

EU-Beitritt: Eine Schweiz ohne Massenüberwachung?

Eine Reise durch die Grundrechtecharte, der einschlägigen Urteile des EUGH und deren eventuellen Konsequenzen für eine Schweiz in der EU

Über mich

- MLaw UZH, CIPP/E
- ehemaliger Journalist und Strafverfolger
- IT- und Datenschutzjurist in der Finanzindustrie
- LL.M.-Student Universität Maastricht



Thema

Über was wir heute reden

- Europäische Grundrechtecharta
- Vorratsdatenspeicherung
- Kabelaufklärung

...unter der Annahme, die Schweiz wäre Mitgliedsstaat der EU.

Thema

Über was wir heute nicht reden

- Politik
- “klassische” Datenschutzgesetze
- Europäische Menschenrechtskonvention
- Erlasse des Europarats
- Rechtssystem der EU
- Symbolbilder

Vorratsdatenspeicherung



Vorratsdatenspeicherung

Was ist damit gemeint?

- obligatorische Speicherung von Telekommunikationsdaten
- durch Telekommunikationsbetreiber
- für Zwecke der Strafverfolgung oder der nationalen Sicherheit

Vorratsdatenspeicherung

Hintergrund

- Zahlreiche Gesetzgebungsinitiativen in Mitgliedsstaaten nach den terroristischen Angriffen in Madrid (2004) und London (2005)
- Rechtsgrundlage war die ePrivacy Richtlinie 2002/58
- kein homogener Rechtsrahmen über die EU
- deshalb wurde die Richtlinie 2006/24 (Richtlinie über die Vorratsdatenspeicherung) als Harmonisierungsmassnahme verabschiedet
- Richtlinie 2006/24 wurde von Beginn weg kritisiert

«the most privacy intrusive measure ever adopted by the EU in terms of scale and the number of persons it affects»

European Data Protection Supervisor, 2010

Vorratsdatenspeicherung

Hintergrund

- einzelne EU-Mitgliedsstaaten konnten die Richtlinie nicht umsetzen, da es im nationalen Parlament Widerstand gegen das Vorhaben gab
- auch nationale Gerichte haben die Umsetzung verhindert, beispielsweise das Deutsche Verfassungsgericht
- die EU hat gegen die fehlbaren Mitgliedsstaaten Bussen wegen Nichtumsetzung verhängt

Vorratsdatenspeicherung

EUGH-Entscheid *Digital Rights Ireland*

- auch Metadaten können zur Verletzung der Privatsphäre führen
- Bekämpfung von Terrorismus und Kriminalität ist im öffentlichen Interesse
- aber die gewählte Massnahme (Aufbewahrung der Daten und Zugriff für Strafverfolgungsbehörden) ist nicht absolut notwendig
- da die Aufbewahrung nicht beschränkt wird, beispielsweise zeitlich, örtlich oder basierend auf einen Anfangsverdacht, sowie in der Art der Daten
- und der Zugriff auf die Daten ist nicht an prozessuale Bedingungen geknüpft

Richtlinie 2006/24 verstösst gegen Charta der Grundrechte der EU

Vorratsdatenspeicherung

EUGH-Entscheid *Tele2 Sverige*

- nationale Gesetze basierend auf ePrivacy Richtlinie müssen die Bedingungen aus *Digital Rights Ireland* befolgen
- Aufbewahrung und Zugriff muss separat behandelt werden, da die Verletzung der Grundrechte sich nicht erst mit dem Zugriff materialisiert
- Aufbewahrung muss zielgerichtet sein; weiterentwicklung des Urteils *Digital Rights Ireland*
- Zugriff muss vorab von einer unabhängigen Behörde erlaubt werden

Vorratsdatenspeicherung

Lösung “zielgerichtete Aufbewahrung”?

- aber wie kann man Terrorismus oder Verbrechen voraussehen?
- werden damit nicht Vorurteile zementiert?
- was ist mit Massnahmen zur nationalen Sicherheit?

weitere Gerichtsurteile! 

