

1. Vorwort

Die Bremische Bürgerschaft hat mich am 29. April 2009 zur Landesbeauftragten für Datenschutz und Informationsfreiheit gewählt. Daher ist dies der erste Jahresbericht zum Datenschutz, den ich der Bremischen Bürgerschaft und dem Präsidenten des Senats der Freien Hansestadt Bremen vorlege. Diese Gelegenheit möchte ich nutzen, meinem Vorgänger Sven Holst, der dieses Amt in den ersten Monaten des Berichtszeitraumes ausfüllte, dafür zu danken, dass ich meine Arbeit in einer Dienststelle mit hoch motivierten Mitarbeiterinnen und Mitarbeitern aufnehmen konnte. Der gute Datenschutzzuf, den Bremen bundesweit genießt, begünstigte auch meinen Start im Kreis meiner Kollegin und meiner Kollegen aus dem Bund und den anderen Ländern.

Datenschutz als Menschenrechtsthermometer

Die Menschenrechte sind kein Luxus, sondern die Basis unseres demokratischen Gemeinwesens. Dies gilt gerade in Zeiten, in denen eine wirtschaftlich schwierige Lage dazu verleitet, das gesellschaftliche Augenmerk allein auf die Überwindung dieser Situation zu lenken, und in denen deshalb das Aufrechterhalten errungener Standards in allen Bereichen schwierig wird. Dabei ist die Einhaltung dieser Standards gerade dann wichtig: Nur selbstbewusste Menschen, die sich wertgeschätzt fühlen und die ihre demokratischen Rechte kennen und nutzen, können die Kreativität und Tatkraft entfalten, die Wirtschaft und Gesellschaft benötigen, um Krisen zu bewältigen.

Zu diesen wichtigen Menschenrechten gehört auch das Grundrecht auf informationelle Selbstbestimmung. Es fußt auf der unabdingbaren Menschenwürde und dem Grundrecht auf freie Entfaltung der Persönlichkeit und drückt den Anspruch aller Menschen darauf aus, dass öffentliche und private Stellen in würdevoller und respektvoller Weise mit Informationen über sie umgehen. Nur die Betroffenen selbst sollen darüber entscheiden dürfen, wer ihre Daten erhält und wer nicht. Angesichts der besonderen Gefahren für das Persönlichkeitsrecht, die aus der rasanten technischen Entwicklung folgen, hat das Bundesverfassungsgericht in seinem Urteil zur Rechtswidrigkeit der Onlineüberwachung zusätzlich das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt. Diese beiden Datenschutzgrundrechte gehören zum Menschenrechtsbollwerk in Zeiten der Wirtschaftskrise. Die Aufgabe, gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern mit dafür zu sorgen, dass diesen Menschenrechten in Bremen und Bremerhaven ein großes Gewicht beigemessen wird, empfinde ich als große Ehre.

Der Grad der Beachtung, den der Datenschutz als Ausformung des Menschenrechts auf informationelle Selbstbestimmung im Staat, in der Wirtschaft und in der Gesellschaft erfährt, ist Ausdruck der Beachtung der Menschenrechte allgemein. Angesichts der öffentlichen Diskussionen über die in den letzten Jahren laufend aufgedeckten Fälle der Missachtung dieser Rechte hat sich unser aller Bewusstsein über unsere Rechte im Zusammenhang mit dem Datenschutz schon deutlich geschärft. Aber wir müssen uns alle immer wieder neu darüber klar werden, wo die Grundrechte gefährdet und deshalb schutzbedürftig sind.

So ist das Bedürfnis, bestimmte Dinge nicht zu offenbaren, das ureigene Recht der Menschen, dessen Bedeutung wir alle selbst kennen. Das verkennt der neuerdings oft geäußerte Satz „Wer nichts zu verbergen hat, hat nichts zu befürchten.“ Im Gegenteil darf daraus, dass jemand dieses Recht auf das Verschweigen in Anspruch nimmt, nicht gefolgert werden, dass dieser Mensch etwas Unrechtes verbergen will. Völlig zu Recht steht deshalb beispielsweise auf den „gelben Zetteln“, die

Ärztinnen und Ärzte ausfüllen, um zu bestätigen, dass Menschen krankheitsbedingt nicht arbeiten können, ganz bewusst nicht die Diagnose. Zu wissen, dass und für wie lange die Menschen arbeitsunfähig sind, muss der Chefin oder dem Chef reichen. Um welche Krankheit es sich handelt, geht erst einmal niemanden etwas an.

