Rede des
Parlamentarischen Staatssekretärs
bei der Bundesministerin der Justiz,
Dr. Max Stadler, MdB

„Datenschutz im Jahr 2010“
bei der Tagung Codex digitalis
Optimierter Persönlichkeitsschutz– digital und vernetzt

am 30. August 2010 in Kiel

Es gilt das gesprochene Wort!

Sehr geehrter Herr Dr. Weichert,
lieber Herr Schaar,
meine sehr geehrten Damen und Herren,

ich möchte Ihnen heute vorstellen, was die Bundesregierung in diesem Jahr in Sachen Datenschutz tut, was wir vorhaben und wo wir die größten Aufgaben für die Zukunft sehen.

Dies lässt sich in drei Punkten zusammenfassen:

- Es geht erstens um klaren Datenschutz im Arbeitsverhältnis. Deshalb werden wir den Beschäftigtendatenschutz gesetzlich völlig neu regeln.

- Es geht zweitens um mehr Datenschutz außerhalb zusätzlicher Gesetzgebung. Hierfür wird der Bund die Stiftung Datenschutz einrichten.

- Und drittens geht es um neue Herausforderungen für den Datenschutz durch das Internet, zum Beispiel in Gestalt von Internetdiensten wie Google Street View.

Beginnen wir mit dem Beschäftigtendatenschutz.

Die Datenskandale zum Beispiel bei der Bahn, bei Lidl und bei der Telekom haben gezeigt, dass es hier noch immer große Defizite gibt. Wir wollen deshalb durch verständliche und klare gesetzliche Vorschriften mehr Rechtssicherheit schaffen und den Schutz der Beschäftigtendaten verbessern.

Dabei gehen wir von fünf Grundsätzen aus:

Erstens: Datensparsamkeit. Es sollen so wenige Daten über die Beschäftigten erhoben werden, wie möglich.

Zweitens: Enge Zweckbindung. Es dürfen nur Informationen erhoben werden, die mit dem konkreten Job etwas zu tun haben.

Drittens: Konkrete Tatbestandsvoraussetzungen. Unbestimmte Klauseln zur „Erforderlichkeit“, die allein der Arbeitgeber definiert, reichen nicht aus.

Viertens: Wir brauchen abgestufte Regelungen: Je vager etwa der Verdacht auf eine Regelverletzung im Unternehmen ist, desto geringere Eingriffe sind erlaubt; wird der Verdacht dagegen stärker und konkreter, ist mehr an Eingriffen zulässig.

Fünftens schließlich: Auch im Unternehmen gilt für den Arbeitnehmer der verfassungsrechtliche Kernbereichsschutz, Überwachungsmaßnahmen, die diesen Bereich verletzen, sind unzulässig.

Konkret bedeutet dies zum Beispiel: Die Gesundheit eines Stellenbewerbers geht ein Unternehmen nur mit Blick auf den konkreten Arbeitsplatz etwas an. Abschreckendes Beispiel: EU-Mitarbeiter von MdEPs.

Wenn Mercedes einen Testfahrer für seine Autos sucht, dann ist ein umfassender Gesundheitscheck erlaubt als bei der Einstellung einer Bürokraft.

Besonders schwierig ist der Bereich der sogenannten Compliance. Wenn ich etwa an die Massen-Screenings denke, die bei der Deutschen Bahn geschehen sind, dann stellt sich doch die Frage: Wie weit darf der Arbeitgeber gehen, um Straftaten oder Pflichtverletzungen aufzuklären? Wie kann er sich etwa vor Korruption oder Unterschlagung schützen, ohne unnötig in die Rechte der Arbeitnehmer einzugreifen?

Künftig soll es ein Stufenkonzept geben [§ 32d Abs. 3]: Ohne konkreten Verdacht dürfen Datenabgleiche nur in anonymisierter oder pseudonymisierter Form durchgeführt werden. Hier hat Vorrang, die Daten des Beschäftigten zu schützen. Erst wenn sich ein konkreter Verdacht ergibt, dürfen die Daten – auf der zweiten Stufe – auch personalisiert werden.

Noch enger müssen die Anforderungen ausgestaltet werden, wenn es um die heimliche Datenbeschaffung geht [§ 32e]. Darf etwa ein Unternehmen einen Detektiv losschicken, der heimlich das Verhalten seiner Beschäftigten ausforscht, zum Beispiel in einer Filiale der Supermarktkette XY? Hier werden wir klare Tatbestandvoraussetzungen haben:

1. Es müssen einerseits Tatsachen vorliegen, die einen Verdacht gegen einen konkreten Beschäftigten ergeben.

2. Andererseits muss dieser Verdacht auf die Begehung einer Straftat oder einer anderen schweren Pflichtverletzung gerichtet sein.

