30 Jahre nach der Datenschutzkonvention des Europarats „Keine Privatsphäre mehr im Netz ?“

Dr. Alexander Dix, LL.M.
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Konferenz
der Luxemburgischen Datenschutzkommission
27. Januar 2011
Luxemburg

Übersicht

- Einleitung
- Notwendigkeit des Schutzes der Privatsphäre
- Möglichkeiten ihres Schutzes im Netz
- Das Beispiel der sozialen Netzwerke
- Notwendigkeit der Modernisierung des Datenschutzes in Europa und weltweit
- Fazit

Einleitung

- 28. Januar 1981: Unterzeichnung der Konvention No. 108 des Europarates zum *Schutz des Menschen* bei der automatischen Verarbeitung personenbezogener Daten beginnt
- Erfolgsgeschichte bis heute: 43 Signatarstaaten, die ersten 7 waren Luxembourg, Dänemark, Frankreich, Österreich, Schweden, Deutschland und die Türkei, 38 Ratifikationen

Die Notwendigkeit des Schutzes der Privatsphäre

- „You have zero privacy anyway – get over it !“

  Scott McNealy

- „The age of privacy is over.“

  Marc Zuckerberg

- Die gesellschaftliche Realität sieht anders aus: Sowohl junge als auch ältere Menschen haben ein Grundbedürfnis nach Rückzugsräumen auch im Netz, in denen sie unbeobachtet sind.

Die Notwendigkeit des Schutzes der Privatsphäre

- Junge Menschen „fliehen“ zum Teil vor familiärer Kontrolle ins Internet, in soziale Netzwerke, um sich dieser Kontrolle zu entziehen

- Sie erliegen einer „Illusion von Intimität“ und erkennen zu spät, dass sie auch dort beobachtet werden (spätestens dann, wenn die Eltern auch bei Facebook sind)

Offenheit und Schutz vor Diskriminierung

Grundlegendes Missverständnis:
Die Protagonisten einer neuen „Offenheit“ (*Californian openness*) verkennen, dass die Gesellschaft (noch) nicht so liberal ist, dass sie auf Diskriminierung aufgrund der veröffentlichten persönlichen Daten verzichtet und alles toleriert. Entsprechende effektiv durchgesetzte Diskriminierungsverbote fehlen (Beispiel: AIDS)

Verwechselung von Ursache und Wirkung

Facebook und andere Unternehmen reagieren nicht auf eine gesellschaftliche Tendenz hin zu weniger Datenschutz, sondern sie bieten ihren Nutzern einen Dienst an, der in der Grundeinstellung erst zu einer Absenkung des Datenschutzes führt, ohne dass sich die Nutzer dessen bewusst wären.

Öffentliche Diskussion über Datenschutz nimmt zu

Umgekehrt zeigen gerade die zunehmenden öffentlichen Diskussionen z.B. über Google Street View oder Facebook zweierlei:

- Datenschutz ist nicht überholt
- Unternehmen realisieren zunehmend, dass sie den Schutz der Privatsphäre nicht vernachlässigen dürfen, wenn sie wirtschaftlichen Erfolg haben wollen

Möglichkeiten des Schutzes der Privatsphäre

- Datensparsame, differenzierte Nutzung der modernen Kommunikationskanäle
- Datenschutzfreundliche Grundeinstellung der Dienste
- Handhabbare Werkzeuge zum Selbstschutz müssen bereitgestellt werden
- Der Umgang mit diesen Werkzeugen muss auf den Unterrichtsplan der Schulen
- Berücksichtigung des Datenschutzes schon bei der Entwicklung von Produkten und Diensten („privacy by design“)

Grenzen des Schutzes der Privatsphäre

- Keine vollständige Kontrolle über die Datenverarbeitung im Netz, insbesondere, wenn sie im außereuropäischen Ausland stattfindet; aber Zusammenarbeit der Behörden wird verbessert

- Bisher kein Recht auf Vergessen im Netz, aber in diesem Bereich gibt es erste positive Entwicklungen

Beispiel: Soziale Netzwerke

- Anbieter sozialer Netzwerke sind gut beraten, wenn sie nicht im trial-and error-Verfahren zu ergründen versuchen, was die Nutzer an Einbußen der Privatsphäre noch hinzunehmen bereit sind. Sie sollten stattdessen von vornherein hohe Datenschutzstandards zugrunde legen, wie sie z.B. in Europa gelten
- Der Wettbewerb im Bereich der sozialen Netzwerke scheint momentan zugunsten des weltweit größten Netzwerks zu verlaufen, das eine erhebliche Sogwirkung entwickelt. Das kann sich aber schnell ändern (z.B. aus Gründen des Datenschutzes)

Datenschutzanforderungen an soziale Netzwerke

- Erstmals aufgestellt von der „Berlin Group“ im Rom-Memorandum (2008) und weiter entwickelt von der Art.-29-Gruppe (Working Paper 163 – 2009)

- Beide Papiere enthalten sowohl Anforderungen an die Betreiber solcher Plattformen als auch an ihre Nutzer