Datenschutz als Eindeichung der Menschenrechte gegen die Flut der Informationsbegehrlichkeiten

Wir leben im Informationszeitalter, in dem Menschen mit Informationen überflutet werden. Der Dienstsitz der Bremischen Landesbeauftragten für Datenschutz und Informationsfreiheit liegt in Bremerhaven, nicht weit hinter dem Seedeich. Angesichts des Klimawandels werden den Bremerhavener Deichen in den nächsten Jahren viele Höhenzentimeter hinzugefügt. Auch die Deiche gegen die Flut der Informationsbegehrlichkeiten müssen dringend erhöht werden. Die Schlüsselqualifikation in der Informations-, oder besser Wissensgesellschaft, die Fähigkeit, erkennen zu können, welche Informationen relevant sind und welche nicht, ist noch unterentwickelt. Als Beispiel hierfür kann die Kritik des US-amerikanischen Präsidenten Obama im Zusammenhang mit dem Anschlagversuch zum Ende des Berichtsjahres dienen. Es hat sich herausgestellt, dass US-Behörden vom Vater des Betroffenen über dessen Attentatspläne informiert worden waren, dass diese Informationen aber nicht genutzt wurden, weil die entsprechenden Dateien riesige Mengen von Informationen aufwiesen und es an einer sinnvollen Auswertung fehlte. Der in Vorratsdatenspeicherungen zum Ausdruck kommenden Sammelwut staatlicher Institutionen ist ein „weniger ist mehr“ entgegenzuhalten.

Angesichts der Sicherheitspanne im Januar 2010 auf dem Münchener Flughafen, bei der mutmaßlich schlecht bezahltes privates Sicherheitspersonal einen – wie sich herausstellte – fälschlich Verdächtigten nicht verfolgte, wurde die Forderung laut, es sei wichtiger, in die Menschen und ihre arbeitsplatzbezogene Ausbildung zu investieren, als in immer neue Techniken, die wieder neue Datenfluten produzieren. Dieses Resümee „Kontrolle statt Scanner“ (Frankfurter Rundschau vom 22. Januar 2010) sollten wir im Kopf behalten, wenn es demnächst um den Einsatz der sogenannten Körperscanner zur Flugsicherung geht. Wissensmanagement, die Fähigkeit, kompetent, effizient, verantwortungsbewusst und respektvoll mit Informationen über Menschen umzugehen, ist das Gebot der Stunde.

Generalverdacht ersetzt die Unschuldsvermutung

Das Bundesverfassungsgericht hat im Berichtsjahr über eine anlasslose sechsmonatige Speicherung aller Telekommunikationsverbindungsdaten (Wer telefoniert oder mailt mit wem zu welcher Zeit und wie lange und bei Mobiltelefonen auch noch von welchem Ort aus?) verhandelt. Dieses Beispiel für Vorratsdatenspeicherung zeigt, dass die im Anschluss an den 11. September 2001 verabschiedeten Antiterrorgesetze die Logik der rechtsstaatlichen Unschuldsvermutung umkehren. Alle Menschen müssen es sich gefallen lassen, ohne einen konkreten Anlass dafür geliefert zu haben, Maßnahmen ausgesetzt zu werden, die zuvor nur gegen Verdächtige möglich waren. Erst einmal stehen alle unter potenziellem Verdacht. Erst weitere Kontroll- oder Überwachungsmaßnahmen können ihre Entlastung ergeben. Die Grenzen zwischen Unschuldigen und Schuldigen, zwischen Unverdächtigen und Verdächtigen werden fließend. Diese Veränderung wird von vielen als Wandlung des Rechtsstaates in einen Präventionsstaat wahrgenommen, in dem alle Bürgerinnen und Bürger nicht mehr als unverdächtig, sondern als potenziell verdächtig, als „noch“ nicht verdächtig betrachtet werden

(Heribert Prantl). Die Freiheitsräume werden in einem solchen Staat immer kleiner. Hier ist zu hoffen, dass das Bundesverfassungsgericht in seinem für das Frühjahr 2010 angekündigten Urteil den beschriebenen Tendenzen Einhalt gebietet.

