
1718/J XXIII. GP

Eingelangt am 31.10.2007

Dieser Text ist elektronisch textinterpretiert. Abweichungen vom Original sind möglich.

Anfrage

Der Angeordneten Mag. Maier

und GenossInnen

an die Bundesministerin für Justiz

betreffend „Data Mining bei der Vorratsdatenspeicherung - ETSI Standards?“

Das **European Telecommunications Standards Institute (ETSI)** hat laut einem ORF-Bericht (futurezone.orf.at) erste Entwürfe für eine Normierung der Vorhaltung von Verbindungs- und Standortdaten entwickelt, die ein sehr weitgehendes Schürfen der Sicherheitsbehörden in den Datenbergen ermöglichen sollen. Es handelt sich einerseits um ein „Pflichtenheft“ sowie andererseits um die davon abgeleiteten technischen „Standards“.

„Vorgesehen ist demnach, dass die umfangreichen Informationshappen aus der Vorratsdatenspeicherung samt dem Einsatz unvollständiger Suchbegriffe und frei definierter Stichwörter in Form so genannter Wildcards durchforstet werden könnten. Die technischen Vorgaben würden damit über die in zahlreichen europäischen Ländern gesetzlich erlaubten Regelungen zur Auswertung der elektronischen Nutzer Spuren, die von den Providern künftig europaweit sechs bis 24 Monate lang zu archivieren sind, deutlich hinausgehen und die Befürchtungen von Datenschützern für einen vorgezeichneten Missbrauch der Informationshalden bestätigen.“ (heise online news vom 25.09.2007)

Es handelt sich laut ORF um technische Normen für flächendeckendes Data-Mining in Telefonie-Verkehrsdaten, die im Zuge der "Vorratsdatenspeicherung" gesammelt werden.

Im einleitenden Absatz über den Geltungsbereich des Pflichtenhefts zur Vorratsdatenspeicherung heißt es wörtlich: "Es enthält ein Set von Anforderungen zu Übergabeschnittstellen für zurückgehaltene Verkehrs- und Stammdaten von Strafverfolgern und anderen zur Anfrage ermächtigten Behörden."

Das ist ein Novum. In allen seit 1996 erstellten ETSI-"Pflichtenheften" zum Thema Telekomüberwachung - die zum Teil vom selben Berichterstatter stammen - ist dieselbe Passage durchwegs konkreter formuliert. Statt "und anderen zur Anfrage ermächtigten Behörden" hieß es da stets und stereotyp "und Agenturen für Staatssicherheit".

ORF- futurezone (Auszug)

„Zwei interne ETSI-Dokumente, die ORF.at vorliegen, demonstrieren sehr anschaulich, wie der Überwachungsstaat "demokratischer" Prägung in naher Zukunft aussehen wird.

Beide Dokumente betreffen die Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung [Data-Retention] von 2006.

"Zurückgehaltene Daten "

Wie bei den längst in alle europäischen Telefonnetze integrierten ETSI-Standards zur Live-Überwachung von Telefon und Internet sind zwei Grundelemente vorhanden: ein "Anforderungen der Strafverfolger für den Umgang mit zurückgehaltenen Daten" genanntes "Pflichtenheft" sowie die davon abgeleiteten technischen Standards.

Der erste, in Version 0.4 vorliegende Standardentwurf trägt den harmlos klingenden Titel "Übergabe-Schnittstelle für Anfrage und Lieferung zurückgehaltener Daten". Der Inhalt beider Dokumente aber hat mit rechtsstaatlichem Denken europäischer Prägung etwa so viel gemein, wie die DDR-Staatssicherheit mit Freiheit und Demokratie am Hut hatte.

"Polizeistaat" als Untertreibung.

Nicht einmal das Epithet "polizeistaatlich" ist angebracht, da es schlicht eine Untertreibung wäre: Beide Papiere haben Geheimdienstmitarbeiter als Autoren.

Das Pflichtenheft stammt vom niederländischen Geheimdienst PIDS [Platform Interceptie, Decryptie en Signaalanalyse], der Standardentwurf selbst wurde federführend vom britischen Geheimdienst MI5 verfasst.

