Big Data für die Big Brothers

Staatliche Massenüberwachung innerhalb und außerhalb der Legalität

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein

32. RDV-Forum

Köln, 13.11.2013

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Snowden und die Geheimdienste
- Nachrichtendienstliche Angriffsszenarien
- Risiken
- Grundrechte
- US-Verfassungsrecht
- Datenschutzgrundsätze
- Big Data
- Bundesverfassungsgericht
- Geheimdienstanwendung
- Verfassungskonformes Big Data

Überwachung durch Geheimdienste

Anfang Juni 2013: Enthüllungen durch Edward Snowden

Politische und wirtschaftl. Spionage, Vollüberwachung der Bevölkerung zw. Terrorismusbekämpfung

- National Security Agency (NSA - USA): Prism u. a.
- Government Communications Headquarters (GCHQ – GB): Tempora u. a.
- Direction Générale de la Securité Extérieure (DGSE – F)
- Bundesnachrichtendienst (BND – D): Strateg. TKÜ u. a.
- Bundesamt für Verfassungsschutz (BfV): u. a. Projekt 6 (Kooperation mit CIA)
- Landesamt f. VerfSch. Niedersachsen: Journalistenerfassg.

Angriffsarten

- Abgreifen von Internetdienstleistern, z. B. Soziale Netzwerke od. Clouds (in den USA, zwangsweise od. freiwillig)
- Verdeckter Zugang zu einem Netzbetreiber (GCHQ-BelgaCom)
- Brechen von Kryptografie
- Verdeckter Zugang zu Internetdiensten (über Backdoors) zur Beschaffung von Meta- und Inhaltsdaten (z. B. Adressbücher)
- Abhören von Internetkabeln oder von Internetknoten
- Beschaffung von (evtl. zulässig erlangten Daten von) „befreundeten“ Diensten (z. B. strategische BND-TKÜ)
- Kapern von Rechnern und Rechnernetzen (unterschiedliche Methoden, z. B. Online-Durchsuchung)
- Verdeckte technische und personale Ermittlungen
- Sammeln und Auswerten „öffentlicher Quellen“ (im Netz)

Risiken

- Ausforschung, Ausspionieren der Privat- und Sozialsphäre
- Wirtschaftsspionage (Betriebs- und Geschäftsgeheimnisse)
- Einschränkung der politischen Freiheiten (freie Meinungs-äußerung, Informations- und Pressefreiheit)
- Einschränkung der wirtschaftlichen Tätigkeit
- Manipulation und Desinformation
- Identitätsdiebstahl und Diskreditierung
- Exekutive Maßnahmen (Strafverfolgung, Inhaftierung, Einreiseverweigerung ...)

Europäische Grundrechte-Charta I

Art. 8:

(1) Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Europäische Grundrechte-Charta II

Art. 1: Würde des Menschen
Art. 6: Freiheit und Sicherheit
Art. 7: Achtung v. Privat- u. Familienlebens, Wohnung u. Kommunikation
Art. 10: Gedanken-, Gewissens- u. Religionsfreiheit
Art. 11: Freie Meinungsäußerung und Informationsfreiheit
Art. 12: Versammlungs- und Vereinigungsfreiheit
Art. 20: Alle Menschen sind vor dem Gesetz frei.
Art. 21: Diskriminierungsverbote
Art. 38: Verbraucherschutz
Art. 42: Recht auf Zugang zu Dokumenten
Art. 44: Petitionsrecht
Art. 47: Anspruch auf Rechtsschutz
Art. 48: Unschuldsvermutung

US-Verfassungsrecht I

1st Amendment: Recht auf anonyme Meinungsäußerung, Vereinigungsfreiheit
3rd Amendment: Schutz der Unversehrtheit der Wohnung
4th Amendment: Schutz vor unangemessener Durchsuchung und Beschlagnahme
5th Amendment: Schutz vor Pflicht zur Selbstbelastung
14th Amendment: Faires Verfahren („due process of law“)

> „Right to (data – information) Privacy“

US-Verfassungsrecht II

Privatheitsschutz durch Supreme Court:

- „Chilling Effects“ bei Meinungs-, Presse-, Versammlungsfreiheit
- Räumliches Verständnis von Privatsphäre
- Schutz vor Selbstbelastung und vor wirtschaftlichem Schaden
- „Reasonable Expectation of Privacy“ (Katz v. USA, 1967)
- Third Party Doctrine > kein Schutz bei freiwilliger Weitergabe an (private) Dritte
- Schützt nur Inländer

> Kein Recht auf informationelle Selbstbestimmung, kein Recht auf Gewährleistung der Integrität und Vertraulichkeit informations-technischer Systeme, kein Grundrecht auf Datenschutz, keine Bindung privater Unternehmen

> Kein Fortschritt seit den 60er Jahren, bürgerrechtliche Kritik seit den 60er Jahren (Alan F. Westin, Privacy and Freedom, 1967)

Big Data I

- Vorläufer: Data Warehousing – Data Mining
- Vorgehen: Verdachtfreie digitale Datenerfassung > Zusammenführung > Verknüpfung > Analyse (Selektion und Auswertung) > Ergebnis
- Personenbeziehbare Anwendungen: Kundenbindung, Marketing in Kommerz und Politik, Kundenbewertung (Targeting, Scoring, Tracking, Profiling), Verkehrswesen, Gesundheitsbereich, Genomanalyse, Internetauswertung, Strafverfolgung, Geheimdienstarbeit

Moderne Datenschutzprinzipien

Europaratskonvention, OECD-Richtlinien, BDSG, Europäische Datenschutzrichtlinie (EU-DSRL), EU-DSGVO-Entwurf, ...