Mangelnde Eignung zur Erreichung des verfolgten Zwecks

Manchmal ist das Datensammeln zudem völlig ungeeignet zur Erreichung des verfolgten Zwecks. Großes Aufsehen erregte im Berichtsjahr die Diskussion über das SWIFT-Abkommen, das die EU mit den USA abschließen wollen. Dieses Abkommen soll es ermöglichen, Bankdaten europäischer Bürgerinnen und Bürger an die USA weiterzugeben (vergleiche Ziffer 14.4 dieses Berichts). Dazu berichtete die Presse Anfang des Jahres 2010, dass das Bundeskriminalamt das von allen Datenschutzbeauftragten stark kritisierte Abkommen „für nutzlos beim Vorgehen gegen den internationalen Terrorismus“ hält. Die aus fachlicher Sicht zu erwartenden Erkenntnisse rechtfertigen nicht den mit der Datenrecherche verbundenen erheblichen materiellen und personellen Aufwand. In diesem Zusammenhang ist wichtig, dass Maßnahmen rechtswidrig sind, die zur Erreichung eines vom Gesetzgeber festgelegten Zieles ungeeignet sind.

Datenschutz als Instrument der Qualitätssicherung

Datenschutz, der Schutz des Grundrechts auf informationelle Selbstbestimmung, kostet nicht unbedingt Geld, aber immer Gehirnschmalz. Die These aller Datenschützerinnen und Datenschützer ist, dass es in der Verwaltung wie in der Wirtschaft immer qualitätssteigernd wirkt, sich Gedanken darüber zu machen, wer wann welche Information benötigt und wie er oder sie diese rechtmäßig und mit dem geringsten Eingriff in Persönlichkeitsrechte erlangen kann. Gerade das Herausfinden, welche Informationen wann relevant sind, ist ein zugegebenermaßen aufwändiger Schritt, der in vielen Prozessen fehlt und sie zu lang und – das spielt in Bremen ja eine besonders wichtige Rolle – zu teuer macht. Auf diese Weise kann auch zu einem frühen Zeitpunkt identifiziert werden, welche Informationen zwar vielleicht wünschenswert wären, aber nicht auf gesetzlichem Wege erlangt werden können.

Für solche Qualitätssicherungsmaßnahmen im Zusammenhang mit der Modellierung von Arbeitsprozessen und auch für andere Aktionen zur Messung der Datenschutztemperatur bieten wir als auf diesem Gebiet Spezialisierte hiermit noch einmal ausdrücklich unsere Hilfe an, weil wir wie alle Menschen lieber im Vorfeld mitgestalten, als nachher zu kritisieren. Wie dieser Bericht bezeugt, haben wir im letzten Jahr in Verwaltung und Wirtschaft in der überwiegenden Zahl der Fälle erlebt, dass der Austausch über datenschutzrechtliche Fragen dazu geführt hat, dass Datenschutzverstöße verhindert, abgestellt oder zumindest gemildert wurden.

„Stopp der Jugendgewalt“

Am Tag vor meiner Wahl berichtete der „Weser-Kurier“, dass im Projekt „Stopp der Jugendgewalt“ das Thema Datenschutz „offenbar zu kurz gekommen“ sei. Das hat sich mittlerweile in den meisten der vielen Einzelprojekte geändert (vergleiche Ziffer 7.2 und Ziffer 5.2 dieses Berichts).