Vorratsdatenspeicherung

EUGH-Entscheide *La Quadrature du Net*

- nationale Sicherheit ist grundsätzlich von der Strafverfolgung zu Unterscheiden (Prävention vs. Untersuchung)
- grundsätzlich ist die nationale Sicherheit Sache der EU-Mitgliedsstaaten
- generelle und unterschiedslose Aufbewahrung im Interesse der nationalen Sicherheit zugelassen, sofern ein **temporärer Notzustand** besteht
- präzisiert “zielgerichtet” und “Eilverfahren”

Vorratsdatenspeicherung

Theorie vs. Realität

- Entscheide sehr Umstritten innerhalb der EU und in Mitgliedsstaaten
- ePrivacy Richtlinie ist in ewiger Überarbeitung und Kritiker versuchen verschiedene Möglichkeiten, die Einschränkungen aufzuheben
- verschiedene Mitgliedsstaaten suchen immer wieder nach Schlupflöchern

Vorratsdatenspeicherung

Fazit der Situation in der EU

- Die EU verlangt für eine Vorratsdatenspeicherung
 - einen Zusammenhang zwischen Zweck und Aufbewahrung
 - zielgerichtete Aufbewahrung, bspw nach Ort, Zeit, Datentyp
 - Zugriff muss einer unabhängigen Vorabprüfung unterliegen
 - Zusammenhang zwischen schwere des Eingriffs und schwere der Tat
 - das Ausklammern von geschützter Kommunikation, z.B. von Anwälten/Ärzten
 - separate Behandlung von Aufbewahrung und Zugriff

Vorratsdatenspeicherung

Situation in der Schweiz

- Die Vorratsdatenspeicherung in der Schweiz nach BÜPF sieht
 - eine verdachtsunabhängige und anlasslose Aufbewahrung aller Randdaten aller Personen in der Schweiz für sechs Monate
 - keine Differenzierung zwischen Datentyp und Schwere der Tat
 - keine Einschränkung des Zugriffs auf schwere Verbrechen
 - keine Vorabprüfung des Gesuchs auf Zugriff
 - beschränktes Ausklammern von geschützter Kommunikation, z.B. von Anwälten/Ärzten

Kabelaufklärung



Kabelaufklärung

Was ist damit gemeint?

- Das NDG erlaubt dem Nachrichtendienst des Bundes die Telekommunikation ins Ausland zu überwachen.
- Provider sind verpflichtet, diese Datenströme an die Schweizer Armee zu liefern.
- Diese durchsucht die Datenströme nach Stichworten und leitet die Resultate an den Nachrichtendienst weiter.
- Ein Überwachungsauftrag muss vom Bundesverwaltungsgericht und der Vorsteherin des VBS bewilligt werden.

Kabelaufklärung

Situation EU

- Eine Kabel- und Funkaufklärung kennt (offiziell) kein EU-Mitgliedsstaat
- EGMR-Entscheid *Big Brother Watch and Others v. the United Kingdom*
- EU-Gesetzgebungsinitiativen gegen Kinderpornographie
- Analoge Anwendung der Urteile bezüglich Vorratsdatenspeicherung?

Kabelaufklärung

EUGH-Entscheide *La Quadrature du Net*

- Ausführungen zur automatisierten **Überwachung von Metadaten** in Echtzeit
- schwerwiegender Eingriff auf Grundrechte, da sich die Überwachung allgemein und unterschiedslos auf alle Daten der Nutzer bezieht und keine Verdachtsmomente vorhanden sind
- die Analyse der Daten darf nicht aufgrund von “sensiblen Daten” geschehen
- jedes positive Ergebnis muss durch nicht-automatisierten Mitteln überprüft werden
- betroffene Personen müssen informiert werden
- gleiche Voraussetzungen wie bei der Vorratsdatenspeicherung sind anwendbar

Kabelaufklärung

Fazit für die Schweiz

- betrifft nicht nur Randdaten, sondern auch Inhalte
- Überwachung wird allgemein und unterschiedslos auf alle Daten der Nutzer ohne Verdachtsmomente angewendet
- gesetzliche Beschränkungen beziehen sich auf den Zugriff
- keine Transparenz darüber, auf welcher Grundlage die Analyse geschieht
- Verwendung und Aufbewahrung der Daten geschieht nicht nach speziellen Kriterien für die Kabelaufklärung
- betroffene Personen müssen nicht in jedem Fall informiert werden

Weitere Themen

Gesetzgebungsvorhaben der EU

- Nutzung von künstlicher Intelligenz in der Strafverfolgung
- Automatische Gesichtserkennungssysteme
- Datenaustausch zwischen Nachrichtendienst und Strafverfolgung, sowie innerhalb der Strafverfolgungsbehörden
- Das Teilen von Fluggastdaten mit ausländischen Behörden
- Aufbewahrungsdauer von personenbezogenen Daten aus der Strafverfolgung

Fragen? 🙋