

Lawful Interception

<<TableOfContents>>

= Lawful Interception =

Lawful interception (LI) ist das legale Mitschneiden von Internet- oder Telefonverkehr durch "Bedarfsträger" (z.B. Polizeien, [[Datenbank der Dienste|Geheimdienste]], [[Zoll]] usw) zur Strafverfolgung, Gefahrenabwehr oder Aufklärung. In der Regel spricht man von LI nur, wenn Kommunikationsinhalte erfasst werden. [[TK-Verkehrsdaten]], also Daten zu Ort, Zeit und Partnern einer Telekommunikation, sind weniger gut geschützt und werden noch weit ausgiebiger genutzt.

Vgl. auch [[Überwachungstechnik|Überwachungstechnik]]; dort geht es vor allem um Überwachung außerhalb des Telekommunikationsbereichs.

== Standard durch ETSI ==

Die Wikipedia:ETSI (European Telecommunications Standards Institute) ist eine europäische Behörde, welche für alle möglichen technischen Anwendungen im Bereich der Telekommunikation Standards festlegt. Für die [[Abhörschnittstelle]] der europäischen Sicherheitsbehörden legt die Wikipedia:ETSI ebenfalls einheitliche Standards fest. Der Standard zum Abhören ist durch RFC 2804 IETF klassifiziert. Dieses wurde in einem [[Datenbanken EU|EU]]-Ratspapier von 1995 vereinbart. Seit dem 1.1.2005 die müssen auch die Internet- und Emailanbieter die Überwachungsinfrastruktur, wie im [[http://www.heise.de/newsticker/meldung/52954|Heise-Newsticker]] steht, bereitstellen.

- [[http://www.gliif.org/LI_standards/TIIT-v1.0.0.0.pdf|TIIT 1.0.0]] -- Die technische Beschreibung des ETSI Standards zum Abhören (pdf)
- [[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML|EU-Ratspapier von 1995]] -- Beschluss zur Einrichtung eines gemeinsamen Standards
- [[http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-baloo.pdf|Blackhat Präsentation vom Juli 2003 zur Lawfull Interception und dem ETSI-Standard]] (pdf)

Inzwischen gibt es den Europäischen Durchsuchungsbefehl, der die verschiedenen europäischen Polizeien zu gegenseitiger Amtshilfe beim Abhören verpflichtet. Damit müssen die Polizeien auch die Schnüffelergebnisse der jeweils anderen lesen können. Dazu bastelt die ETSI etwas, das freundlich SMILE (Smart Handover Interface between Law Enforcement Agencies) heißt. [[https://digit.site36.net/2017/03/23/project-smile-interface-for-european-telecommunications-interception/|Infos dazu von Matthias Monroy]].

== Überwachungsarten ==

=== Telefonüberwachung ===

Das übliche Abhören von Telefonen wird im Strafverfahren durch §100a/b geregelt und setzt in der Regel schwere Straftaten voraus (129a zählt aber natürlich). Die Maßnahmen müssen gerichtlich angeordnet werden.

Abgehört wird in aller Regel an den großen Vermittlungsstellen der Telekommunikationsunternehmen (im Mobilfunk an den MSCs). Die dort sitzenden Rechner werden aus der Ferne von den Bedarfsträgern bedient, die abgehörten Gespräche normalerweise asynchron (also gesammelt) an die Polizei übertragen. Das System ist so gebaut, dass die Telekoms nicht erfahren (sollen), wer abgehört wird.

Im digitalen Telefonnetz (also mittlerweile durchgehend) gibt es durch Abhören kein Knacken, Rauschen oder Echo -- entsprechende Effekte haben also andere Gründe (umgekehrt bedeutet ihre Abwesenheit natürlich keine Vertraulichkeit).