Die größte datenschutzrechtliche Herausforderung in dem Projekt ist der erklärte Wille, Informationen gleichzeitig an mehrere Stellen mit unterschiedlichen Aufgaben weiterzugeben. In solchen Konstellationen muss gewährleistet sein, dass nicht nach dem Motto „Jeder sagt allen alles, für irgendetwas wird es schon gut sein ...“ ein der Vorratsdatenspeicherung strukturell gleichgelagerter Fall entsteht. So lange es zwei Akteure gibt, ist die Beurteilung einfach: Anknüpfungspunkt ist die

Frage, wer welche Informationen zu welchem Zweck braucht. Handelt es sich um einen legitimen gesetzlichen Zweck und ist die Informationsweitergabe der einen an die andere Stelle gesetzlich vorgesehen und geeignet, den Zweck zu erreichen, so muss gefragt werden, ob es im Vergleich zur Informationsweitergabe nicht andere, ebenso geeignete Mittel gibt. Ist das nicht der Fall und steht die Informationsweitergabe auch nicht außer Verhältnis zu dem gesetzlichen Ziel, so ist sie rechtmäßig.

Komplizierter wird es dann, wenn eine Information – wie beispielsweise bei den geplanten Fallkonferenzen – durch eine Handlung (nämlich die Äußerung in einer Gruppe) gleich an mehrere Institutionen weitergegeben wird. Dann muss jede dieser Informationsweitergaben rechtmäßig sein. In den Fällen, in denen beispielsweise gesetzlich erlaubt oder sogar gefordert wird, dass eine Information vom Amt für Soziale Dienste an die Polizei gelangt, eine gesetzliche Übermittlungserlaubnis an die ebenfalls in der Konferenz sitzende Schule aber nicht existiert, wird es für diese zweite Informationsübermittlung schwierig. Hier fehlt es unter Umständen schon an der Eignung der Informationsübermittlung zur Erfüllung des gesetzlichen Ziels, das die Stelle verfolgt, die die Information nur deshalb mithört, weil sie mit am Tisch sitzt.

Als datenschutzrechtliche Lösung für die Fallkonferenzen diskutierten wir mit dem Senat über das Ob und das Wie von Einwilligungen der Betroffenen in Datenweitergaben.

Privatisierungstendenzen im Zusammenhang mit der öffentlichen Sicherheit

In der durch Medienberichte bestärkten öffentlichen Wahrnehmung ist die öffentliche Sicherheit zunehmend gefährdet. In einer Situation, in der die öffentliche Hand auch im Bereich der Polizei Personal tendenziell abbaut, öffnet sich damit eine Schere zwischen den ansteigenden Aufgaben und den tatsächlich zur Erfüllung dieser Aufgaben zur Verfügung stehenden Beschäftigten. Auf diese Situation wird zum Teil mit der Einbeziehung Privater in die Aufgabenerfüllung reagiert. Die Einbeziehung Privater findet ihre Grenze dort, wo der Bereich der Prävention, also der Verhinderung von Straftaten, verlassen wird und es um die Strafverfolgung bereits begangener Taten geht. Die Aufgaben der Strafverfolgung sind den hoheitlich tätigen und hierfür ausgebildeten Polizistinnen und Polizisten beziehungsweise der Staatsanwaltschaft vorbehalten.

Im Berichtsjahr gab es auch in Bremen Bestrebungen zur Privatisierung der Aufgabe der öffentlichen Sicherheit. Zwischen dem Senator für Inneres und Sport und dem Bundesverband Deutscher Wach- und Sicherheitsunternehmen e. V. (BDWS) wurde die „Vereinbarung zur Verbesserung der Sicherheit in Bremen“ abgeschlossen. Danach sollte eine neu einzurichtende gemeinsame Informations- und Ansprechstelle der Mitglieder des BDWS der Polizei bedeutsame Informationen für „die Kriminalprävention, die Kriminalrepression und die Gefahrenabwehr“ mitteilen. Die Polizei sollte ein „gemeinsames Sicherheitslagebild“ erstellen und dies an die Sicherheitsunternehmen übermitteln. Der Senator für Inneres und Sport hat die Polizei gebeten, die beabsichtigte Kooperation „in dieser Form“ nicht weiter zu betreiben, woraufhin die Vereinbarung einvernehmlich wieder aufgehoben wurde.