3. Und dieser Verstoß muss zudem so gravierend sein, dass er den Arbeitgeber zu einer fristlosen Kündigung berechtigen würde.

Daten, die den Kernbereich privater Lebensgestaltung betreffen, darf der Arbeitgeber nicht erheben oder verwenden. Dauerobservationen oder der Einsatz besonderer technischer Überwachungsmittel sollen verboten sein.

All dies macht deutlich: Die heimliche Datenerhebung ist nur unter sehr engen Voraussetzungen möglich.
Eine besonders eingriffsintensive Maßnahme ist die heimliche Videoüberwachung. Hier haben wir nach schwierigen Diskussionen durchgesetzt, dass sie generell unzulässig sein soll.

Letzter wichtiger Punkt: die Abdingbarkeit des Gesetzes.

Weil der Beschäftigte in einem Arbeitsverhältnis als der strukturell schwächere Vertragspartner gegenüber dem Arbeitgeber anzusehen ist, dürfen datenschutzrechtliche Einwilligungen im Beschäftigungsverhältnis nicht generell erlaubt sein. Dies könnte nämlich dazu führen, dass Arbeitgeber routinemäßig Einwilligungen anfordern und dadurch die gesetzlichen Regelungen mit ihren dahinterstehenden Wertungen kurzerhand für obsolet erklärt werden. Hier ist aus unserer Sicht besondere Vorsicht nötig.

Ähnliches gilt für Betriebs- oder Dienstvereinbarungen. Wir möchten, dass von den Vorschriften des Beschäftigtendatenschutzes grundsätzlich nicht zu Ungunsten der Beschäftigten abgewichen werden kann. Allerdings sollten solche Vereinbarungen möglich bleiben, die die gesetzlichen Vorschriften bezogen auf die speziellen Bedürfnisse eines Unternehmens konkretisieren.

Meine Damen und Herren,
beim Beschäftigtendatenschutz sehen wir zum Schutz der Arbeitnehmer gesetzgeberischen Handlungsbedarf. Aber wir wissen auch: Datenschutz darf keine gut gemeinte Bevormundung sein, bei der die Menschen vor sich selbst geschützt werden. Es geht vielmehr um informationelle *Selbst*bestimmung. Wie Peter Schaar einmal so treffend gesagt hat: Der Datenschutz ist nicht die „Supernanny der Nation“.

Die Fähigkeit zur informationellen Selbstbestimmung will die Bundesregierung durch eine neue Stiftung Datenschutz stärken.

Diese Stiftung soll vor allem drei Aufgaben haben:

- Die Stiftung wird durch ihre Aufklärungsarbeit mehr Sensibilität wecken im Umgang mit persönlichen Daten – vor allem bei jungen Menschen. Viele geben noch immer viel zu leichtfertig persönliche Daten von sich und anderen preis, vor allem im Internet.

- Die Stiftung kann auch Vergleichstests nach dem Vorbild der Stiftung Warentest durchführen. Das erleichtert den Verbrauchern die Orientierung am Markt.

- Und sie kann ein Gütesiegel für besonders datenschutzfreundliche Produkte und Dienstleistungen entwickeln. Dieses Siegel kann für die Unternehmen ein echter Wettbewerbsvorteil werden, und Verbraucher könnten sich dann ganz bewusst für ein hohes Datenschutzniveau entscheiden.

Derzeit beraten wir hierzu innerhalb der Bundesregierung noch einige offene Fragen, zum Beispiel wie wir den privaten Sektor einbeziehen können. Außerdem müssen wir noch klären, wie die Finanzierung der Stiftung bestmöglich gelingt. Dem Bundesministerium der Justiz ist vor allem wichtig, dass die Stiftung möglichst bald das Licht der Welt erblickt. Sie wird sich denn schon weiter entwickeln.

Eine solche Stiftung ist ein guter Weg, mehr Datenschutz zu erreichen, denn ich meine, wir brauchen beides: bessere Gesetze, aber auch andere Wege zu mehr Eigenverantwortung.

Meine Damen und Herren,
ein Thema, das in diesem Sommer viele Gemüter bewegt, ist Google Street View. Viele Bürger beunruhigt, dass ihr Haus samt Vorgarten und Auto ungefragt weltweit im Internet veröffentlicht werden soll. Die wachsenden Möglichkeiten, solche sogenannten georeferenzierten Daten mit persönlichen Daten im Netz zu verknüpfen, bereiten vielen Menschen Sorgen. Für den Datenschutz ist das eine enorme Herausforderung; und auch für den Staat schlechthin, denn das globale Internet zeigt hier die Grenzen der Regelungsmacht des einzelnen Staates auf.

Ich weiß, dass sich beim Thema Google Street View der zuständige Hamburgische Datenschutzbeauftragte stark engagiert. (Lieber Herr Professor Caspar, ich bin Ihnen für den Einsatz in dieser Sache außerordentlich dankbar.)