So richtig gut funktionieren die Abhörschnittstellen aber wohl selbst im digitalen Zeitalter nicht immer. So berichtet <http://annalist.noblogs.org/post/2007/10/03/sicherheitsknoten/> im Zusammenhang mit dem [\[129a Verfahren#mg-Verfahren|mg-Verfahren\]](#):

```
{ { {#!blockquote [Andrej Holm] ruft sich selbst von einem Festnetztelefon an, und erreicht statt seines Handys meine Mailbox. Er ruft daraufhin mich vom selben Festnetztelefon an mit der Bitte, sein Handy anzurufen, was ich auch mache. Und erreiche meine eigene Mailbox, mit der Aufforderung, meine Mailbox-PIN einzugeben, was sonst nur geschieht, wenn ich sie von einem anderen Telefon als meinem Handy anrufe. } } }
```

=== Überwachung in Internetverbindungen ===

Internetprovider sind verpflichtet eine [\[Abhörschnittstelle\]](#) für die Sicherheitsbehörden anzulegen. Diese erlaubt insbesondere die Ausleitung von Internetverkehr nach "Anschluss" (also unabhängig von einer konkret zugewiesenen IP-Adresse) und Dienst.

In einem <http://www.kuechenradio.org/wp/?p=624>|Küchenradio-Interview] hatte der Ex-Terrorverdächtige Soziologe [\[129a Verfahren#mg-Verfahren|Andrej Holm\]](#) erzählt, dass ihre Internetverbindung auf einmal langsamer wurde, nachdem wahrscheinlich mit dem Mitlesen begonnen wurde. ETSI-Black Boxes sollten eigentlich keinen derartigen Effekt bewirken, insofern kann diese Beobachtung als ungeklärt gelten.

In einem <http://www.sueddeutsche.de/politik/iran-ueberwachung-made-in-germany-1.115367>|Artikel in der Süddeutschen Zeitung von 2009] über die Überwachung der Dissidenten im [\[Iran\]](#) wird die Technologie zum Überwachen des Internetverkehrs beschrieben. Dort werden IP-Pakete auch aktiv manipuliert. Die ETSI-Black-Boxes, die in der BRD eingesetzt werden, können das nicht. Das System wurde von Siemens entwickelt.

=== Quellen-TKÜ ===

"Quellen-Telekommunikationsüberwachung" ist ein Propagandabegriff des Sicherheits-Industriellen Komplexes, der suggerieren soll, das heimliche Einbrechen in Rechner der Bürger sei eigentlich nichts anderes als das bekannte heimliche Abhören.

Diese Suggestion ist rechtlich wie technisch unfug und wurde nur ersonnen, um das [\[\[http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html|Verfassungsurteils 1 BvR 370/07, 1 BvR 595/07\]\]](http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html) (27.2.2008) zu umgehen, das eigentlich staatliche Computersabotage stark beschränkt hat.

Material zu Staatstrojanern, unter welcher Flagge auch immer, gehört nach [\[\[Staatstrojaner\]\]](#).

=== Weiteres ===

==== Stille SMS und Funkzellenauswertung ====

vgl [\[\[TK-Verkehrsdaten#Stille_SMS\]\]](#) und [\[\[TK-Verkehrsdaten#Funkzellenauswertung\]\]](#)

==== Direktes Abhören von GSM-Verbindungen ====

Die Verschlüsselung auf der Luftschnittstelle von Wikipedia:GSM kann inzwischen als gebrochen angesehen werden, gehört aber nicht zu Lawful Interception, sondern zur Grauzone der [\[\[Überwachungstechnik\]\]](#).

vgl [\[\[Überwachungstechnik#Direktes_Abhören_von_GSM-Verbindungen\]\]](#)

== Statistik zum Abhören ==

[\[\[http://www.bundesjustizamt.de/cln_108/nn_1629916/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/Telekommunikationsueberwachung__node.html?__nnn=true|Schöne Daten\]\]](http://www.bundesjustizamt.de/cln_108/nn_1629916/DE/Themen/Justizstatistik/Telekommunikationsueberwachung/Telekommunikationsueberwachung__node.html?__nnn=true) gibts derzeit (2011) beim Bundesjustizamt. Für den Fall, dass sich das bewegen sollte, mal google nach "Die Telefonüberwachungsstatistik enthält die Anzahl der nach den Mitteilungen der Landesjustizverwaltungen" fragen. TODO: Den Kram mal auswerten und aufbereiten.