Aus unserer Sicht gehört auch der Einsatz von Sprühanlagen mit „künstlicher DNA“ in diesen Zusammenhang (vergleiche Ziffer 5.1 dieses Berichts). Gegen den Diebstahlschutz durch die Markierung von Gegenständen mit der lackartigen Flüssigkeit haben wir keine grundsätzlichen Bedenken. In der Besprühung von Menschen mit „künstlicher DNA“ durch eine kurz zuvor von Privaten aktivierte Lichtschranke – und damit in der Markierung dieser Menschen als einer Straftat Verdächtige – sehen wir dagegen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung, für den sich Private auf keine Rechtsgrundlage berufen können und der daher für

Private nicht zu rechtfertigen ist. Da diese Markierung die spätere Strafverfolgung erleichtern soll, handelt es sich nach unserer Auffassung bei der Besprühung um eine Maßnahme der Strafverfolgung. Zur Strafverfolgung sind die hierfür ausgebildeten Polizistinnen und Polizisten zuständig. Für eine Markierung von Menschen durch Private zur Erleichterung der Strafverfolgung gibt es unseres Erachtens gegenwärtig keine Rechtsgrundlage. Unserer Auffassung nach ist der Grund hierfür unter anderem die zutreffende Einschätzung des Gesetzgebers, dass Private für Strafverfolgungsmaßnahmen nicht genügend ausgebildet sind. Im Gegensatz dazu erlernen Polizistinnen und Polizisten deeskalierende Techniken und können deshalb angemessen reagieren, wenn beispielsweise ein besprühter Waffenträger aus Wut über die von einem eindeutig identifizierbaren anderen Menschen ausgelöste Besprühung wieder zurückkehrt. In der vom Senat angekündigten polizeilichen Beaufsichtigung des privaten Einsatzes von „DNA-Sprühanlagen“ sehen wir deshalb einen Fortschritt für den Schutz des Grundrechts auf informationelle Selbstbestimmung. Gleichwohl vertreten wir die Auffassung, dass sich auch die so gestaltete Einbeziehung Privater nicht auf eine gesetzliche Grundlage berufen kann.

Unterschiede bei der Kontrolltätigkeit über die Verwaltung und über Private

Datenschutzrechtliche Regelungen wirken in der Verwaltung in folgender Weise: Aus dem Rechtsstaatsgebot folgt das Prinzip der Gesetzmäßigkeit der Verwaltung. Im öffentlichen Bereich gehört das Datenschutzrecht zu den Rechtsnormen, die die Verwaltung zu beachten hat. Wenn die Landesbeauftragte für Datenschutz und Informationsfreiheit und die Verwaltung gleichermaßen zu dem Ergebnis kommen, dass Verwaltungshandeln das Datenschutzrecht verletzt, wird dies abgestellt. Komplizierter wird es, wenn – wie dies gelegentlich der Fall ist – die Meinungen darüber auseinandergehen, ob ein Verwaltungshandeln wegen Verstoßes gegen datenschutzrechtliche Regelungen als rechtswidrig anzusehen ist oder nicht. Dann geht es um juristische Fragen, die ja bekanntermaßen von verschiedenen Juristinnen und Juristen unterschiedlich beantwortet werden können. Die Landesbeauftragte für Datenschutz und Informationsfreiheit vertritt dabei ihrem gesetzlichen Auftrag entsprechend im Zweifel die Auffassung, bei der das Grundrecht auf informationelle Selbstbestimmung am stärksten geschützt wird. Dass die Verwaltung das Grundrecht auf informationelle Selbstbestimmung besonders im Fokus hat, ist wichtig, weil sie eine Vorbildfunktion für die Wirtschaft hat, in der sich die Datenmissbrauchsskandale der letzten Jahre ja vor allem zugetragen haben.

Die Wirkungsweise von datenschutzrechtlichen Regelungen in der Wirtschaft ist eine andere. Dort gibt es zunehmend „Compliance“ – Abteilungen, Regelungsüberwachungsabteilungen, die für das regelkonforme Verhalten eines Unternehmens im Hinblick auf alle gesetzlichen Ge- und Verbote sorgen sollen. Ziel der Compliance ist die Vermeidung von Kosten, insbesondere durch Schäden, Strafzahlungen, notwendige Maßnahmen oder Imageschäden. Der erste Arbeitsschritt ist deshalb die Identifikation und Analyse des „rechtlichen Risikos“. Hier ist es für die Durchsetzung datenschutzrechtlicher Standards ungünstig, wenn das Risiko, „erwischt“ zu werden, relativ gering ist, weil der Landesbeauftragten für Datenschutz und Informationsfreiheit aufgrund der Ressourcenknappheit zu wenige anlassunabhängige Kontrollen möglich sind. Ebenfalls ungünstig für die Durchsetzung datenschutzrechtlicher Standards ist es, wenn die durch Regelverletzungen entstehenden Kosten für die betreffenden Privaten nicht ins Gewicht fallen. Die im Zuge der Novellierung des Bundesdatenschutzgesetzes (vergleiche Ziffer 13.1 dieses Berichts) erfolgte Erhöhung des Bußgeldrahmens auf 300.000 Euro war hier ein Schritt in die richtige Richtung.