- Rechtmäßigkeit (Art. 5 ff. EU-DSRL, § 4 BDSG)
- Einwilligung (Art. 7 lit. a EU-DSRL, § 4a BDSG)
- Zweckbindung (Art. 6 I EU-DSRL, §§ 28 ff. BDSG)
- Erforderlichkeit und Datensparsamkeit (Art. 6 I c, e EU-DSRL, § 3a BDSG)
- Transparenz und Betroffenenrechte (Art. 11 ff. EU-DSRL, § 33 ff. BDSG)
- Datensicherheit (Art. 17 I EU-DSRL, § 9 BDSG)
- Kontrolle (Art. 28 EU-DSRL, § 38 BDSG)

Big Data II

Umsetzung der Prinzipien am Beispiel Geheimdienste

- Einwilligung (informiert, explizit, freiwillig)
- Rechtmäßigkeit (Patriot Act, FISA, RIPA: unbestimmt, ineffektive Verfahren, geheim, rechtsmittelfrei)
- Zweckbindung (Terrorismusbekämpfung, Sicherheit, Wirtschaftsspionage, politische Spionage)
- Betroffenenrechte (sind bisher nicht bekannt)
- Datenschutzkontrolle (FTC funktioniert nicht, fehlt bei Diensten, FISC unwirksam)
- Technisch-organisatorische Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettbarkeit, Transparenz, Intervenierbarkeit)

BVerfG-E

- 16.7.1969: Verbot totaler Persönlichkeitsbilder
- 15.10.1970: Einschränkung von Art. 10 GG: nachträgliche Benachrichtigung, Kontrolle zumindest gerichtsähnlich
- 15.12.1983: Informationelle Selbstbestimmung, Verbot der Vorratsdatenspeicherung
- 14.07.1999: Art. 10 GG schütz im Ausland, strenge Zweckbindung bei G-10-Maßnahmen
- 11.03.2008: Automatisierte Erfassung (von Kfz-Kennz.) anlasslos und flächendeckend unzulässig
- 02.03.2010: „Dass Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesreplik D."
- 27.02.2008: Digitale Privatsphäre, heimliche Infiltration in IT-System nur bei konkretem Anlass, konkrete Gefahr für überragend wichtiges Rechtsgut

Reaktionen der deutschen Bundesregierung

- Bundeskanzlerin Merkel – 19.07.2013: Deutschland ist kein Überwachungsstaat. In Deutschland und Europa gilt nicht das Recht des Stärkeren, sondern die Stärke des Rechts.
- Geheimdienstkoordinator Pofalla – 26.07.2013: Datenschutz wird von Deutschen Geheimdiensten zu 100% eingehalten.
- Reg.Sprecher – 02.08.2013: Die Bundesregierung nimmt die Sorgen der Bürgerinnen und Bürger sehr ernst.
- Pofalla – 12.08.2013: GCHQ und NSA haben schriftlich versichert, dass sie sich in Deutschland an Recht und Gesetz halten.
- Bundesinnenminister Friedrich – 16.08.2013: Der Verdacht der „Totalausspähung" deutscher Bürger ist vom Tisch. Die Vorwürfe haben sich „in Luft aufgelöst".
- Bundesinnenministerium – 11.09.2013: Datenschützer für NSA-Skandal nicht zuständig.
- Seit 24.10.2013: Kanzlerin-Handy wurde abgehört: Merkel: „Geht gar nicht"

Big Data ist verfassungskonform möglich

- Normenklare Gesetzliche Grundlage nötig, verhältnismäßig und mit technischen und prozeduralen Vorkehrungen
- Einwilligungen genügen i.d.R. nicht
- Anonymisierung, Aggregierung, Pseudonymisierung
- Verzicht auf sensible Daten
- Grundrechtsschutz durch Verfahren: Treuhänderlösungen, Zertifizierungen
- Dokumentation und Transparenz des Verfahrens und der Datenverarbeitung
- Verbot automatisierter Entscheidungen
- Unabhängige interne und externe Kontrolle
- Effektiver Rechtsschutz

Schlussfolgerungen

- Freiheitlich-demokratische Gesellschaft kann nicht von Algorithmen, sondern muss von Menschen bestimmt werden
- Big-Data-Praxis muss aufgearbeitet und rechtlich eingehegt werden (Rechtsprechung und Gesetzgebung)
- Verfassungskonformes Big Data muss erforscht werden.
- Demokratische Kontrolle durch Transparenz ist unabdingbar.

Big Data für die Big Brothers

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de