KANTON LUZERN

Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt “Telefonüberwachung“

1. Zweck des Merkblattes

Grundsätzlich geht man in demokratischen Gesellschaften davon aus, dass Telefongespräche zum Privatbereich zählen und deshalb nicht überwacht werden sollen. Andererseits hat der Staat zum Zweck der Strafverfolgung oftmals ein Interesse daran, gerade diese privaten Informationen von einzelnen Personen zu kennen und setzt dazu die Telefonüberwachung ein.

Dass tatsächlich überwacht wird, ist immer wieder den Medien zu entnehmen. Zum Zeitpunkt der Erstellung dieses Merkblattes sind die Fälle der Abhörung der US-Bürger durch die NSA, der Skandal der Bespitzelung von Deutschen Journalisten durch den BND und die Affäre um die Bespitzelung des französischen Innenministers Sarkozy in den Medien. In diesen Fällen geht es um die höchstwahrscheinlich missbräuchliche Abhörung von Personen. In der Regel findet die Belauschung allerdings gesetzeskonform statt.

Für die Bürger ist es kaum zu erkennen, wie häufig dieses Instrument eingesetzt wird, wer es einsetzt und unter welchen Voraussetzungen es eingesetzt werden darf. Dieses Merkblatt soll die rechtliche Situation erläutern, einige statistische Angaben zum tatsächlichen Umfang des Einsatzes der Telefonüberwachung geben und so einen genaueren Überblick über die Telefonüberwachung liefern.

Nicht Thema dieses Merkblattes sind andere Überwachungsarten wie Überwachung des Internet, des E-Mail-Verkehrs, die Lokalisierung von Mobiltelefonen, die Installation von Wanzen usw.

Ebenfalls nicht Thema dieses Merkblattes ist die Telefonüberwachung am Arbeitsplatz[1] und die Aufzeichnung von Telefongesprächen im Geschäftsverkehr[2].

2. Die rechtliche Situation

Das Fernmeldegeheimnis wird in der Bundesverfassung in Art. 13 ausdrücklich garantiert. Dort heisst es im ersten Absatz:

[1] Hierzu hat jedoch der Eidgenössische Datenschutzbeauftragte ein Merkblatt verfasst: http://www.edsb.ch/d/themen/weitere/telefonueberwachung_d.pdf.
[2] Hierzu hat der Eidgenössische Datenschutzbeauftragte einige Informationen auf seiner Webseite veröffentlicht: http://www.edsb.ch/d/themen/weitere/aufzeichnung-telefongespraeche.htm.

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

Wie bei allen Grundrechten sind allerdings Ausnahmen möglich, wenn es ein entsprechendes Gesetz gibt, das gewissen Bedingungen standhält. Im Fall der Telefonüberwachung ist dieses Gesetz das Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1). Die Bedingungen für die Durchführung einer Überwachung sind gemäss Art. 3 BÜPF grundsätzlich:

- Ein dringender Tatverdacht muss sich auf einen der ca. 70 Straftatbestände beziehen, die in Art. 3 BÜPF aufgelistet werden. Die zu überwachende Person hat gemäss dem Verdacht die strafbare Handlung entweder selbst begangen oder war daran beteiligt.
- Andere Untersuchungshandlungen sind erfolglos geblieben, oder die Ermittlungen wären ohne die Überwachung aussichtslos oder unverhältnismässig erschwert.
- Es wurde ein Strafverfahren eröffnet, d.h. ein blosses polizeiliches Ermittlungsverfahren genügt nicht.

Darüber hinaus sind weitere Überwachungen zulässig, wie beispielsweise die Überwachung von Drittpersonen, wenn davon auszugehen ist, dass eine straffällige Person den Telefonanschluss der Drittperson verwendet.

Der Wunsch zur Überwachung kann von Bundes- oder kantonalen Strafverfolgungsbehörden, in der Regel einem Untersuchungsrichter oder einer Untersuchungsrichterin, ausgehen[3]. Am häufigsten dürfte die Initiative von den kantonalen Polizeistellen ausgehen. Deshalb sind zwar die Kantone in den Ablauf und die Möglichkeiten der Überwachung integriert, weil es sich aber beim BÜPF um ein Bundesgesetz handelt, fällt seine Einhaltung aus Sicht des Datenschutzes nicht in die Zuständigkeit des kantonalen Datenschutzbeauftragten.