Für den Bereich der Datenschutzkontrolle über den öffentlichen Bereich sieht das Bremische Datenschutzgesetz eine Stellungnahme des Senats zum Jahresbericht der Landesbeauftragten für den Datenschutz vor, die im Parlament gemeinsam mit dem Jahresbericht beraten wird. Leider gibt es im Bundesdatenschutzgesetz keine entsprechende Regelung für eine Stellungnahme der Wirtschaft zu den im Bericht genannten Datenschutzverstößen im nicht öffentlichen Bereich.

Internetsperren

Nach heißer Diskussion wurde im Berichtsjahr das Gesetz über Internetsperren verabschiedet. Das Strafgesetzbuch gilt uneingeschränkt auch für Handlungen im Zusammenhang mit dem Internet. Es ist dort aufgrund der technischen Spezifika jedoch in der Regel schwerer durchzusetzen. Bei der Debatte um die Internetsperren ging es darum, was der Staat im Internet darf. Das Gesetz sah vor, dass die Internetnutzerinnen und Internetnutzer mit einem „Stoppschild“ konfrontiert werden, wenn sie Seiten mit Inhalten öffnen wollen, auf denen Kindesmissbrauch gezeigt wird. Auch die Befürworterinnen und Befürworter der Internetsperren gingen davon aus, dass die Sperren relativ leicht zu umgehen sind und dass das einzig sichere Mittel, den Zugang zu diesen Seiten zu verhindern, die Löschung dieser Internetseiten ist. Daher war der eigentliche Gegenstand der Debatte der, ob der Staat die von allen Seiten nicht infrage gestellte gesellschaftliche Ächtung des Kindesmissbrauchs und des strafbaren Herunterladens der entsprechenden Internetseiten mit Hilfe der Internetsperren lediglich dokumentieren soll, obwohl es ein Mittel, die Löschung, gibt, das die Straftat des Herunterladens der Seiten sogar verhindern kann und, obwohl es ein durch die größte Massenpetition der Bundesrepublik – 135 000 Petentinnen und Petenten – dokumentiertes Misstrauen gegen den Staat gibt, dass er das einmal vorhandene Werkzeug der Internetsperren auch für die Sperrung von anderen Internetinhalten benutzt. Die Koalitionsvereinbarung auf Bundesebene sieht nun vor, dass das Gesetz ein Jahr lang nicht zur Anwendung kommt und stattdessen die Löschungsmöglichkeiten von Internetseiten mit rechtswidrigen Inhalten effektiviert werden. Die Ergebnisse dieser Bemühungen sollen evaluiert werden, bevor das Gesetz wieder zur Anwendung gelangen soll.

Diese Situation bietet die Möglichkeit, die gesellschaftliche Diskussion darüber zu führen, in welchem Grad Freiheit im Internet gewahrt werden muss und soll und an welchen Stellen – über die bereits bestehenden Regelungen hinaus – Regelungen getroffen werden müssen und sollen.