Normiertes Data-Mining

Ihr Inhalt ist dergestalt, dass einem Verfassungsrichter die Haare zu Berge stehen müssten. Der kommende ETSI-Standard schreibt genau das fest, was Datenschützer stets befürchtet und die damit befassten Politiker - egal welcher Partei - stets bestritten haben.

Es handelt sich dabei um die technische Standardisierung von Data-Mining in den Verkehrsdaten

aller Telefonieteilnehmer. Das bedeutet: In naher Zukunft können normierte Vollsuchen samt dem Einsatz von "Wildcards" über den gesamten Datenbestand von Telekommunikationsverkehrsdaten gefahren werden.

Nicht nur in Österreich, sondern in praktisch allen EU-Staaten ist eine derartige Vorgangsweise illegal, das wussten auch die Verfasser des Standardentwurfs. Formuliert haben sie es entsprechend euphemistisch. "Nicht notwendigerweise in allen Jurisdiktionen legal" bedeutet: Es ist praktisch überall in Europa de lege momentan [noch] illegal.

Legal, illegal

"Die Anfragenstruktur, definiert in Sektion 7.5.1, erlaubt ein breites Spektrum von Anfragen. Einige der Anfragen, die unter dieser Struktur möglich sind, werden nicht notwendigerweise in allen Jurisdiktionen legal sein ... Das Ziel des vorliegenden Dokuments ist es, eine Struktur zu definieren, die technisch ein breites Spektrum von Anfragen zulässt. Bloß weil eine Anfrage im Rahmen von 7.5.1 möglich ist, bedeutet das nicht, dass sie auch automatisch legal ist. Es ist nationale Angelegenheit zu definieren, ob eine Anfrage legal und angemessen ist oder nicht."
[Handover interface for the request and delivery of retained data, v0.4, Abschnitt 7.5.2]

Das heißt:

Es wird ein umfassendes technisches Regelwerk als Norm vorgegeben, das allen Vorstellungen von europäischer Rechtsstaatlichkeit und bestehenden Gesetzen quer durch Europa offen widerspricht.

Einschränkungen durch nationale Legislaturen sind als die Ausnahme der kommenden ETSI-Norm definiert.

Die Anfragen

Im Pflichtenheft wiederum werden die Arten der Anfragen so definiert:

1] Eine Einzelanfrage basierend auf einem einzigen Anfragekriterium

2] Multiple Anfragen basierend auf aggregierten Einzelanfragen

3] Anfragen, die auf einer Reihe von Anfragekriterien basieren

4] Assoziierte Anfragen

[Requirements of Law Enforcement Agencies for handling Retained Data, v0.2.1, Abschnitt 4.3e]

Wildcards

Während Punkt eins, eng ausgelegt, noch in den Rahmen bestehender Gesetze fallen kann, sind

die übrigen Punkte in Deutschland und Österreich klar illegal.

Normiert werden sie trotzdem, das korrespondierende Standarddokument erwähnt sogar Suchmöglichkeiten mit "Wildcards", also völlig willkürlich definierte Suchen über die gesamte Datenbank.

Verkehrsdatenanalyse

Durch die Analyse der Verkehrsdaten - wer mit wem wann wo kommuniziert hat - lassen sich nicht nur komplette Personenprofile erstellen, sie ermöglicht auch die Erfassung von Gruppenkommunikation. Die Auswertungsmethoden und -programme sind mittlerweile dermaßen verfeinert, dass eine Person durch eine Kommunikationsanalyse ihrer Verkehrsdaten gleichsam nackt ausgezogen wird.

Die Ausnahme: Personen und Gruppen, die sich dessen bewusst sind, können sich der Auswertung durch eine ganze Anzahl von Tricks weitgehend entziehen. Dazu gehört etwa der periodische Wechsel von SIM-Karte, Handy und Netzbetreiber, wie ihn Kriminelle längst betreiben.

Verisign, FBI

Zu den Sponsoren und aktiven Beiträgern dieses ETSI-Standards gehört neben dem deutschen Bundesamt für Verfassungsschutz auch die mit dem militärisch-elektronischen Komplex der USA eng verbundene Firma Verisign.

Die wiederum wird im ETSI unter anderem durch einen hochrangigen Ex-FBI-Mann repräsentiert, der davor für die Umsetzung der Telefonüberwachung in den USA zuständig war.

