„Wir sind auf dem richtigen Weg“

Interview mit Tine Larsen, Präsidentin der Datenschutzkommission, über die kommende EU-Datenschutzreform, die Arbeit der Kommission und die Existenz einer Datenschutzkultur in Luxemburg

In Brüssel wird immer noch über die neue Datenschutzverordnung verhandelt. Was ändert sich mit dieser Reform prinzipiell gegenüber der aktuellen Rechtslage, die nicht mehr zeitgemäß erscheint?

Tine Larsen: Die aktuelle Gesetzgebung beruht auf einer Richtlinie von 1995 – als es weder Facebook noch Google gab. Die Entwicklung seitdem war rasant, und unsere Texte sind nicht mehr der Situation angepasst. In Brüssel wird seit 2012 an der neuen Verordnung gearbeitet, und es ist nicht ausgeschlossen, dass es gegenüber der Richtlinie von 1995 auch Rückschritte geben wird. Die Unternehmen drängen auf mehr Flexibilität, denn Daten sind für die Wirtschaft heute ein wichtiges Kapital. Trotzdem ist es bereits jetzt ersichtlich, dass neue Rechte und Pflichten eingeführt werden.

Was bedeutet das für die Bürger?

T. L.: Für die Bürger wird eine der wichtigsten Änderungen ein erweitertes Recht auf Löschung ihrer Daten sein, die ein Unternehmen gespeichert hat. Bisher gibt es dieses Recht nicht *per se.* Jeder kann das Löschen seiner Daten einfordern, aber danach wird abgewogen, ob es sich um Daten handelt, die falsch oder nicht mehr aktuell sind. Bisher besteht jedoch kein grundsätzliches Recht darauf, Informationen löschen zu lassen. Es wird viel darüber diskutiert, ob das Recht auf Vergessenwerden in der neuen Verordnung ausdrücklich gesetzlich geregelt werden soll. In einem rezenten Urteil (Google vs Agencia Española de Protección de Datos) spricht der Gerichtshof der Europäischen Union (EuGH) aber nicht von einem solchen Recht, sondern von einem Recht auf Auslisten von Suchergebnissen. Das Recht auf Vergessenwerden geht weiter als das Recht auf Löschung, da es eigentlich schon von vornherein ein Verfallsdatum für die Datenverarbeitung vorsieht, wogegen das Recht auf Löschung von Fall zu Fall eingefordert werden muss. Die Zustimmung *(consentement)* des Bürgers wird gestärkt, auch wenn die Form der verlangten Zustimmung – explizit oder implizit – noch nicht ganz klar ist. Die Unternehmen werden den Bürger auch besser informieren müssen. Ein weiteres Recht für den Konsumenten, das gestärkt werden soll, bezieht sich auf die sogenannte Datenübertragbarkeit, d. h. wenn Daten zu einem anderen Anbieter mitgenommen werden können, wie man es etwa heute bei den Handynummern kennt. Und schließlich wird es einfacher für den Bürger sein, Beschwerden einzureichen, weil er sich in Zukunft an die Datenschutzbehörde seines Wohnortes wenden kann und nicht mehr wie bisher an jene Behörde, die dort zuständig ist, wo das Unternehmen seinen Sitz hat.

Die aktuelle Gesetzgebung beruht auf einer Richtlinie von 1995 – als es weder Facebook noch Google gab.

Inwieweit wird das die Arbeit der Commission nationale pour la protection des données (CNPD) verändern?

T. L.: Auf die Datenschutzkommission kommen große Veränderungen zu: Wir werden zusätzliche Aufgaben bekommen, aber vor allem andere. In Bezug auf das Beschwerderecht bedeutet dies vor allem, dass die Datenschutzbehörden in der EU sehr viel enger zusammenarbeiten werden, was durchaus eine große Herausforderung sein wird.

Wie sieht die Zusammenarbeit bisher aus?