2003: Aus der [\[\[http://dip.bundestag.de/btd/15/040/1504011.pdf|Drucksache 15/4011\]\]](http://dip.bundestag.de/btd/15/040/1504011.pdf) des Bundestages (S. 5) geht hervor: Für polizeiliche Überwachungsmaßnahmen (incl. Staatsschutz): Verwendung in 4276 Verfahren, bei denen 24501 Einzelanordnungen neu erlassen und 4937 verlängert wurden (2002: 26177 Anordnungen insgesamt). Betroffen waren 34317 Kennungen (2002: 30478). Der Löwenanteil davon (28314) waren Mobiltelefone. Betroffen waren 10439 Personen.

Aus dem Politbereich waren 19 Verfahren mit Abhören im Bereich Friedens- und Hochverrat, 115 Straftaten gegen die öffentliche Ordnung, und 260 Straftaten nach Ausländer- und Asylgesetz. Der größte Teil der Verfahren (2664) war im Bereich Betäubungsmittel (BTM).

Überwachungen durch Verfassungsschutz oder BND sind hier natürlich nicht enthalten.

Der LfD Ba-Wü spricht [\[\[http://www.baden-wuerttemberg.datenschutz.de/lfd/tb/2005/tb-2.htm|2005\]\]](http://www.baden-wuerttemberg.datenschutz.de/lfd/tb/2005/tb-2.htm) davon, die Zahl der überwachten Anschlüsse sei von 3730 im Jahr 1994 auf 19896 im Jahre 2001 gestiegen. Dabei habe es nur in 17% der Fälle mit Telefonüberwachung Ermittlungserfolge gegeben, die auf die Ursache der Überwachung bezogen waren.

Christiane Schulzki-Haddouti spricht von [\[\[http://www.heise.de/ct/03/12/048/default.shtml|31 Millionen\]\]](http://www.heise.de/ct/03/12/048/default.shtml) abgehörten Gesprächen für 2002, diesmal in 3981 Anordnungen im Festnetz und 17888 Anordnungen im Mobilnetz. Diese Angaben müssen sich nicht ausschließen, da zu einer Maßnahme mehrere Anordnungen gehören können.

Zu 2005 gibt [\[\[http://dip.bundestag.de/btd/16/030/1603054.pdf|BT-Drucksache 16/3054\]\]](http://dip.bundestag.de/btd/16/030/1603054.pdf) Auskunft: 4925 Verfahren mit 12606 Betroffenen, 49226 Kennungen (etwa +25% gegenüber 2004). Bei Mail Anstieg von 63 auf 279 (+342%), bei Internetzugängen von 92 auf 193 (+110%). Ein politischer Hintergrund dürfte bei etwa 300 (ca. 6%) zu vermuten sein.

Eine Vorstellung, wie sich die Zahl der Verfahren in Betroffene und Gespräche übersetzt, geben [\[\[http://www.heise.de/newsticker/1-1-Millionen-Telefonate-in-Berlin-abgehoeert--meldung/134735|Zahlen aus Berlin\]\]](http://www.heise.de/newsticker/1-1-Millionen-Telefonate-in-Berlin-abgehoeert--meldung/134735): Dort hatte es 2008 157 Verfahren mit Lawful Interception gegeben, in deren Gefolge 1052 Anschlüsse von 511 Personen überwacht wurden. Insgesamt wurden 1.1 Millionen Telefonate abgehört. Die Zahl von 7000 Gesprächen pro Verfahren scheint etwas hoch, dürfte aber die Größenordnung treffen. Mit denen Zahlen von 2005 wären dann bundesweit mehr als 40000000 abgehörte Gespräche zu erwarten, was ganz gut zu Schulzki-Haddoutis Schätzung oben passt.

<<Doclink(2006-BfDI-TB21.pdf,21. TB BfDI (2006))>> zählt die Anordnungen:

||2003||24441|| ||2004||29018|| ||2005||35015||

=== Statistik des BMJ zum Abhören ===

[\[\[http://www.bmj.bund.de/enid/82ce200cb5fc066479a43879d3a90106,0/Statistiken/Telefonueberwachung_z2.html|Statistiken vom BMJ zum Telefonabhören\]\]](http://www.bmj.bund.de/enid/82ce200cb5fc066479a43879d3a90106,0/Statistiken/Telefonueberwachung_z2.html)

Version #1

Erstellt: 2025-10-27 22:44:14 UTC von Datenschmutz Migration Bot

Zuletzt aktualisiert: 2025-10-27 22:44:14 UTC von Datenschmutz Migration Bot