Anforderungen an die Betreiber sozialer Netzwerke

Betreiber sollten:

die Nutzer in (altersabhängig) verständlicher und offener Weise darüber informieren, was mit ihren Daten geschieht, welche Risiken dies verursacht;

die gegebenen Versprechen einhalten;

datenschutzfreundliche Standard-(Grund-)einstellungen vorsehen;

die Kontrolle der Nutzer über ihre Profildaten verbessern;

die Verwendung von Pseudonymen (Spitznamen) zulassen und

die Sicherheit der Informationssysteme verbessern

Empfehlungen für Nutzer sozialer Netzwerke (1)

Nutzer sollten:

vorsichtig bei der Online-Veröffentlichung eigener Daten sein; es ist technisch nicht zu verhindern, dass „Freunde“ ihre Daten ins offene Internet kopieren;

in der Regel ein **Pseudonym** (Spitznamen); verschiedene Plattformen für verschiedene Zwecke oder Lebenszusammenhänge nutzen;

Empfehlungen für Nutzer sozialer Netzwerke (2)

Nutzer sollten vor allem:

die **Privatsphäre anderer respektieren** (insbesondere beim Hochladen von Bildern, aber auch bei Texten);

sich umfassend über die Plattform informieren, bevor man sich dort registriert, bei unzureichenden Informationen Anbieter wechseln;

auf das achten, was die eigenen **Kinder** in sozialen Netzwerken machen.

Eine nützliche Broschüre

„Ich suche Dich“
Soziale Netzwerke & Datenschutz
Tipps für Jugendliche

Herausgegeben vom Jugendnetz-berlin.de und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit (online verfügbar unter *http://www.datenschutz-berlin.de/content/veroeffentlichungen/a-z*)

Beispiel:
Facebooks Friendfinder (1)

Facebook bietet Nutzern die Möglichkeit, ihre Kontakte bei F hochzuladen und abzugleichen, wer von ihnen schon bei F ist.

Bisher begnügt sich F nicht mit dem Abgleich, sondern nutzt die Daten der noch nicht Registrierten, um ihnen unaufgefordert Werbung zu schicken **(Sogwirkung)**

Beispiel:
Facebooks Friendfinder (2)

- Dieses Vorgehen widerspricht deutschem und europäischem Datenschutzrecht

- Facebook hat sich jetzt gegenüber dem Hamburgischen Datenschutzbeauftragten bereiterklärt, das Verfahren datenschutzgerechter zu gestalten, aber nur in Deutschland (ähnlich wie vorher schon Google für Street View)

Insellösungen machen keinen Sinn

- Unternehmen wie Google oder Facebook, die ihre Angebote weltweit machen, sollten sie auch weltweit datenschutzgerecht gestalten
- Nationale Insellösungen sind aufwändig und unwirtschaftlich
- Zudem laufen die Unternehmen Gefahr, in anderen Ländern auch in Konflikt mit dem Datenschutz zu kommen

Beispiel: Apps

- Apps (Applications) sind Programme (z.B. Spiele wie *Farmville* oder *Angry Birds*), die man in sozialen Netzen kaufen oder sich auf sein iPhone laden kann

- Problem: Unkontrollierbare Datenflüsse des Nutzers zum App-Anbieter (nicht identisch mit Facebook oder Apple); es werden auch Daten übermittelt, die für die App nicht erforderlich sind.

Datenschutzfreundliche Einbindung von Apps

- Der deutsche Anbieter VZ Netzwerke (schuelerVZ, studiVZ, meinVZ) verwendet ein datenschutzfreundliches System von Visitenkarten, bei dem der Nutzer im Detail entscheiden kann, welche Daten einem App-Anbieter übermittelt werden sollen

- Gutes Beispiel für andere Plattformen

Notwendige Modernisierung des Datenschutzes in Europa und weltweit

- Europarat, OECD und Europäische Union feiern gerade ihre 30 Jahre geltenden Datenschutzregeln

- Das sollte auch Anlass sein, sie grundlegend zu erneuern und fit zu machen für die Informationsgesellschaft des 21. Jahrhunderts

Modernisierung des Datenschutzes in Europa

- Die EU-Kommission hat die weitreichendsten Vorschläge gemacht (Gesamtkonzept für einen neuen europäischen Rechtsrahmen für den Datenschutz)
- Dazu zählen die Stärkung der Rechte des Betroffenen gerade auch im Netz durch Sicherung von Auskunfts- und Löschungsrechten („digitales Radiergummi“) und durch die Übertragbarkeit (*portability*) von Nutzerkonten

Modernisierung des Datenschutzes weltweit

- Die Rechtsentwicklung in Europa hat auch Einfluss auf die internationale Entwicklung im Datenschutz
- Die US Federal Trade Commission hat Vorschläge zum *behavioural targeting* gemacht, die schon zu Reaktionen bei den Browser-Anbietern geführt haben
- Europarat und OECD werden bei ihren Modernisierungsbestrebungen die Vorschläge der EU-Kommission nicht außer Acht lassen können

Vielen Dank !

dix@privacy.de