# Sommerakademie 2010
# Codex digitalis

Infobörse 7

Polizei im Internet

Barbara Körffer

Unabhängiges Landeszentrum für Datenschutz

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein



## *Übersicht*

- Erhebung von Informationen im Internet
- Überwachung verschlüsselter Inhalte
- Auskunftsersuchen an Dritte

# Medienberichte

Vorsitzender des Bundes Deutscher Kriminalbeamter Klaus Jansen:

Staat und Polizei seien derzeit kaum im Internet präsent. Neben rechtlichen Befugnissen fehle qualifiziertes Personal, um Tatorte im Internet sichern zu können. Bei 42 Mio. Internetnutzern in Deutschland und nur 60.000 erfassten Internet-Delikten im vergangenen Jahr sei eine hohe Dunkelziffer von Straftaten zu vermuten. (Heise Online, 23.4.2010)



ULD www.datenschutzzentrum.de

# Medienberichte

stern.de, 16.4.2009

Ermittler heben Kinderporno-Tauschbörse aus

„Das baden-württembergische Landeskriminalamt hob eine Tauschbörse aus, was bundesweite Durchsuchungen nach sich zog. […] Den Angaben zufolge beobachteten die Fahnder die Verbreitung von Filmen über diese Plattform bereits seit Mitte 2008. Dazu sei eine neuartige Software eingesetzt worden. Das […] Computerprogramm ermögliche eine Überwachung rund um die Uhr.“

# Medienberichte

www.news.de, 19.3.2010

## Der neue Internet-Freund trägt Uniform

„So mancher tritt [im Internet, insbesondere in den sozialen Netzwerken] unter falschem Namen auf, wenn er sich Vorteile davon verspricht. Das kann auch die Polizei sein. In den USA gehört die verdeckte Recherche der Ermittler mittlerweile zur Standardrepertoire, wie aus einem internen Papier des FBI hervorgeht.“





# Medienberichte

www.wdr.de, 28.7.2010

## Ermittler durchstöbern das Netz nach Beweisen

„Private Blogs, YouTube, Facebook, Twitter, Kommentare unter Online-Artikeln, Chatkanäle - die Internet-Quellen, in denen die Polizei Hinweise auf Ursachen für die Loveparade-Katastrophe finden könnte, scheinen unerschöpflich.“

# Medienberichte

Spiegel Online, 13.3.2009

Innenminister verließ sich auf falsche Spur im Internet

„Panne im Fall Tim K.: Vom PC daheim habe der Amokläufer seine Taten angekündigt, verkündete Baden-Württembergs Innenminister Rech. Tatsächlich saßen er und einige Staatsanwälte wohl einem Betrüger auf, der das Bild eine Web-Forums fälschte.“





# Informationen im Internet

- Eigene Websites von Internetnutzern
- Einträge auf Websites anderer Nutzer (z.B. Schule, Universität, Arbeitgeber)
- Soziale Netzwerke
- Blogs
- Foren, Chatrooms
- Videoplattformen (z.B. YouTube)
- Auktionen (z.B. ebay)
- Online-Spiele

# Staatliches Interesse an Information

- Aufklärung von Internetkriminalität, d.h. Ermittlung solcher Inhalte, die für sich genommen eine Straftat darstellen oder aus der Begehung einer Straftat gewonnen wurden
- Aufklärung bekannter Straftaten sowohl aus der realen wie aus der virtuellen Welt
- Ermittlung von Informationen über Verdächtige einer Straftat
- Informationsgewinnung zur Vorbereitung besonderer Überwachungsmaßnahmen (WÜ, TKÜ, Einsatz verdeckter Ermittler, Vertrauenspersonen)
- Gefahrenabwehr





# Nutzen der Informationen für polizeiliche Tätigkeit

- Ermittlung von Personalien, Spitznamen, Kontaktdaten
- Ermittlung besonderer körperlicher Merkmale, z.B. Tattoos oder Piercings
- Ermittlung besonderer Vorlieben, Interessen
- Fotos / Videos
- Ermittlung von Aufenthaltsorten
- Benutzte Kraftfahrzeuge
- Alibi-Überprüfungen
- Ermittlung des Umfeldes / Kontaktpersonen

# Erhebung personenbezogener Daten durch Recherche im Internet





## Verfassungsrecht

Grundrechtseingriff nach BVerfG abhängig davon

- ob öffentlich zugängliche Daten erhoben werden oder nicht → kein Grundrechtseingriff
- ob bei Erhebung nicht öffentlich zugänglicher Daten ein schutzwürdiges Vertrauen des Nutzers in die Identität seines Kommunikationspartners ausgenutzt wird
  → Grundrechtseingriff RiS
- ob zugangsgesicherte Inhalte (z.B. passwortgeschützter Bereich eines Forums) unter Nutzung der Zugangsschlüssel ohne oder gegen den Willen der Nutzer erhoben werden → Grundrechtseingriff Art. 10

# Öffentlich zugängliche Daten - 1

BVerfG v. 27.2.2008 (Online-Durchsuchung NRW):

- Kein Eingriff in das Recht auf informationelle Selbstbestimmung, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten.

