



## **Digital Enlightenment Forum (Forum Digitale Aufklärung)**

**„Personenbezogene Daten und Bürgerschaft in der digitalen Gesellschaft“**

**Crowne Plaza, Brüssel, 19. September 2013**

---

### **Zweiter Tag: Politik, Visionen und Debatte - Eröffnungssitzung**

*Peter Hustinx*

*Europäischer Datenschutzbeauftragter*

#### **Eröffnungsrede**

Ich freue mich über die Gelegenheit, einen Beitrag zum „Digital Enlightenment Forum“ 2013 leisten zu können.

Das digitale Umfeld, in dem wir heute alle leben, ist mit Sicherheit ein Raum, in dem viel Platz für Kreativität, Innovation und technische Meisterleistungen besteht. Gestatten Sie mir aber gleich den Hinweis, dass noch mehr Kreativität erforderlich ist, um eine bessere digitale Governance und echte Bürgerschaft für alle in der digitalen Gesellschaft zu gewährleisten.

Ereignisse der jüngsten Vergangenheit – heute als Prism-Story und ähnliche Enthüllungen bekannt – haben aufgezeigt, wie gefährdet unser aktuelles digitales Umfeld aufgrund rechtmäßiger oder unrechtmäßiger Überwachung, des Abhörens und des umfassenden Screenings eines Großteils, wenn nicht gar des gesamten weltweiten elektronischen Verkehrs ist.

Es handelt sich wohl um eine Fortsetzungsgeschichte, und von Woche zu Woche dürften weitere Einzelheiten ans Licht kommen.

Nach dem heutigen Wissensstand fällt jedoch nicht nur ins Auge, in welchem Umfang und wie tiefgehend diese Überwachung betrieben wurde, sondern auch, dass ganz offensichtlich zahlreiche Akteure wie bekannte Internetprovider entweder aktiv oder passiv daran beteiligt waren und auch Hintertüren in die Verschlüsselung eingebaut haben, was weit reichende verheerende Wirkungen hatte und dem Vertrauen der Öffentlichkeit unermesslichen Schaden hinzugefügt hat, von dem doch die Existenz und die weitere Entwicklung unseres digitalen Umfelds abhängen.

All dies hat Schockwellen rund um den Globus ausgelöst und löst sie noch immer aus.

Wir sollten uns jedoch der Tatsache bewusst sein, dass diese Gefährdungen auch auf andere Faktoren zurückgehen, die im Verlauf der Jahre allmählich an Bedeutung gewonnen haben, wie die derzeitige Machtverteilung im Internet, die Ausdruck sowohl seiner Architektur als auch der wirtschaftlichen Bedingungen für sein Funktionieren ist.

Ein weiterer Faktor ist die Tatsache, dass sich viele Menschen an die Verfügbarkeit kostenloser Dienste als Gegenleistung für eine praktisch permanente intensive Überwachung ihres Verhaltens gewöhnt haben. Nicht jeder ist sich in vollem Umfang der Tatsache bewusst, dass es in Wirklichkeit keine kostenlosen Dienste gibt. Damit besteht nun eine Grundlage für die Einbeziehung privater Akteure in die Überwachungstätigkeit des öffentlichen Sektors in großem Maßstab.

Wir erleben gerade einen Paradigmenwechsel: Dort, wo vor gar nicht allzu langer Zeit die Vertraulichkeit der Kommunikation ein unumstößlicher Grundsatz und eine sorgfältig gehütete Vorgehensweise war, stehen wir nun vor der Transparenz der Kommunikation, die von einigen sogar gefeiert wird, und das alles ohne irgendeine Änderung einer Verfassung oder irgendeiner Form von fundierter Debatte. Es scheint im Wesentlichen eine Modeerscheinung zu sein, angetrieben von der Faszination der Technologie und dem Wunsch nach einem bequemen Leben.

