Präsenz der deutschen Polizei und zu polizeilichen Ermittlungen in sozialen Netzwerken

Thilo Weichert, Leiter des ULD

Arbeitstagung der bDSB der Bundes- und Länderpolizeien

22. Mai 2014, Kiel

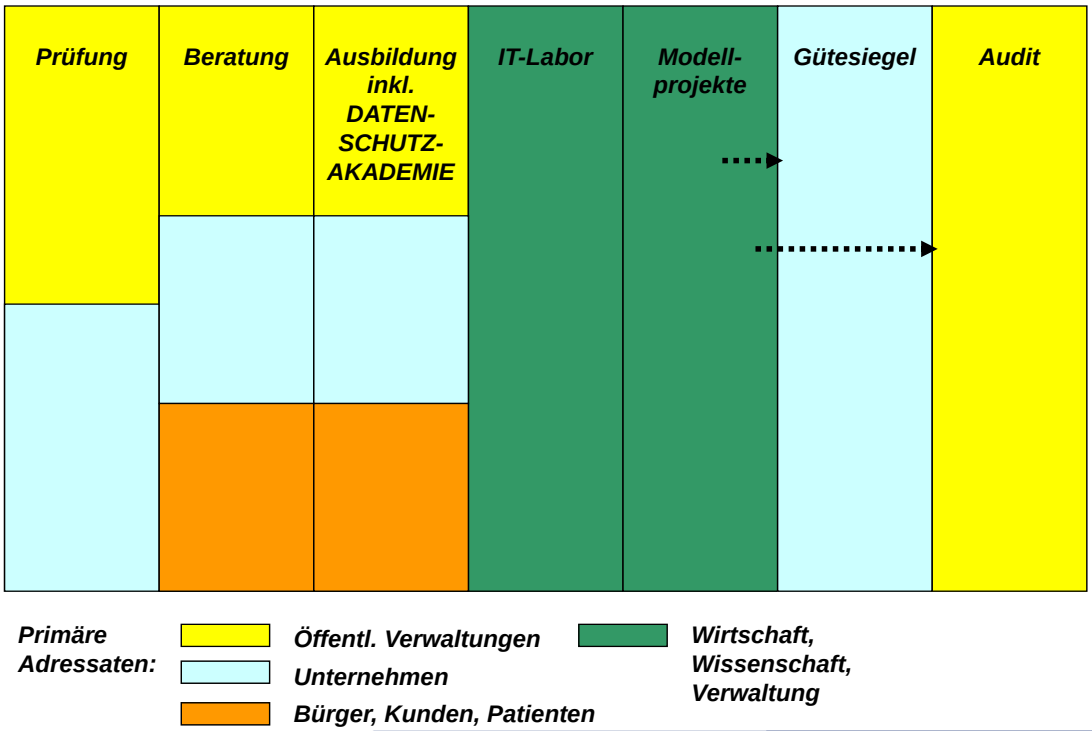
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Polizeilicher Nutzen
- Datenschutz bei sozialen Medien
- Rechtlicher Klärungsbedarf generell
- Öffentlichkeitsfahndung
- Polizei-Apps
- Ermittlungen in Netzwerken
- Big Data
- Schlussfolgerungen und Hinweise

Kurzvorstellung: Was macht das ULD?

Datenschutz und Informationsfreiheit



Polizeilicher Nutzen von sozialen Medien

- Werbung für die Polizei
- Nachwuchsrekrutierung
- Öffentlichkeitsfahndung
- Öffentliche Recherche im Netz
- Verdeckte Recherche im Netz, Ermittlung unter einer Legende, Big Data im Internet

Verfassungsrecht

- Art. 1 I iVm 2 I GG Recht auf informationelle Selbstbestimmung
- Art. 1 I iVm 2 I GG Grundrecht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme
- Art. 10 GG Telekommunikationsgeheimnis
- Art. 13 GG Schutz der Wohnung
- Art. 5 GG Meinungs- und Informationsfreiheit
- Sonstige Grundrechte (z. B. Art. 8, 12, 14 GG)

- Kein Eingriff bei nicht-zielgerichteter Streife im öffentlichen Internet

Generelle Datenschutzprobleme in sozialen Medien

- Einwilligungen sind nach deutschem Recht unwirksam (Facebook, Google), weil nicht informiert, nicht explizit, nicht freiwillig, nicht hinreichend dokumentiert
- Informationspflichten werden missachtet über Datenverarbeitung (im Ausland), über Widerspruchsrechte
- Pseudonyme Nutzung wird oft nicht erlaubt
- Missachtung der Betroffenenrechte (Auskunft, Löschung, Sperrung, Widerspruch)
- Verantwortlichkeiten sind nicht klar (erkennbar)
- Umfassende Profilerstellung durch Portalbetreiber
- (unfreiwillige) Weitergabe an US-Sicherheitsbehörden (z. B. NSA)

Streitige Datenschutzthemen:

- Anwendbarkeit des deutschen Rechtes

Pro: EuGH 13.05.2014 (C-131/12), KG Berlin 24.01.2014 (5 U 42/12), BGH 29.03.2011 (bei Inlandsbezug, VI ZR 111/10)
Kriterien: Wer ist verantwortliche Stelle, Niederlassung, wer ist betroffen (Marktortprinzip)?