Datenschutz als Bildungsaufgabe

Die Bremische Bürgerschaft hat im Herbst 2008 in ihren Beschlüssen zum Datenschutz die Schaffung beziehungsweise Stärkung des Datenschutzbewusstseins der Bremerinnen und Bremer angemahnt. Menschenrechtsbildung, zu der auch das Wissen über das Grundrecht auf informationelle Selbstbestimmung und über das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme gehört, muss also auf die Tagesordnung gelangen. Wir, die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, haben dazu in unserer Herbstsitzung in Berlin gefordert, dass der Datenschutz zur Bildungsaufgabe wird (vergleiche Ziffer 16.11 dieses Berichts). Nach unserer Konzeption geht es dabei darum, die informationelle Selbstverantwortung aller Menschen, nicht nur der jungen, zu stärken. Dazu müssen die Grundrechte auf informationelle Selbstbestimmung und auf Vertraulichkeit und Integrität informationstechnischer Systeme zunächst inhaltlich vermittelt werden. Ihre Ableitung aus der Menschenwürde und dem Grundrecht auf freie Entfaltung der Persönlichkeit müssen ebenso wie ihre Bedeutung für die Einzelnen und die Gesellschaft deutlich werden. In einem zweiten Schritt müssen die Menschen von den diesen Rechten

drohenden Gefahren erfahren. Sie müssen über die Gefahren im Internet, aber auch über die in der realen Welt aufgeklärt werden. Es soll allen Menschen bewusst werden, wo sie Datenspuren hinterlassen, wer diese lesen kann und welche Konsequenzen dies für die Einzelnen haben kann. Im dritten und wichtigsten Schritt muss den Menschen vermittelt werden, welche Möglichkeiten sie haben, um diesen Gefahren selbst begegnen zu können. Zum Selbstschutz gibt es viele Vorschläge unter www.datenschutz.de, der Internetseite des Virtuellen Datenschutzbüros, des gemeinsamen Services der Datenschutzinstitutionen des Bundes und der Länder, sowie auf unserer Homepage unter www.datenschutz.bremen.de.

Die Bildungsaufgabe Datenschutz braucht allerdings nicht bei null anzufangen. Angesichts der öffentlich gewordenen Skandale im Umgang mit personenbezogenen Daten ist unser aller Datenschutzbewusstsein bereits angewachsen. Einer Studie zufolge haben sogar mehr Menschen Angst davor, dass ihre Daten missbraucht werden, als dass ihr Eigentum angetastet wird. Es ist wichtig, das Datenschutzbewusstsein weiter zu stärken und neues zu wecken.

Vor allem, soweit es um die Jugendlichen geht, sollte diese Bildungsaufgabe nicht mit dem erhobenen Zeigefinger erfüllt werden. Schon gar nicht sollte Menschen von der Nutzung des Internets abgeraten werden. Das würde der gesellschaftlichen Realität nicht gerecht. Jugendliche und Erwachsene sind in der Lage, auch im Internet selbstbewusste Entscheidungen zu treffen, wenn sie informiert sind und auch sonst gelernt haben, Gelesenes kritisch zu hinterfragen. Und Jugendliche können sich gegenseitig, aber auch uns Erwachsenen beim technischen Selbstschutz meistens sehr viel beibringen.

Die Datenschutzbeauftragten sind nicht die einzigen, die sich mit dem Thema auseinandersetzen. Zur Medienkompetenz ist vom bremischen Rathaus ein runder Tisch angekündigt worden, der die vielen Akteurinnen und Akteure, die allein in Bremen an diesem Thema arbeiten, zusammenbringen will, um gemeinsame Initiativen zu planen und vor allem auch, um bei diesem so drängenden Thema Doppelarbeit zu vermeiden.

Ist Privatheit unmodern geworden?

Was alle dabei unbedingt erfahren müssen, ist, dass auch im Internet gelegentlich ohne ihren Willen über sie entschieden wird: Der Gründer des sozialen Netzwerkes „Facebook“ – und damit jemand, der an den Nutzerdaten gut verdient – ist der Auffassung, die Privatsphäre – und er meint nicht seine eigene, sondern die der Nutzerinnen und Nutzer seines Netzwerkes – sei „nicht mehr zeitgemäß“. Es habe ein entsprechender sozialer Wandel stattgefunden. Übrigens nutzte er diese Äußerung als Begründung dafür, dass die Daten Name, Profilbild, Geschlecht, Wohnort, Freundeliste, alle abonnierten Seiten und so weiter der Nutzerinnen und Nutzer des von ihm kreierte sozialen Netzwerkes in der Grundeinstellung öffentlich sichtbar, und damit recherchierbar sind, und die Nutzerinnen und Nutzer diese Grundeinstellung jetzt aktiv verändern müssen, um ihre Daten nur denjenigen zur Verfügung zu stellen, denen sie sie offenbaren wollen.