- Grenze: Gezieltes Zusammentragen und Speichern und Auswerten (ggf. unter Hinzuziehung weiterer Informationen), wenn sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt





# Öffentlich zugängliche Daten - 2

Welche Daten sind öffentlich zugänglich?

Beispiele des BVerfG:

- Aufruf einer allgemein zugänglichen Website im World Wide Web,
- Abonnement einer jedermann offen stehenden Mailingliste,
- Beobachtung eines offenen Chats.

# Öffentlich zugängliche Daten - 3

Nach BVerfG sind öffentlich zugängliche Daten verfassungsrechtlich nicht vor Zugriff durch Dritte geschützt.

Kritik:

- Berücksichtigt nicht etwaige schutzwürdige Interessen der Betroffenen (z.B. Daten wurden ohne deren Kenntnis oder Einverständnis veröffentlicht)
- Entspricht nicht dem europäischen und nationalen Datenschutzrecht





# Öffentlich zugängliche Daten - 4

- Allgemein zugängliche Daten nach dem BDSG (§ 14 Abs. 2 Nr. 5; § 28 Abs. 1 Nr. 3), LDSG SH (§ 11 Abs. 2): Daten, die sich nach ihrer Zielrichtung und Publikationsform dazu eignen, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln.

- Unterliegen nach BDSG und LDSGen dem Gesetzesvorbehalt (z.B. § 14 Abs. 2 Nr. 5, § 28 Abs. 1 Nr. 3, § 29 Abs. 1 Nr. 2 BDSG). Schutzwürdige Interessen des Betroffenen sind zu berücksichtigen.

- Einfachgesetzliche Rechtsgrundlagen für Strafverfolgung und Gefahrenabwehr:
  - §§ 161, 163 StPO
  - § 179 LVwG SH

# Sonderfall: Soziale Netzwerke

- AGB der Betreiber erlauben den Zugang meist nur natürlichen Personen zu privaten Zwecken unter Verwendung der echten Identität. Die Echtheit der Identität wird allerdings nicht überprüft.
- Sind Informationen in sozialen Netzwerken öffentlich zugänglich bzw. allgemein zugängliche Daten nach dem allgemeinen Datenschutzrecht?
  - Dagegen spricht, dass alle Informationen nur registrierten Personen zugänglich sind, die nach den AGB nur natürliche Personen sein dürfen und das Netzwerk nur für private Zwecke nutzen dürfen.
  - Dafür spricht, dass eine Überprüfung der Identität nicht stattfindet, was jedem Nutzer zwangsläufig bekannt sein muss, so dass ein echtes Vertrauen in die Beschränkung auf natürliche Personen nicht entstehen kann.
  - Grenze: Geschützter Bereich
- Ein „Polizeiaccount“ ist mit den AGB der meisten Betreiber nicht vereinbar.
- Nutzung privater Zugänge von Polizeibeamten?





# Nicht öffentlich zugängliche Daten Zugang unter Ausnutzung eines schutzwürdigen Vertrauens - 1

BVerfG v. 27.2.2008 (Online-Durchsuchung NRW):

- Nicht jeder Aufbau einer Kommunikationsbeziehung unter Verwendung einer Legende ist ein Eingriff in das Recht auf informationelle Selbstbestimmung.
- Ein Eingriff liegt erst dann vor, wenn dabei ein schutzwürdiges Vertrauen in die Identität und die Motivation des Kommunikationspartners ausgenutzt wird, um persönliche Daten zu erheben, die ohne dieses Vertrauen nicht zugänglich wären.

# Nicht öffentlich zugängliche Daten Zugang unter Ausnutzung eines schutzwürdigen Vertrauens - 2

Frage: Wann ist das Vertrauen von Internetnutzern in die Identität ihrer Kommunikationspartner schutzwürdig?

- BVerfG: kein schutzwürdiges Vertrauen, wenn keine Überprüfungsmechanismen zur Verfügung stehen
- Welche Anforderungen müssen an die Überprüfungsmechanismen gestellt werden? Identitätsprüfung durch den Anbieter erforderlich oder reicht eine wie auch immer geartete Identifizierungsmöglichkeit durch den Nutzer?