Contra: OVG Schleswig 22.04.2013, 4 MB 10/13 u. 11/13: Anwendbar ist ausschließlich irisches Recht

- (Mit-)Verantwortlichkeit der nutzenden Stelle (für Nutzungsdaten)

Pro: ULD, DSB-Konferenz seit 2011

Contra: VG Schleswig 09.10.2013 (8 A 218/11), bald OVG SH

Praktische (Nicht-) Lösung: Hinweis und Link

Öffentlichkeitsfahndung

- §§ 131 ff. StPO grds. anwendbar
- aber Eingriff besonders gravierend: weltweit recherchierbar, Kopierbarkeit (Suchmaschinen-Cache)
- Kommentierungsfunktion unter externer Kontrolle
- hohe Diskriminierungsträchtigkeit und Schadensgefahr von Kommentierungsfunktion (Shitstorm) > 7/24-Überwachung

> Anforderungen:

- Beachtung Verhältnismäßigkeitsgrundsatz (Tatschwere, Nutzen, Risiken)
- Richterliche Anordnung mit präziser Bezeichnung von Art, Umfang u. Dauer
- Sicherung der informationstechnischen Kontrolle

Polizei- Apps

- Notruf
- Aktuelle Geschehnisse, Warnung von Personen (z. B. Sexualtäter)
- Nächste Polizeidienststelle
- Anzeigeerstattung
- App ist Telemediendienst (> TMG anwendbar)
- Bereitstellung in App-Store (in US-Verantwortung)
- Informationspflichten
- Beschränkung der Datenverarbeitung auf Erforderlichkeit (Lokalisierung), ungeklärt: zweckwidrige Nutzung
- Opt-in, Opt-out

Polizeiliche Ermittlungen

- Bei zielgerichteter Datenbeschaffung ist Verhältnismäßigkeitsgrundsatz zu beachten (Generalermächtigung, PolR, StPO) auch unter Pseudonym (Schutz der Ermittler)

Ausnutzung schutzwürdigen Vertrauens:

Vertrauen in Klarnamen? (§ 13 VI TMG vs. US-AGB)

- Generalklausel nicht anwendbar (Beschlagnahme §§ 94 ff. StPO als offene Maßnahme, § 35 StPO)
- Anwendung von § 100a StPO (Inhalts-TKÜ) (-), da Handeln als TK-Partner, nicht laufende Kommunikation
- Anwendung von §§ 110a ff. StPO (Verdeckter Ermittler) evtl., Anordnungsbefugnis beachten

Big Data?

Rechtmäßigkeit

- der Datenerhebung (evtl. Übermittlung)
- der Datenspeicherung (Speicherdauer)
- der Auswertung (Zweckänderung, Abgleich §§ 98a ff. StPO)

Neue Regelungen nötig (z. B. @rtus SH)?

> Verhinderung der Massenüberwachung (skalierende, technikoffene Normen)

> Dokumentation und Kontrollierbarkeit

> Prozedurale Kontrolle (Richtervorbehalt, Anordnungsbefugnis, Kontrolle durch bDSB, evtl. Evaluation)

Schlussfolgerungen

- Bessere personelle und technische Ausstattung der Polizei nötig
- Politischer Diskurs über Sicherheit und digitaler Grundrechtsschutz nötig
- Insbes. Diskurs über Globalität und Einbeziehung Privater nötig
- Modernisierung der gesetzlichen Grundlagen nötig

Nachweise

- Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 http://www.datenschutz.sachsen-anhalt.de/konferenzen/nationale-datenschutzkonferenz/entschliessungen/entschliessungen-der-87-datenschutzkonferenz-27-bis-28-maerz-2014-in-hamburg/oeffentlichkeitsfahndung-mit-hilfe-sozialer-netzwerke/
- Weichert, Facebook, der Datenschutz und die öffentliche Sicherheit, in: Möllers, van Ooyen, Jahrbuch Öffentliche Sicherheit 2012/2013: https://www.datenschutzzentrum.de/facebook/JBOES-2012-2013-Sonderdruck-Weichert.pdf
- ULD, Polizeiliche Recherchen in sozialen Netzwerken zu Zwecken der Gefahrenabwehr und Strafverfolgung, 3/2012https://www.datenschutzzentrum.de/polizei/20120312-polizeiliche-recherche-soziale-netzwerke.pdf

Präsenz der deutschen Polizei und zu polizeilichen Ermittlungen in sozialen Netzwerken

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

https://www.datenschutzzentrum.de