Thesen aus den Workshops

Sommerakademie 2012

„Sozialere Netzwerke im Internet
– durch Datenschutz“

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Praktische Auswirkungen der Nutzung sozialer Medien

- **Trag- und Reichweite von Beiträgen** in sozialen Netzen ist vielen Nutzern nicht klar
- **Adressierung und Löschung** von Beiträgen ist vollständig abhängig von technischer und organisatorischer Mithilfe des Betreibers
- Betreiber **erschleichen** sich teilweise Daten über Nutzer
- Vor allem bei der **mobilen Nutzung** bleibt der **Umfang** von erhobenen Daten oft vor dem Nutzer verborgen
- **Verfolgung der Nutzer** über Netzwerkgrenzen hinweg nimmt rapide zu
- Tracking-Schutz wird zunehmend schwierig, da Netzwerkbetreiber **Dienste in verschiedenen Nutzungssegmenten** anbieten, die dann eine ständige Verkettbarkeit ermöglichen

Verteilte soziale Netzwerke – Technik, Chancen und Risiken

- Risikosituation in sozialen Netzwerken wird wesentlich durch **Betreibermodell** beeinflusst
- Zentrale Modelle leiden aktuell unter Intransparenz der Anbieter und werden vom **Risiko „Anbieter als Angreifer“** dominiert
- **Dezentrale, servergestützte Modelle** sind Fortschritt, aber keine Lösung für „Anbieter als Angreifer“
- Dezentrale, servergestützte Modelle im **Eigenbetrieb** bilden eine gute Alternative zu großen Anbietern sozialer Netzwerke
- **P2P-basierte Ansätze mit Ende-zu-Ende-Sicherheit** sind aus Datenschutzsicht anzustreben und zu unterstützen

Öffentliche Stellen und soziale Netzwerke – geht das?

- **Verantwortlichkeiten** müssen zum umfassenden Schutz personenbezogener Daten an die technischen und praktischen Gegebenheiten **angepasst** werden

- Daher: **gemeinsame Verantwortlichkeiten aller Beteiligten**, wie z. B. im Umweltrecht

Attribut-basierte Credentials im Praxistest – mehr Datenschutz im sozialen Netzwerk einer schwedischen Schule

- Attribut-basierte Credentials (ABCs)
  - kombinieren **Anonymität / Nicht-Verkettbarkeit** mit **Authentizität** und
  - ermöglichen **Einzelfall-Aufdeckung** unter vordefinierten Bedingungen
- **Pilot** in schwedischer Schule im EU-Projekt ABC4Trust: Einsatz von ABCs in der Kommunikation zwischen Schülern / Lehrkräften / Sozialarbeitern / Eltern
- Ziel: **Blaupause** für datenschutzförderndes Identitätenmanagement mit **Privacy-ABCs** – auch für soziale Netzwerke

„Wir müssen da rein“ – was Unternehmen bei der Eigenpräsentation in sozialen Netzwerken beachten müssen

- Unternehmen sind in der Regel **verantwortlich** für ihr Auftreten in sozialen Netzwerken und müssen Rechtsrahmen beachten (u. a. Impressumspflicht, Datenschutzerklärung)
- Problembereich **Fanpages**
  - Betrieb unzulässig, wenn pseudonyme Nutzung bzw. Verzicht auf Profilbildung nicht möglich ist
- Problembereich **Social-Plugins**
  - Direkte Einbindung i.d.R. problematisch
  - Ggf. Zwei-Klick-Lösung, sofern informierte Einwilligung eingeholt wird

„Wir sind drin. Und nun?“ – Nutzung von Social Media durch, für und gegen Beschäftigte

- Wichtig: Rechtsrahmen abstecken
  - Insbesondere **Social-Media-Guidelines** entwickeln / festlegen
  - Betriebsrat / Personalrat einbinden
- Unterscheiden zwischen **privater und dienstlicher Nutzung**
- Problembereich: **Verhaltenskontrolle** durch den Arbeitgeber
- Grenzen der **Meinungsfreiheit** vs. Unternehmenstreue
- Ausblick auf Weiterentwicklung des **Arbeitnehmerdatenschutzes**

Soziale Netzwerke – Ermittlungshelfer für die Polizei?

- Soziale Netzwerke sind mittlerweile **maßgebliches Kommunikationsmittel** und integraler Bestandteil der heutigen Gesellschaft

- Bestehende **gesetzliche Grundlagen** für Ermittlungsmaßnahmen der Polizei sind **unzureichend**, weil nicht normenklar

- Maßstab für die Notwendigkeit eigener gesetzlicher Rechtfertigungen bei staatlichen Ermittlungsmaßnahmen: Schutzwürdigkeit des Vertrauens in die **Integrität der Kommunikationspartner** und **Vertraulichkeit der Kommunikation**

Gesichtserkennung, Friendfinding, Social-Plugins, Schattenprofile – Nutzung von Daten Dritter durch Social Media-Dienste

- Die Datenverarbeitung von Sozialen Netzwerkbetreibern ist immer stärker geprägt durch die Erhebung von **Daten Dritter**, die keinen unmittelbaren Kontakt zum Anbieter haben
- Die derzeit geltenden **Vorschriften** regeln die sich daraus ergebenden datenschutzrechtlichen Probleme nur **unzureichend**
- Defizite lassen sich vor allem bei der Zuordnung der datenschutzrechtlichen **Verantwortlichkeit**, der Herstellung der **Transparenz** und der Wahrung der **Betroffenenrechte** feststellen
- Die Etablierung einer datenschutzrechtlichen **Störerhaftung**, institutionalisierter **Transparenzanforderungen** und **geringerer Hürden** bei der Wahrnehmung der Betroffenenrechte könnten ein Beitrag zur Erhöhung des Datenschutzniveaus liefern

Facebook – Datenschutzstrategien für Nutzende

- Rechtliche Einschätzungen:
  Welches Datenschutzrecht ist anwendbar?
- Was Facebook faktisch tut:
  - Funktionalitäten
  - gespeicherte Daten
  - „gelöschte“ Daten
- Beschwerdeverfahren bei der irischen Datenschutzaufsicht
- Nutzerpflichten für Privatpersonen

Liquid Democracy und Online-Beteiligung – wie es die Datenschützer gestalten würden

- Große **Bandbreite** von (möglichen) Online-Beteiligungs-verfahren und Anwendungen:

  Diskussionsplattform, Petitionsverfahren, Bürgerbeteiligung, Abstimmungen, ...

- Konsequenz: ebenso große Bandbreite bei Rahmen-bedingungen und datenschutzrechtlichen Anforderungen
- **Einsatzbedingungen** (z.B. öffentlich/geschlossen; pseudonym/namentlich, ...) müssen festgelegt und konfiguriert werden
- Kennzeichen: flexible **Delegationsmöglichkeiten** für Abstimmungen und Bewertungen
- Transparenz über **Funktionsweise** und **Betrieb** relevant