien nachgewiesen werden.

Aufgaben für den Gesetzgeber

Die Datenschutzbestimmungen sollten sicherstellen, dass aus nicht personenbezogenen Daten keine personenbezogenen Daten werden können

Die Datenschutzbestimmungen sollten einen angemessenen Schutz der Daten sicherstellen, vor allem wenn nicht ausgeschlossen werden kann, dass aus ihnen personenbezogenen Daten werden könnten.

Als Form der Ausübung des Rechts auf Schutz der Privatsphäre und des Rechts auf Schutz der personenbezogenen Daten muss das Recht auf Anonymität fortlaufend mit anderen Grundrechten abgewogen werden. Da es in der Regel keine absolute Anonymität geben kann, sollte Formen angemessener Anonymität Raum gegeben werden.

Besonders wenn sensible Daten betroffen sind, sollten möglichst dem Zweck angemessene Anonymisierungsprogramme verwendet werden.

Sobald ein Recht gesetzlich verankert und gegen andere Rechte abgewogen ist, sollten die entsprechenden Vorschriften mit entsprechenden technologischen Mitteln umgesetzt werden. Die Wirksamkeit des Rechts auf Anonymität muss durch die Technologie sichergestellt werden, die Lösungen für verschiedene Anonymitätsstufen bereitstellen muss.

Die Forderung, eine Folgenabschätzung für den Datenschutz durchzuführen, sollte rechtlich verankert werden.

Für die Fälle, in denen eine Folgenabschätzung ergibt, dass mit der Verarbeitung der Daten erhebliche Datenschutzrisiken verbunden sind, könnte der

Gesetzgeber die Implementierung geeigneter Sicherheitseinrichtungen vorschreiben, um diese Risiken abzufedern.

Aufgaben im Kommunikationsbereich

Durch zunehmende Sensibilisierung werden die Gefahren der Online-Welt für EU-Bürger verringert.

Informationskampagnen, die zu einem besseren Technologieverständnis beitragen, das den Nutzer stärkt und ihn davon überzeugt, dass er seine Daten schützen muss, bewirken einen besseren Umgang der Nutzer mit den IKT und tragen so dazu bei, die Gefahren für EU-Bürger in der Online-Welt zu verringern.

Durch den systematischen Einsatz harmonisierter Methoden und Prozesse für die datenschutzrechtliche Folgenabschätzung trägt die Industrie zu mehr Transparenz und zur Verringerung der Risiken in Bezug auf die Daten, die sie verarbeitet, bei und profitiert letztlich vom gestiegenen Vertrauen der Nutzer in die Technologie.

Außerdem wird durch Kampagnen dieser Art die Nachfrage nach datenschutzfreundlichen Technologien, die verständlich und effizient sind, angekurbelt.

Links

In der Richtlinie 95/46/EG[22] wird der Begriff der personenbezogenen Daten und der auf sie anwendbare Rechtsrahmen definiert.

Der Begriff der personenbezogenen Daten wurde 2007 in einer Stellungnahme der Artikel-29-Datenschutzgruppe[23] weiter erhellt und eingehend erörtert.

4.11 Schutz der Privatsphäre und Social Sorting

Social Sorting kann die Privatsphäre von Menschen verletzen, auch wenn die verarbeiteten Daten nicht personenbezogen sind.

In vielen Fällen liegt den datenverarbeitenden Stellen nichts an einer Identifizierung Einzelner, d. h. an personenbezogenen Daten, weil sich die Auswertung der Daten auf bestimmte Gruppen der Bevölkerung konzentriert, und eine Art Kategorisierung angestrebt wird, auch Social Sorting, Schichtung, Segmentierung oder Klassifikation genannt. Das geschieht beispielsweise durch Profiling (Profilerstellung) und Scoring (Berechnung der Wahrscheinlichkeit eines bestimmten zukünftigen Verhaltens von Personen) für verschiedene Zwecke wie Marketing, Beurteilung der Kreditwürdigkeit, Preisdiskriminierung, Entscheidungsfindung im e-Recruitment, Gesundheitssektor oder polizeiliche Ermittlungen. In diesen Fällen werden die Daten selbst häufig nicht als personenbezogen betrachtet, weil sie nicht mit bestimmten Personen in Verbindung gebracht werden, d. h. die für die Datenverarbeitung verantwortlichen Stellen kennen die Namen der Personen, deren Daten

[22] http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.
[23] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf.

verarbeitet werden, nicht. Doch die Folgen dieser Datenerhebungen und -analysen wirken sich häufig auf einzelne Personen aus und verletzen so ihre Privatsphäre. Diese Konstellation wird durch Artikel 15 der EU-Datenschutzrichtlinie über automatisierte Einzelentscheidungen nicht abgedeckt.