T. L.: Aktuell besteht eine Zusammenarbeit innerhalb der sogenannten Artikel-29-Datenschutzgruppe, die sich aus Vertretern der Datenschutzbehörden aller Mitgliedstaaten zusammensetzt. In unterschiedlichen Arbeitsgruppen werden dort Stellungnahmen und Empfehlungen ausgearbeitet, die zwar nicht bindend aber richtungsweisend sind. Kürzlich haben wir etwa die Frage behandelt, wie die Kamera einer von einer staatlichen Behörde verwendeten Drohne einzuschätzen sei. Da haben wir auf einen Text der Artikel-29-Gruppe zurückgegriffen. In Zukunft

wird diese Gruppe durch einen European Data Protection Board ersetzt, das mächtiger werden soll.

Wird die CNPD nach der Reform mehr Befugnisse bekommen?

T. L.: Die größte Änderung für uns und die Unternehmen bzw. Institutionen wird sein, dass es kaum noch Genehmigungen oder Benachrichtigungen im Voraus geben wird. Die Unternehmen müssen Verantwortung übernehmen und bei jedem Projekt von Beginn an den Datenschutz mitdenken – man spricht von „privacy by design". Ob die Unternehmen die Regeln korrekt umsetzen, kontrollieren wir dann im Nachhinein. Dann werden wir auch Geldstrafen verhängen können – bisher können wir eine Verwarnung aussprechen, die oft wenig mehr als ein Schmunzeln bei den Unternehmen oder Einrichtungen bewirkt.

Verfügt die CNPD für diese Aufgaben über die nötigen Ressourcen?

T. L.: 87 Prozent der Genehmigungen, die wir ausstellen, betreffen die Überwachung am Arbeitsplatz. Diese Arbeit wird voraussichtlich wegfallen und dadurch werden Ressourcen für Kontrollen frei. Trotzdem sind wir nicht gerade optimal besetzt. Wir haben das auch der Regierung mitgeteilt. Die Stelle für einen zusätzlichen Juristen ist gerade ausgeschrieben. Diese Verstärkung ist allerdings nicht ausreichend.

Inwieweit spielt die Beratung von Unternehmen oder öffentlichen Einrichtungen eine Rolle in ihrer Arbeit?

T. L.: Alle Unternehmen müssen ab einer gewissen Projektgröße eine sogenannte Datenschutzrisikobewertung durchführen. Je nach Situation begleiten wir sie bei dieser Prozedur. Aktuelle Beispiele sind etwa die „intelligenten Stromzähler" und das Projekt „E-santé", wo wir die Datenschutzrisiken bewerten.

Kürzlich wurde der CNPD von dem deutschen Onlineportal heise.de eine zu konziliante Haltung gegenüber der Datensammelwut von Amazon vorgeworfen. Die woxx *kritisierte, die CNPD verstehe sich allzu oft als eine „Service-Einrichtung für Internetriesen". Wie reagieren Sie auf diese Kritik?*

T. L.: Wir sind ein Serviceprovider für alle Betroffenen. Unsere Mission ist es, die Privatsphäre des Bürgers zu schützen, aber wir sind auch gesetzlich dazu verpflichtet Unternehmen zu beraten. Unsere Aufgabe ist es, ein Gleichgewicht zwischen den Rechten und Pflichten auf beiden Seiten herzustellen. Weder im Konkurrenzrecht noch im Verbraucherschutz haben wir Kompetenzen. Im Fall Amazon waren wir der Auffassung, dass es aus Sicht des Datenschutzes legitim ist, dass Amazon die Kaufhistorie seiner Kunden speichert. Ein Recht auf Löschen gibt es, aber nur in Bezug auf falsche oder nicht mehr aktuelle Daten. Insoweit hat heise.de unsere Position verkürzt dargestellt. Und insgesamt empfinde ich die Qualifikation „Serviceeinrichtung" nicht als Kritik, denn in der Dienstleistung besteht ja unsere Rolle.

Wir sind ein Serviceprovider für alle Betroffenen. Unsere Mission ist es, die Privatsphäre des Bürgers zu schützen, aber wir sind auch gesetzlich dazu verpflichtet Unternehmen zu beraten.