Auch ein Zukunftskongress in Oldenburg prognostizierte im Berichtsjahr, dass die Menschen in zehn Jahren keine Wertschätzung mehr für die Privatheit haben würden. Dass die Nutzerinnen und Nutzer eines sozialen Netzwerkes ihre Privatsphäre nicht mehr für schützenswert halten, ist eine unbewiesene Behauptung, und darüber, ob die Menschen in zehn Jahren keine Wertschätzung mehr für ihr Recht auf Privatheit aufbringen werden, müssen sie schon selbst entscheiden! Jedenfalls wird

niemand dieses Recht deshalb aufgeben wollen, weil er anderen die Möglichkeit geben will, an den dadurch gewonnenen Informationen zu verdienen.

Wir alle können an uns bemerken, dass das Gefühl, beobachtet zu werden, das Verhalten verändert. Jedes Verhalten, das wir unter diesem Gefühl an den Tag legen, bezieht sich auf den Umstand der Beobachtung: Wenn ich im bekanntermaßen videoüberwachten, ansonsten menschenleeren Raum bin, unterlasse ich es, in der Nase zu bohren, oder mache es trotzdem oder gerade aufgrund der Überwachung. Alle Handlungsweisen reflektieren jedenfalls die Situation, beobachtet zu sein. Dieses ständige Mit-Bewusstsein, in immer mehr sozialen Räumen nicht ohne potenzielles, aber nicht selbst sichtbares Gegenüber zu sein, sich der Beobachtung immer weniger entziehen zu können, verändert unseren Raum der Freiheit. Das Recht auf Privatheit wird immer mehr zum Luxus. Und das sollten wir nicht ohne eine große gesellschaftliche Debatte geschehen lassen. Und darin können wir dann auch daran erinnern, dass die Moderne einmal mit der Erklärung der Menschen- und Bürgerrechte zusammenhing.

„Cookies löschen?“

Auf der Titelseite dieses Berichts kommt das Krümelmonster in arge Bedrängnis: Kann es wirklich richtig sein, Cookies zu löschen? Was ist denn gegen Kekse einzuwenden? Cookies (Keks heißt auf Englisch Cookie) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer übermittelt, dort gespeichert und für einen späteren Abruf der den Cookie sendenden Stelle bereitgehalten werden. Betreiber von Internetdiensten können aus geeignet gewählten und eingerichteten Cookies ein Nutzungsprofil erstellen, das vielfältige Auskunft über die Nutzerin oder den Nutzer gibt. Eine Manipulation des Computers über Cookies selbst ist nicht möglich. Allerdings können Unberechtigte mit anderen Mitteln auf die Datei auf dem Computer zugreifen, in der die Cookie-Informationen, die auch benutzerbezogene Passwörter für Internetseiten, zum Beispiel von Banken, umfassen können, gespeichert werden. Das Hauptproblem an Cookies ist ihre mangelnde Transparenz: Der Datenaustausch mittels Cookies erfolgt zwischen den beteiligten Computern vollkommen im Hintergrund, ohne dass die Nutzerinnen und Nutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert werden, sofern sie keine besonderen Maßnahmen ergreifen. Diese Parameter sind innerhalb der Cookies selbst festgelegt und werden damit allein vom Betreiber des Internetservers bestimmt. Es hängt von der Initiative der Nutzerinnen und Nutzer ab, ob sie sich vor Cookies schützen können oder diese zumindest bemerken und dann löschen können.

Was können Sie also tun? Sie können Ihren Browser so konfigurieren, dass Cookies nicht oder wenigstens nicht automatisch akzeptiert und Cookies, die gespeichert werden sollen, angezeigt werden. Bereits gespeicherte Cookies können gelöscht werden, zum Beispiel die Datei cookies.txt bei Netscape-Browsern. Außerdem können Sie Cookie-Filter einsetzen. Und wenn Sie das alles geschafft haben, dann können Sie sich in Ruhe genüsslich einen Keks gönnen. Aber bitte nicht so krümeln ...

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und
Informationsfreiheit der Freien Hansestadt Bremen