Die Israelis

Weitere Sponsoren der Vorratsdatenschnittstelle sind die israelischen Telekom-Überwachungsspezialisten Verint und Nice. Beide Firmen sind im Schatten des militärisch-elektronischen Komplexes Israels groß geworden.

Das sind freilich nur die deklarierten Mitarbeiter von Geheimdiensten und deren Technikausstattern in den beiden einschlägigen Arbeitsgruppen des ETSI.

"Informelle Mitarbeiter"

Wie viele als Telekomtechniker oder Mitarbeiter von Telekomregulationsbehörden getarnte Agenten und "informelle Mitarbeiter" in den beiden Arbeitsgruppen tätig sind, ist nicht bekannt.

Auch ein Beamter des österreichischen Verkehrsministeriums nimmt regelmäßig an den Sitzungen der ETSI-Arbeitsgruppe 3GPP SA LI teil, die sich mit den Überwachungsnormen für Mobilfunknetze und drahtloses Internet befasst.

Den Sekretär dieser Arbeitsgruppe stellt eine Abteilung des britischen Inlandsgeheimdienstes MI5, die auf den vielsagenden Namen "National Technical Assistance" hört."

Aus: <http://futurezone.orf.at/it/stories/223854/>

Die unterzeichneten Abgeordneten richten daher an die Bundesministerin für Justiz nachstehende

Anfrage:

1. Sind Ihnen die im Einleitungstext zit. internen Dokumente des European Telecom Standards Institute (ETSI) bekannt?
2. Wenn ja, wie werden diese vorgeschlagenen Normen seitens des Ressorts beurteilt?
3. Ist es richtig, dass beide Dokumente die Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung betreffen? Wenn nein, was dann?
4. Ist es richtig, dass die darin vorgesehenen technische Normen flächendeckendes Data-Mining bei Telefonie-Verkehrsdaten vorsehen (Verbindungs- und Standortdaten), die im Zuge der Vorratsdatenspeicherung gesammelt werden? Wenn nein, wofür dann?
5. Ist es richtig, dass es sich dabei um die technische Standardisierung von Data-Mining in den Verkehrsdaten aller Telefonieteilnehmer handelt?
6. Wie beurteilen Sie rechtlich die Suchmöglichkeiten mit „Wildcard“ über den gesamten Datenbestand der gespeicherten Telekommunikationsverkehrsdaten?
7. Sehen Sie eine potentielle Missbrauchsgefahr beim Einsatz von Wildcards?
8. Sind Sie auch der Auffassung, dass eine derartige Vorgangsweise (d.h. Datamining in dieser Form) illegal ist, der EMRK, der österreichischen Bundesverfassung, dem DSG und dem TKG widerspricht?

9. In welchen EU-Mitgliedsstaaten wäre zur Zeit diese Vorgangsweise legal und rechtlich möglich?
10. Ist es richtig, dass in ETSI-Dokumenten nationale Regelungen als die **Ausnahme** von der geplanten ETSI-Norm definiert werden? Wenn ja, was bedeutet dies?
11. Wer sind die Mitglieder in dieser ETSI-Arbeitsgruppe, die diese beiden internen Dokumente erarbeitet haben?
12. Wie beurteilen Sie die offensichtlichen Verbindungen zwischen diesem Normierungsgremium und den beiden internen Dokumenten mit der internationalen Geheimdienstszene und Sicherheitsunternehmen?
13. Ist es richtig, dass das Pflichtenheft vom Niederländischen Nachrichtendienst PIDS (Platform Interceptie, Decryptie en Signalanalyse) stammt? Wenn nein, von wem dann?
14. Ist es richtig, dass beim Entwurf über technische Standards der britische Geheimdienst MI 5 mitgearbeitet hat? Wenn nein, von wem dann?
15. Wie viele Mitarbeiter der Geheimdienste arbeiten in diesem ETSI-Normungsgremium überhaupt mit?
16. Nach welchen Kriterien erfolgte überhaupt die Zusammensetzung dieses Gremiums? Wer ist darin vertreten?
17. Welchen Rechtscharakter soll diese zukünftige ETSI-Norm in der EU bzw. in Österreich bekommen?
18. Wie werden Sie in Österreich die Einhaltung von europäischem und österreichischem Recht bei Verabschiedung des nun im Entwurf vorliegenden Pflichtenheftes und den davon abgeleiteten technischen Standards sicherstellen?