Die anordnende Behörde hat die Überwachungsanordnung und die Begründung samt der für die Genehmigung wesentlichen Strafverfahrensakten innert 24 Stunden der Genehmigungsbehörde einzureichen.

Die Genehmigungsbehörde ist zwingend eine richterliche Behörde. Die Befugnisse der Genehmigungsbehörde richten sich wiederum nach dem BÜPF[4]. Die genehmigte Überwachungsanordnung wird an den Dienst für besondere Aufgaben (DBA), der dem UVEK administrativ unterstellt ist, weitergeleitet. Dieser erteilt der Anbieterin von Fernmeldediensten Anweisungen darüber, wie die Überwachung durchzuführen ist. Auch interne Fernmeldenetze und Hauszentralen dürfen überwacht werden. Der DBA nimmt ausserdem den umgeleiteten Fernmeldeverkehr entgegen gibt entsprechende Dokumente und Datenträger an die anordnende Behörde zurück. Ausserdem sorgt er für die Durchführung von Direktschaltungen. Bei einer Direktschaltung wird der überwachte Verkehr nicht vom DBA entgegengenommen, sondern direkt zum zuständigen Polizeikorps weitergeleitet und dort aufgezeichnet. Die Direktschaltung stellt in der heutigen Praxis den Regelfall dar, sie ist aber bei Überwachungsmassnahmen von Personen, die Träger eines Berufsgeheimnisses sind, ausdrücklich verboten. Ausserdem dürfen Berufsgeheimnisträger nur überwacht werden, wenn davon auszugehen ist, dass sie selbst eine Straftat begangen haben[5].

[3] Eine Auflistung der Behörden, von denen die Überwachungsmassnahme ausgehen kann, findet sich in Art. 6 BÜPF.
[4] Vgl. Art. 3,4,7,8,9,10,14 BÜPF.
[5] Vgl. Art. 4 Abs. 3 BÜPF.

Die Überwachung muss beendet werden, wenn sie für die weiteren Ermittlungen nicht mehr notwendig ist oder wenn die Genehmigung oder Verlängerung verweigert wurde[6].

Die Überwachungsmassnahme ist der verdächtigen Person (resp. der Drittperson), deren Fernmeldeanschluss überwacht wird, mitzuteilen[7]. Verlangt ist, dass spätestens vor Abschluss der Strafuntersuchung oder Einstellung des Verfahrens der Grund, die Art und Dauer der Überwachung mitgeteilt worden ist. Allerdings kann die Mitteilung über eine durchgeführte Überwachung hinausgeschoben werden oder sogar unterbleiben, wenn die Genehmigungsbehörde zustimmt.

Vom Zeitpunkt der Mitteilung an beginnt die Rechtsmittelfrist zu laufen. Die betroffene Person kann innerhalb von 30 Tagen ab Erhalt der Mitteilung wegen fehlender Rechtmässigkeit oder Verhältnismässigkeit der Überwachung Beschwerde erheben[8].

3. Wer kann Telefongespräche überwachen?

Die Abhörmassnahmen werden grundsätzlich durch den DBA oder bei Direktschaltungen durch die Bundes- oder kantonalen Polizeiorgane durchgeführt, wobei diese die Fernmeldedienstanbieter zur Mithilfe heranziehen. Ausserhalb des Bereichs des BÜPF ist es denkbar, dass Telefongespräche durch ausländische Geheimdienste mitgehört werden. Inländischen Geheimdiensten, insbesondere dem Dienst für Analyse und Prävention (DAP), ist die Überwachung des Fernmeldeverkehrs hingegen bisher nicht erlaubt.

4. Überwachung der Mobiltelefonie

Das GSM-Netz (Natel D) galt anfangs als abhörsicher, weil die digitalen Daten hier verschlüsselt übertragen werden können. Allerdings ist diese Verschlüsselung angreifbar und stellt seit längerem kein Hindernis für die Telefonüberwachung mehr dar.

5. Umfang der Überwachung in der Schweiz

Die Tendenz der Anzahl der Überwachungsmassnahmen (aktive und rückwirkende Massnahmen zusammengefasst) in den letzten Jahren war stark steigend. Im Jahr 1998 waren es insgesamt 4089 Massnahmen, 2002 bereits 6446 Massnahmen und 2005 6924 Massnahmen[9]. Immerhin ist die Anzahl der Überwachungsmassnahmen von 2004 bis 2005 nur geringfügig angestiegen und auf das Jahr 2006 sogar leicht zurückgegangen, nämlich auf 6322 Massnahmen. Es besteht also immerhin Anlass zur Hoffnung, dass die Anzahl der Überwachungsmassnahmen nicht weiterhin dramatisch ansteigt.