# Nicht öffentlich zugängliche Daten Zugang unter Ausnutzung eines schutzwürdigen Vertrauens - 3

Beurteilung des Vorgangs nach der StPO

- Abgrenzung Verdeckter Ermittler (§ 110a StPO) - nicht offen ermittelnder Polizeibeamter
- Verdeckter Ermittler:
  - auf Dauer angelegte Legende
  - Ermittlungsauftrag geht über einzelne, konkret bestimmte Ermittlungshandlungen hinaus
  - Täuschung einer unbestimmten Vielzahl von Personen über Identität erforderlich
- Voraussetzungen für den Einsatz des verdeckten Ermittlers:
  - bestimmte Straftaten (z.B. Staatsschutz) oder
  - Verbrechen - bei Wiederholungsgefahr oder besonderer Bedeutung der Tat
  - Zustimmung der Staatsanwaltschaft und in bestimmten Fällen des Gerichts

## Zugang zu Kommunikation unter Nutzung besonderer Zugangsschlüssel

BVerfG v. 27.2.2008, Rn. 292 (Online-Durchsuchung NRW):

- Heimliches Aufklären des Internet ist Eingriff in Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG, wenn die überwachende Stelle zugangsgesicherte Kommunikationsinhalte überwacht, indem sie Zugangsschlüssel nutzt, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat.
- Beispiel: Einsatz eines Passworts, das mittels Keylogging erhoben wurde, um Zugang zu einem E-Mail-Postfach oder zu einem geschlossenen Chat zu erlangen.





# Überwachung verschlüsselter Kommunikation

# Quellen-Telekommunikationsüberwachung

- Überwachung der Kommunikation nicht bei der Übertragung, sondern bereits bei Dateneingabe (z.B. durch Keylogger)
- Maßnahme erfordert in der Regel eine Infiltration des informationstechnischen Systems, das zur Kommunikation genutzt wird
- Die Infiltration stellt grundsätzlich einen Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar; es sei denn, die Infiltration kann technisch auf die Überwachung von Telekommunikation beschränkt werden. Ist Letzteres praktisch möglich?
- Daher bedarf es einer speziellen Ermächtigungsnorm, die die besonderen materiellen Voraussetzungen sowie technischen und organisatorischen Vorkehrungen anordnet, die bei Eingriffen in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu beachten sind.





# Auskunftsersuchen an Betreiber von Internetangeboten

# Telekommunikation

- Auskunft über Bestandsdaten von Nutzern
  - § 113 TKG
  - §§ 161, 163 StPO; § 179 LVwG SH
- Auskunft über Verkehrsdaten nach § 96 TKG
  - § 100g StPO; § 185a LVwG SH
  - Keine Pflicht zur Vorratsdatenspeicherung





# Telemedien

- Auskunft über Bestandsdaten von Nutzern
  - § 14 Abs. 2 TMG
  - §§ 161, 163 StPO; § 179 LVwG SH
- Auskunft über Nutzungsdaten nach § 15 TMG
  - § 15 Abs. 5 Satz 4 TMG - Übermittlungsbefugnis für den Telemedienanbieter
  - Erhebungsbefugnis für ersuchende Stelle?
    - §§ 161, 163 StPO; § 179 LVwG SH ausreichend im Hinblick auf die Schwere des Eingriffs?
    - § 100g StPO und § 185a LVwG beziehen sich ausdrücklich nur auf Verkehrsdaten nach § 96 TKG, nicht auf Nutzungsdaten nach § 15 TMG - besondere Regelung nur in § 20m Abs. 2 BKAG

# Inhaltsdaten

- Übermittlungsbefugnis für den Betreiber:
  - § 28 Abs. 2 Nr. 2 Buchst. b BDSG
  - Für Gefahrenabwehr oder Strafverfolgung erforderlich
  - kein überwiegendes schutzwürdiges Interesse des Betroffenen
  - keine Übermittlungspflicht
- Erhebungsbefugnis für die ersuchende Stelle?





# Datensicherheit

- Authentizität der Daten
  - Es muss sichergestellt sein, dass die Daten tatsächlich in vollem Umfang von dem Nutzer stammen
- Integrität der Daten
  - Es muss sichergestellt sein, dass die Daten nicht durch Dritte verändert wurden

# Weiterführende Literatur


- Schulz/Hoffmann, „Grundrechtsrelevanz staatlicher Beobachtungen im Internet“, CR 2010, 131 ff.
- Petri, „Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung““, DuD 2008, 443 ff.
- Henrichs/Wilhelm,“Polizeiliche Ermittlungen in sozialen Netzwerken“, Kriminalistik 2010, 30 ff.
- Hoffmann-Riem, „Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme“, JZ 2008, 1009 ff.
- Hornung, „Ein neues Grundrecht“, CR 2008, 299 ff.






# Vielen Dank für Ihre Aufmerksamkeit


Barbara Körffer

Unabhängiges Landeszentrum für Datenschutz

Schleswig-Holstein

uld5@datenschutzzentrum.de

www.datenschutzzentrum.de