Konkrete Sicherheitslücken

Social Sorting für den Einzelnen nicht transparent

Die Hauptlücke besteht darin, dass die einzelnen Personen nicht bemerken, wenn ihre Daten für Social Sorting verwendet werden, und wie bestimmte, sie betreffende Entscheidungen zustande kommen. Das bedeutet, sie wissen weder, ob die Daten, die für die Kategorisierung herangezogen werden, richtig, noch ob die Algorithmen, Scoring-Anwendungen und andere Analysewerkzeuge zuverlässig sind. Insbesondere kann die Stelle, die Entscheidungen über Einzelpersonen trifft, eine andere sein, als die Stelle, welche die Informationen sammelt und kombiniert, was es dem Einzelnen erschwert, sich erfolgreich zu wehren. Außerdem ist es bei Szenarien, bei denen es um Wahrscheinlichkeitsannahmen geht, normalerweise nicht möglich zu beweisen, dass die Voraussagen falsch sind.

Das individuelle Recht auf Schutz der Privatsphäre greift nicht bei nicht personenbezogenen Daten

Solange die verarbeiteten Daten als nicht personenbezogene Daten betrachtet werden, schwächt das die Ausübung des Rechts auf Schutz der Privatsphäre (Recht auf Auskunft, Berichtigung, Löschung von personenbezogenen Daten, wenn diese auf nicht legale Weise gespeichert wurden, Widerruf der Einwilligung). Um Gebrauch von dem Recht machen zu können, müsste nachgewiesen werden, dass die betreffenden Daten einzig und allein zu der betroffenen Person gehören. Es gibt beispielsweise Fälle, in denen die Dateneinsicht verweigert wurde, wenn es um Cookie-Daten ging, nur weil Cookies Daten enthalten, die nicht unbedingt allein an eine Person gebunden sind. Das macht deutlich, dass viele Kennungen Daten enthalten, die von ausreichender Qualität sind, um zu den intendierten aussagekräftigen Informationen verarbeitet zu werden, wobei aber die Daten für sich genommen nicht geschützt sind und somit der Einzelne nicht von seinem Recht auf Schutz der Privatsphäre Gebrauch machen kann.

Erreichbarkeit kann direkte Manipulation erleichtern

Außerdem gibt es Einstellungen, mit denen Personen ausfindig gemacht und erreicht werden können, z. B. per Telefon, E-Mail oder personalisierte Werbung über Fernsehen oder Website. Insbesondere die Arten von Werbung, die auf potenzielle Käufer abzielen, können manipulativ sein und das Recht des Einzelnen auf Schutz der Privatsphäre verletzen. Außerdem können so Reaktionen provoziert werden, die es der datenverarbeitenden Stelle ermöglichen, die gesammelten Daten zu vervollständigen oder eine Verbindung zu einer Person herzustellen.

Lösungsvorschläge

Das Recht auf informationelle Selbstbestimmung kann nur verwirklicht werden, wenn der Einzelne alles über die Verarbeitung ihn betreffender Daten erfährt.

Aufgaben für Forschung und Entwicklung

Vollständige Prüfpfade für alle Datenverarbeitungsprozesse

Eine mögliche Lösung wäre ein organisatorischer und technischer Rahmen, der gewährleistet, dass die betroffenen Personen ihre Privatsphäre schützen und ihr Datenschutzrecht ausüben können. Dazu könnte es erforderlich sein, dass bei jeder Verarbeitung von personenbezogenen oder nicht personenbezogenen Daten, bei der Individualrechte verletzt werden können, ein vollständiger Prüfpfad angelegt wird. Das würde bedeuten, dass jeder Schritt der Datenverarbeitung mit allen Ein- und Ausgaben einschließlich der Informationen über den für die Datenverarbeitung Verantwortlichen, die Algorithmen und die Anwendungen für die betroffenen Personen oder Dritte ihres Vertrauens nachvollziehbar würden. Dadurch könnten unrichtige Daten oder Schwachstellen in der Datenverarbeitung ermittelt und korrigiert werden.