Die Zusage von Google, bei Aufnahmen aus Deutschland alle Gesichter und Autokennzeichen von vornherein zu verpixeln und bei Widersprüchen auch ganze Gebäude unkenntlich

zu machen, ist gut und richtig. Es gibt aber ernste Zweifel, ob diese Zusagen wirklich ausreichend sind. Natürlich war auch die Frist von vier Wochen für einen Widerspruch während der Sommerferienzeit viel zu kurz bemessen. Hier hat der öffentliche Druck immerhin Erfolg gehabt.

Ich meine, wir haben es bei diesem Thema mit einem grundlegenden Problem zu tun. Die Frage ist, ob wir wirklich alles wollen, was im Internet technisch machbar ist. Führt uns dieses technische „anything goes“ nicht letzten Endes in eine Gesellschaft ohne Privatsphäre und ohne „Gnade des Vergessens“? Die Google-Street-View-Thematik steht stellvertretend für eine grundlegende Debatte.

Einen äußerst wertvollen Impuls für diese Diskussion verdanken wir dem Bundesverfassungsgericht und seinem Urteil zur Vorratsdatenspeicherung. Dessen Bedeutung reicht weit über die Vorratsdatenspeicherung hinaus. Das Gericht hat in seiner Entscheidung betont, dass es zur Verfassungsidentität unseres Landes gehört, dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf.

Diese Feststellung betrifft nicht nur staatliche Aktivitäten. Sie hat auch Auswirkungen auf Datennutzungen und Dienste privater Unternehmen, vor allem im Zusammenhang mit dem Internet. Wenn heute georeferenzierte Daten mit persönlichen Daten in Windeseile elektronisch verknüpft werden, dann droht nicht mehr der Überwachungs*staat*, sondern eine Überwachungsgesellschaft, in der sich die Bürger ständig gegenseitig im Blick behalten können. Ich meine, dass hier der Staat gefordert ist. Er hat die Pflicht, die freiheitliche Verfassungsidentität unseres Landes zu wahren.

Der Bundesinnenminister, der hier federführend ist, hat viele Akteure für den 20. September zusammengerufen. Das Bundesministerium der Justiz legt Wert darauf, dass dies nicht nur eine unverbindliche Diskussionsrunde wird. Dieses Treffen muss der Vorbereitung eines konkreten Gesetzentwurfs dienen. Ein Vorschlag des Bundesrates liegt bereits auf dem Tisch. Diesem Entwurf, der wie ein Einzelfallgesetz zu Google Street View erscheint, möchte sich die Bundesregierung allerdings nicht anschließen. Es besteht die Gefahr, dass wir immer wieder der technischen Entwicklung hinterherlaufen und nachbessern müssen, wenn wieder ein neuer Dienst erfunden wird. Notwendig ist vielmehr eine generelle Regelung zu georeferenzierten Daten im Internet und deren Verknüpfung mit anderen Daten. Dabei dürfen wir das Kind natürlich nicht mit dem Bade ausschütten; natürlich sind Stadtplan- oder Landkartendienste eine gute Sache, die will niemand verbieten. Aber dass Regelungsbedarf besteht, liegt ja auf der Hand: Was macht Google denn, wenn der Mieter eines Hauses gegen die Abbildung Widerspruch einlegt, der Vermieter aber, der das Gebäude vielleicht ver-

kaufen will und ein Interesse an einer Abbildung hat, *gegen* eine Verpixelung ist? Wie werden solche Interessenkonflikte gelöst? Eine gesetzliche Regelung muss unter anderem auf solche Fragen Antworten geben.

Hier steht vor allem das zuständige Bundesinnenministerium in der Pflicht. Und wir Liberalen haben dabei die klare Erwartung, dass dieses Thema nicht auf die lange Bank geschoben wird. Wir hatten in der Koalition vereinbart, das Datenschutzgesetz mit Blick auf das Internet generell auf den Prüfstand zu stellen; jetzt sollte das Thema „Geodaten“ vorgezogen werden, um zumindest für diesen Bereich rasch zu einer Lösung zu kommen.

Dabei dürfen wir natürlich einen Umstand nicht außer Acht lassen. Nationale Regelungsmacht hat in Zeiten des World Wide Web Grenzen. Und wir müssen auch bedenken, dass wir nicht durch nationale Alleingänge Wettbewerbsnachteile für deutsche Unternehmen schaffen.

Meine Damen und Herren,
wie sich Privatheit und informationelle Selbstbestimmung im digitalen Zeitalter effektiv schützen lassen, ist vielleicht eine der größten rechtspolitischen Fragen unserer Zeit. Fertige Antworten habe ich nicht zu bieten. Aber manchmal ist ja der wichtigste Schritt, die richtigen Fragen zu stellen und dank Google Street View kann diese Fragen jetzt niemand mehr überhören.