Es trifft allerdings noch immer zu, dass das digitale Vertrauen in den kommenden Jahren im Wesentlichen von unserer Fähigkeit abhängen wird, rechtliche und technische Infrastrukturen bereitzustellen, die ein Vertrauen schaffen und bewahren können, das auf allgemein anerkannten Grundsätzen und Vorgehensweisen verantwortungsvollen staatsbürgerlichen Handelns in der digitalen Gesellschaft beruht.

Die EU befindet sich derzeit in einer ambitionierten Reform ihres geltenden Rechtsrahmens für den Schutz der Privatsphäre und den Datenschutz, um sie in der Praxis wirksamer und in der EU einheitlicher zu gestalten. Grundlage hierfür ist die Anerkennung dieser Konzepte als Grundrechte, die in der Europäischen Charta der Grundrechte verankert sind, die wiederum durch den Vertrag von Lissabon rechtsverbindlich geworden ist, und zwar nicht nur für Organe und Einrichtungen der EU, sondern auch für die Mitgliedstaaten, wenn sie im Rahmen des EU-Rechts tätig werden.

Ein in der Praxis wirksamerer Datenschutz bedeutet mehr Rechte für betroffene Personen, größere Verantwortung für Organisationen, die personenbezogene Daten verwenden, und eine strengere Aufsicht und Durchsetzung durch die Datenschutzbehörden. Die vorgeschlagene Verordnung, die an die Stelle der derzeitigen Richtlinie treten soll, wird für mehr Kohärenz innerhalb der EU sorgen. Sie wird für alle gelten, die ihre Waren oder Dienstleistungen auf dem europäischen Markt anbieten und somit für mehr Chancengleichheit sorgen, als es der aktuelle Rechtsrahmen vermag.

Kommission, Rat und Parlament arbeiten hart daran, diesen neuen Rechtsrahmen noch vor den Europa-Wahlen im Frühjahr 2014 anzunehmen. Schon in einigen Wochen wird der LIBE-Ausschuss des Parlaments über seinen Bericht abstimmen. Nach dieser Abstimmung werden wir dann vermutlich Zeuge intensiver Bemühungen um einen gemeinsamen Wortlaut, den Rat und Parlament mittragen können. Ich bin optimistisch und gehe davon aus, dass dies innerhalb der verfügbaren Zeit geschehen wird.

Nach der Annahme dieses neuen Rechtsrahmens wird es möglich sein, wirksamer als derzeit gegen übermäßiges Orten und Verfolgen, Überwachen und Erstellen von Verhaltensprofilen im Internet vorzugehen. Er wird ein größeres Gegengewicht gegen aktuelle Trends im Internet sein und kann dazu beitragen, ansatzweise wieder einen annehmbaren Interessenausgleich herzustellen und gestärktes Vertrauen in dieses Umfeld aufzubauen.

Die Wirtschaft sollte mit Vorgehensweisen, die sich auf Datenschutz durch Technik, Transparenz und Rechenschaftspflicht stützen, diesen Bemühungen anschließen. Bitte verstehen Sie mich nicht falsch: Es ist weder möglich noch wünschenswert, Innovation zu „regulieren“, aber das Gesetz kann die richtigen Verantwortlichkeiten festlegen und die richtigen Anreize bieten, und genau das wird der neue Rechtsrahmen tun.

Es sollte auch auf allen relevanten Ebenen eigenständig der Frage nachgegangen werden, inwieweit es Regierungen und in ihrem Namen tätigen Einrichtungen erlaubt sein sollte, elektronischen Verkehr abzuhören, und wenn ja, unter welchen Bedingungen und mit welchen Garantien.

Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte äußert sich diesbezüglich ganz klar, und dies schon seit mehreren Jahrzehnten. Sie gilt für alle Mitgliedstaaten und kann auch Denkanstöße für Diskussionen mit der anderen Seite des Atlantiks geben, wenn die Zeit reif ist, auch in diesem Bereich Fortschritte zu erzielen.