Der organisatorische und technische Rahmen ist umso notwendiger angesichts unserer sich wandelnden Welt mit ihren vielfältigen Sensoren, die untereinander kommunizieren und Informationen über ihre Umgebung, auch über Personen, sammeln. In dieser Hinsicht wären transparenzfreundliche Technologien eine Hilfe für die betroffenen Personen [Hildebrandt/Koops 2007].

Aufgaben für den Gesetzgeber

Ein in sich konsistenter Rechtsrahmen für jegliche Verarbeitung personenbezogener Daten

Die aktuellen diesbezüglichen Rechtsvorschriften sind offensichtlich auf verschiedene Rechtstexte verteilt, z. B. finden sich einige Regelungen im Datenschutzgesetz, andere in Rechtsvorschriften zum Diskriminierungsverbot und wieder andere erscheinen nicht umfassend genug. Daher ist die wichtigste regulatorische Aufgabe die Entwicklung eines in sich geschlossenen, umfassenden Rechtsrahmens, mit dem alle Arten der Verarbeitung von personenbezogenen und nicht-personenbezogenen Daten, die Folgen für den Einzelnen haben können, abgedeckt sind. Dieser Rechtsrahmen sollte insbesondere eine Verpflichtung zu mehr Transparenz und Verständlichkeit der Datenverarbeitung für die Betroffenen beinhalten.

Aufgaben im Kommunikationsbereich

Den Einzelnen über Datensammlung und -analyse informieren

Einzelne sollten, wenn sie unwissentlich Datenspuren hinterlassen, darüber unterrichtet werden, welche Informationen über sie erhoben und von verschiedenen Stellen kombiniert werden oder wenn sie – womöglich zu Unrecht – in Bezug auf bestimmte Aktionen für verantwortlich gehalten werden. Außerdem sollten sie informiert werden, wie sie am besten reagieren können, wenn sie sich in Bezug auf den Schutz ihrer Privatsphäre unfair behandelt fühlen.

Links

Hildebrandt, Mireille, Serge Gutwirth (Eds.): D7.4: Implications of profiling practices on democracy and rule of law, FIDIS Deliverable, Frankfurt a. M., September 2005, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.4.implication_profiling_practices.pdf.

Hildebrandt, Mireille, Bert-Jaap Koops (Eds.): D7.9: A Vision of Ambient Law, FIDIS Deliverable, Frankfurt a.M., Oktober 2007, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-d7.9_A_Vision_of_Ambient_Law.pdf.

Lessig, Lawrence: Code and other laws of cyberspace, Basic Books, New York, 1999.

Lyon, David: Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination, Routledge, 2002.

Phillips, David J.: Privacy policy and PETs – The influence of policy regimes on the development and social implications of privacy enhancing technologies, in: New Media & Society, Vol. 6, No. 6, SAGE Publications, London, Thousand Oaks, CA and New Delhi, 2004, S. 691-706.

Artikel-29-Datenschutzgruppe: Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, angenommen am 20. Juni 2007, 01248/07/DE, WP 136, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf.

4.12 Privatsphäre, Datenschutz und Raum

In der digitalen Welt fehlen klare Grenzen

Die Unverletzlichkeit des privaten Raums spielt in der realen Welt seit langem eine wichtige Rolle beim Schutz der Privatsphäre („my home is my castle“). Unter einem Territorium versteht man im Allgemeinen einen abgegrenzten räumlichen Bereich; die realen und digitalen Elemente, die zu einer Person gehören, können jedoch an verschiedenen Orten koexistieren (letzten Endes wird jedes digitale Element auf einer Festplatte oder einem anderen Medium gespeichert, das eine spezifische körperliche Beschaffenheit und ein bestimmtes Ortsmerkmal aufweist, wobei sich letzteres mit der Zeit verändern kann, z. B. bei mobilen Geräten). Das Fehlen klarer räumlicher Grenzen in der digitalen Welt führt zu spezifischen rechtlichen Problemen und allgemeinen Problemen der Wahrnehmung wenn es um die Privatsphäre geht.