Das heißt Kooperation statt Konfrontation …

T. L.: Eine durchdachte Datenschutzstrategie können Unternehmen durchaus als Werbung nutzen. Vor etwa zwei Jahren haben wir zusammen mit anderen europäischen Datenschutzbehörden die Geschäfts- und Nutzungsbedingungen der Cloud-Dienste von Microsoft Online überprüft. Unter dem Vorsitz der CNPD wurden Microsoft anschließend Änderungen vorgeschlagen, die dann auch umgesetzt wurden. Am Ende stand eine Einschätzung der Artikel-29-Gruppe, die Microsoft bestätigte, regelkonform zu sein. Microsoft hat dies dann auch zu Werbezwecken eingesetzt. Andere Firmen sind nachgezogen, so etwa Amazon für seine Cloud-Dienste, die Amazon Web Services. In Reaktion auf Beschwerden von Bürgern setzen wir uns regelmäßig mit den Datenschutzbeauftragten von Ebay, Paypal und Amazon zusammen und besprechen die Probleme.

Gibt es in Luxemburg eine Datenschutzkultur? Fehlen der CNPD Ansprechpartner in der Gesellschaft oder ist eine solche Kultur dabei, sich zu entwickeln?

T. L.: Als wir im Herbst als neue Kommission angetreten sind, war unser Ziel, für alle offen zu sein. Wir hatten unter anderen Treffen mit der Piratenpartei, dem Chaos Computer Club und der Patientenvertretung. Wir haben auf alle Fragen transparent geantwortet. Eine sehr ausgeprägte Datenschutzkultur besteht noch nicht unbedingt, aber es existieren viele unterschiedliche Initiativen. Als Gérard Lommel 2002 die CNPD aufbaute, war das noch etwas völlig Neues. Heute hat die CNPD eine viel größere Sichtbarkeit und wir stehen mit zahlreichen staatlichen und privaten Akteuren im Kontakt. Im Bereich der Sensibilisierung arbeiten wir sehr eng mit SMILE (Security made in Lëtzebuerg) zusammen – auch wenn deren Schwerpunkt mehr im Bereich der Datensicherheit liegt. 2013 entstand die Association pour la protection des données au Luxembourg, deren Mitglieder sich beruflich mit Datenschutz auseinandersetzen. Das Bildungsministerium wird mit der Initiative Digital 4 Education ebenfalls aktiv. Ich denke, wir sind auf dem richtigen Weg.

Oft hat man das Gefühl, Datenschutz ist schwarz oder weiß: Entweder ich verweigere mich einer ganzen Kategorie von Diensten – wie etwa Sozialen Netzwerken oder Fitnessarmbändern – oder ich gebe alle meine Daten preis …

T. L.: Es gibt immer Alternativen. Sie können das begrenzen, was Sie von sich preisgeben. Man muss nicht jedes Mittagessen auf Facebook teilen. Oft tun Menschen Dinge, ohne groß nachzudenken. Dave Eggers beschreibt etwa in seinem Roman *The Circle,* wie Menschen eingetrichtert wird, dass es unsozial sei, seine Erlebnisse und Emotionen nicht zu teilen. Jeder Einzelne muss sich wirklich fragen, wie weit er gehen will.

Bergen die neuen Trends Big Data und Internet der Dinge neue Risiken für den Datenschutz?

T. L.: Es gibt vielfältige Risiken bei Big Data und Internet der Dinge: das Profiling, die permanente Überwachung –

etwa durch einen „smarten“ Fernsehapparat, der weiß, was die Nutzer, wann und wie lange schauen. Die große Gefahr bei Big Data ist, dass Daten aus ganz unterschiedlichen Quellen miteinander verbunden werden und zu einem sehr genauen Profil zusammengesetzt werden können. Aber viele Menschen akzeptieren die Risiken, weil sie dadurch Zugriff auf Dienstleistungen haben, die ihnen das Leben vereinfachen.

Wäre es nicht die Aufgabe der Datenschutzbehörden, die Bürger zu schützen?

T. L.: Ja, unsere Aufgabe ist es auch, den Nutzer vor sich selbst zu schützen. Ein Prinzip des Datenschutzes ist die Zweckgebundenheit der Datenerhebung. Ein zweites Prinzip, die Datenerfassung so weit wie irgend möglich zu minimieren, also z. B. anonymisierte Daten zu verwenden. Dabei bleibt allerdings die Gefahr, dass durch die Masse der Daten eine Re-Identifikation möglich ist. Es geht aber nicht ohne einen verantwortungsvollen Umgang der Bürger mit ihren Daten – sie dürfen nicht zu bequem werden.