Konkrete Sicherheitslücken

Warum die personenbezogenen Daten in der europäischen Rechtssprechung verbleiben müssen

Gemäß Artikel 25 der Datenschutzrichtlinie 95/46/EG werden personenbezogene Daten in der Regel nur an Drittländer übertragen, wenn in dem betreffenden Land ein ausreichendes Datenschutzniveau sichergestellt ist. Es gibt Ausnahmen von dieser Regel, wie beispielsweise den Datentransfer an Unternehmen in den Vereinigten Staaten, die sich verpflichtet haben, die Grundsätze der Safe-Harbor-Datenschutzvereinbarung zu beachten.

In allen Fällen außereuropäischer Rechtsprechung wird im Rahmen des festgelegten Datenschutzniveaus jedoch nicht die Möglichkeit des Zugriffs nationaler Sicherheitsbehörden berücksichtigt. Das bedeutet, dass alle Daten in

diesen Ländern dem Zugriff und der Analyse dieser Stellen ausgesetzt sein können, was unerwünschte Folgen für die betroffene Person aber auch für Unternehmen haben kann, deren Handelsgeheimnisse offen gelegt werden könnten.

Real versus digital

In der Informationsgesellschaft fehlt die Territorialität, und deswegen gibt es keine schützenden Grenzen. Gleichzeitig werden immer mehr unsichtbare und unkontrollierte Verbindungen zwischen realen und digitalen Umgebungen hergestellt. Während wir in der realen Welt die Mittel haben, unsere Privatsphäre (durch Distanz) zu wahren, ist das in der digitalen Welt noch nicht der Fall. Durch die zunehmenden Verbindungen zwischen beiden Welten wird diese neue Umgebung jedoch zu einem festen Bestandteil unseres Alltags und des Raums, in dem wir uns bewegen.

Gesetzliche Regelungen, stillschweigende soziokulturelle Normen und Gepflogenheiten dienen den Menschen als Orientierung für ihre Auffassung von privatem bzw. öffentlichem Raum oder für das, was gesellschaftlich als privater oder öffentlicher Raum akzeptiert wird. Obwohl die Unterscheidung zwischen den beiden Räumen nicht immer ganz klar ist, sind sich die Menschen bewusst, dass Grenzen bestehen und verhalten sich entsprechend (z. B. eingezäuntes Privatgrundstück, „Betreten verboten“-Schild auf einem privaten Rasengelände, fragender oder leicht irritierter Blick, wenn Fremde die Kneipe „um die Ecke“ betreten).

Wahrnehmung von Raum im Cyberspace

Im realen Raum haben die Menschen ein intuitives Gespür für Verletzungen der Privatsphäre, im Cyberspace fehlt ihnen eine entsprechende Wahrnehmung. Zum Beispiel ist selbst in öffentlichen Räumen für alle klar, dass jemand, der andere belauscht, dessen Privatsphäre verletzt. Im Cyberspace ist sowohl unklar, ob jemand andere belauscht, als auch, ob es sich dabei um eine Verletzung der Privatsphäre handelt. Wie können diese Grenzen im Cyberspace deutlicher werden?

Fernspeicherung verkompliziert den Begriff der räumlichen Grenzen im Cyberspace

In diesem Kontext und ohne die ohnehin schon komplizierte Beschaffenheit der Privatsphäre im realen Raum sowie die Schwierigkeiten ihres angemessenen Schutzes zu unterschätzen, erscheint die Privatsphäre in der digitalen Welt als leichter verletzlich und ungleich schwieriger zu schützen. In der digitalen Welt lassen sich unerwünschte Berührungen nicht einfach abschütteln. Dazu kommt, dass im Cyberspace die Missachtung der Privatsphäre eher an der Tagesordnung ist und somit immer ein angemessenes Handeln (angemessene Reaktion) des Nutzers erfordern. Denken Sie nur an das automatische Abonnement des Newsletters oder anderer Dienste, die ohne Ihr Zutun bei der Installation eines Programms oder der Anmeldung bei einem Online-Internetdienst abgeschlossen werden: Sie werden dann lediglich im Nachhinein darüber informiert, auf welcher Website Sie den Newsletter oder Dienst wieder abbestellen können. Oder denken Sie an das Fotoalbum im Wohnzimmerschrank, das eigentlich Mitgliedern des Haushalts vorbehalten ist, vielleicht noch Freunden und

Verwandten gezeigt wird; ein digitales Fotoalbum, das im Internet verfügbar und sogar suchbar ist, ist in der Regel nicht vergleichbar geschützt[24].