Ihr Vorgänger Gérard Lommel sprach oft vom notwendigen Realismus und Pragmatismus im Datenschutz, und doch ist Datenschutz ein Grundrecht, das die Bürger immer öfter einfordern. Wie positioniert man sich heute als Datenschützer in diesem Dilemma?

T. L.: Realismus gefällt mir als Ansatz sehr gut. Pragmatisch sein, heißt nicht, den Unternehmen alles zu erlauben, sondern es bedeutet, die richtige Balance zu finden. Wir müssen eine Balance finden zwischen einer Informationsgesellschaft, die ganz unterschiedliche Dienste hervorgebracht hat, und dem Datenschutz als Grundrecht. Das heißt, dass die Gesetzgebung, die aus dem Jahr 1995 stammt, endlich aktualisiert werden muss. Aber auch die Bürger müssen sich für ihre Rechte einsetzen, es muss Vorreiter wie die Piratenpartei oder den Chaos Computer Club geben. Und schließlich braucht es sehr viel Aufklärungsarbeit. Ein Beispiel: Kaum jemand liest den gesamten *Code de la route* und trotzdem kennen alle die wichtigsten Regeln, weil sie ihnen immer wieder vermittelt werden.

Die Demo „Freedom Not Fear“ richtete sich 2014 gegen alle Formen staatlicher Überwachung (©Freedom not Fear)

Das heißt, das Grundrecht Datenschutz ist relativ?

T. L.: Wir haben alle ein Recht auf Sicherheit und ich will nicht, dass es in Luxemburg oder anderswo zu Terroranschlägen kommt. Aber will ich zu diesem Zweck meine Flugdaten hergeben und zum gläsernen Menschen werden? Da sind Grundrechte gegeneinander abzuwägen. Datenschutz ist eine schwierige Materie, weil sie so viele andere Rechte betrifft. Es gilt das zu tun, was in einer bestimmten Situation nützlich, realistisch und notwendig ist.

Das Safe-Harbor-Abkommen zwischen der EU und den USA steht seit dem NSA-Skandal in der Kritik, weil es das Grundrecht auf Datenschutz nicht garantiere …

T. L.: Im Rahmen von Safe Harbor haben sich US-amerikanische Unternehmen bei der Foreign Trade Commission in eine Liste eingetragen, wodurch sie mit ihrem Namen dafür haften, dass sie ein adäquates Datenschutzniveau gewährleisten. Nun stellt sich seit dem NSA-Skandal die Frage, inwiefern man den Unternehmen vertrauen kann. Doch Luxemburg sind dabei Hände und Füße gebunden. Luxemburg kann hier nicht ein Abkommen zwischen der EU und den USA infrage stellen. Das war auch das Problem bei der Beschwerde, die der österreichische Aktivist Max Schrems gegen Skype bei uns eingereicht hat. Skype fällt unter das Safe Harbor Abkommen. Wir hatten auch nichts in der Hand außer Zeitungsartikeln – Hören-Sagen, aber keine ausreichenden Beweise.

Das heißt, dieses Problem müsste auf EU-Ebene geregelt werden?

T. L.: Ja, denn die EU ist dabei, das Safe-Harbor-Abkommen mit den USA neu zu verhandeln. Die Affäre Schrems ist nun anhängig vor dem Europäischen Gerichtshof. Max Schrems hatte in Luxemburg vor dem Verwaltungsgericht geklagt, er hat aber mittlerweile diese Klage zurückgezogen, weil es prozedurale Schwierigkeiten gab, die ihn eventuell blockiert hätten. Seine Klage in Irland hat hingegen die prozeduralen Hürden überwunden. Das Gericht in Irland hat eine „question préjudicielle“ an den EuGH gestellt. Die Zukunft von Safe Harbor wird sich also sowohl in den Verhandlungen der EU-Kommission als auch mit einem Urteil des EUGh entscheiden.

Vielen Dank für das Gespräch! ◆

Das Interview fand am 20. August 2015 statt. Die Fragen stellte Laurent Schmit.