Das Opt-out ist also meistens viel schwieriger und erfordert eine besondere Anstrengung des Nutzers sowie bestimmte technische Kenntnisse. Was die Sache noch schlimmer macht ist, dass der Nutzer sich häufig nicht der Menge und der Art der Informationen (z. B. IP-Adresse, Cookies, Web-tracking, Cache, Suchbegriffe usw.) bewusst ist, die erfasst werden, während er im Netz surft oder andere Online-Tätigkeiten ausführt, und es so für ihn schwieriger wird, seine Zustimmung zu verweigern oder seine Daten zu schützen.

Virtuelle Welten

So genannte virtuelle Welten stellen einen weiteren Bereich dar, in dem es diesbezüglich an Transparenz und Eindeutigkeit mangelt. Manche sagen voraus, dass virtuelle Welten bald von Mainstream-Unternehmen eingesetzt werden. Anwendungen wie Kaneva tauchen auf, bei denen Social Networks mit virtuellen Welten verschmelzen. In diesem Bereich gibt es viele unerforschte Datenschutzfragen. Wie sind beispielsweise virtuelle Finanzdaten (z. B. Linden-Dollar-Konten) rechtlich einzuordnen? Eine andere interessante Frage wäre, was es bedeuten könnte, einen Personalausweis für einen Avatar auszustellen – der Punkt ist, dass sogar rein virtuelle Personen von einer strengen Authentifizierung und Verknüpfbarkeitskontrolle profitieren könnten. Ein Avatar als Verkörperung einer digitalen Teilidentität wäre außerdem ein nützliches datenschutzfreundliches Nutzerinterface.

Lösungsvorschläge

Aufgaben für Forschung und Entwicklung

Datenspeicherung und Infrastruktur in der EU-Rechtsprechung

Um die Daten europäischer Bürger zu schützen, sollten Mechanismen eingeführt werden, die die Daten so weit wie möglich im Bereich der europäischen Rechtsprechung halten. Bei Internet-Suchmaschinen könnte dies durch Proxies für Fremdleistungen oder als eigene Suchmaschinen erreicht werden.

Ähnlich kritische Infrastrukturen sollten nur im Bereich der europäischen Rechtsprechung errichtet, Abhängigkeiten von anderen Ländern vermieden werden.

[24] Ein anschauliches Beispiel sind die nicht gut konfigurierten sogenannten Online Social Networks wie z. B. mySpace.com, Flickr, YouTube oder Facebook, in denen man Fotos und Videos online speichern, zugänglich und vor allem suchbar machen kann.

Aufgaben für den Gesetzgeber

Der Umgang mit den Daten innerhalb europäischer Dienste müsste dem europäischen Datenschutzrecht unterstellt werden, wodurch eine unnötige Speicherung und Nutzung von Daten vermieden würden.

Begriff des digitalen Territoriums

Durch die Digitalisierung des privaten Bereichs und seiner Grenzen bietet der Begriff des digitalen Territoriums (Digital Territory) die Möglichkeit, die Begriffe Territorium, Eigentum und Raum in digitalen Umgebungen einzuführen. Das Ziel besteht dabei darin, ein Instrument zu entwickeln, mit dem der Nutzer Nähe und Distanz im digitalen Raum – im legalen und im sozialen Sinne – nach dem Vorbild des Schutzes seiner Privatsphäre in der realen Welt wahren kann.

Der reale und traditionelle Begriff der Wohnung begründet ein unveräußerliches Grundrecht, das den Bürger vor Eingriffen oder Eindringen von außen schützt[25]. Dieses Grundrecht gilt es nun auf den digitalen Teil unseres Privatbereichs auszudehnen.

Aufgaben im Kommunikationsbereich

Es müssen kommunikative Instrumente entwickelt werden, um darüber zu informieren, welche Elemente diesem privaten Bereich angehören.

Links

Beslay, Laurent, Hannu Hakala: Digital Territory: Bubbles. In: Paul T. Kidd (Ed.): European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society, Cheshire Henbury, 2007, S. 69-78.

Benoliel, Daniel: Law, Geography, and Cyberspace: The Case of online Territorial Privacy, CFP 2004.[26]

Daskala, Barbara, Ioannis Maghiros: Digital Territories, Towards the protection of public and private space in a digital and Ambient Intelligence environment.[27]

[25] Siehe Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union.
[26] http://www.cfp2004.org/spapers/benoliel-caseOfTerritorialPrivacy.pdf.
[27] http://ftp.jrc.es/eur22765en.pdf.