Im internationalen Vergleich dürfte die Schweiz damit in der Zahl der Überwachungen relativ zur Bevölkerungsgrösse an der Spitze liegen. In Deutschland, das in der EU als Spitzenreiter in Sachen Telefonüberwachung gilt, wurden im Jahre 2005 42'508 Überwachungsmassnahmen genehmigt. Die Deutsche Bevölkerung ist allerdings mehr als zehn Mal so gross wie die Schweizerische Bevölkerung, so dass in der Schweiz relativ zur Bevölkerungsgrösse mehr Überwachungen durchgeführt wurden.

[6] Vgl. Art. 10 Abs. 1 BÜPF.
[7] Vgl. Art. 10 Abs. 2-4 BÜPF.
[8] Vgl. Art. 10 Abs. 5-6 BÜPF.
[9] Quelle: http://www.uvek.admin.ch/themen/kommunikation/00690/00691/00692/index.html?lang=de

6. Gegenmassnahmen

Das Ausweichen auf die von den Internetprovidern angebotene Telefonie über das Internet mit Voice over IP (VoIP) ist keine abhörsichere Alternative zur gewöhnlichen Telefonie, weil auch der Internetverkehr überwacht werden kann. Immerhin ist es bei Verwendung des eigenen PCs zur Internettelefonie[10] möglich, das übermittelte Gespräch so zu verschlüsseln[11], dass es auch von den Behörden nicht entschlüsselt werden kann. Aus diesem Grund gehen die Strafverfolgungsbehörden nun den Weg, Spionageprogramme auf den Computern der zu überwachenden Person zu installieren[12]. Die rechtliche Grundlage dafür ist momentan nicht vorhanden. Mit diesen Spionageprogrammen können die in das Mikrofon gesprochenen Wörter belauscht werden, bevor sie verschlüsselt werden. Auch ist es mit solcher Software technisch möglich, das Computermikrofon oder die Webcam für die Überwachung des Raumes, in dem der Computer steht, einzusetzen. Man kann damit natürlich auch alle Benutzereingaben über die Tastatur, beispielsweise beim Verfassen von E-Mails, mitlesen. Wer sicher sein möchte, dass der eigene Computer nicht zum Spion geworden ist, muss daher entweder den Computer von einer CD/DVD booten[13] oder ein Betriebssystem einsetzen, für das es diese Software nicht gibt. Gemäss vorliegenden Informationen existiert diese Software für Windows, MacOS und Linux.

Erschwert wird die Belauschung durch die Kommunikation in Internet-Cafes ohne Identifizierung, durch das Verwenden von mobilen Internetanschlüssen, die Verwendung von WLAN-Hotspots ohne Benutzerauthentifizierung und das Wechseln der Kommunikationskanäle (Chatroom, E-Mail, Telefon, Instant Messaging).

Es existieren Mobiltelefone[14], mit denen sicher verschlüsselte Verbindungen aufgebaut werden können. Dazu müssen allerdings beide Gesprächspartner ein derartiges Gerät besitzen.

7. Ausblick

Mit dem Entwurf der Bundespolizei fedpol des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 31.01.2006 soll der Dienst für Analyse und Prävention (DAP) unter anderem neu die Möglichkeit erhalten, den Fernmeldeverkehr abzuhören, sofern „konkrete und aktuelle Tatsachen oder Vorkommnisse vermuten lassen, dass er diese Kommunikationsmittel dazu benutzt, seinen Zwecken dienliche Sendungen oder Mitteilungen entgegenzunehmen oder weiterzugeben“[15]. Auch hier könnten die Anschlüsse Dritter überwacht werden und nach diesem Gesetzesentwurf dürften sogar

[10] Beispielsweise Ekiga, OpenWengo, Gizmo oder Skype.
[11] Für die Software Skype wird beispielsweise angegeben, dass der Verschlüsselungsalgorithmus AES mit einer Schlüsselstärke von 256 bit eingesetzt wird. Damit wäre ein Abhörversuch durch den DBA höchstwahrscheinlich zum Scheitern verurteilt. Die Sicherheit von Skype ist allerdings noch Gegenstand von Diskussionen unter Sicherheitsexperten. Auch lässt sich wegen dem nicht einsehbaren Source-Code dieser Software nicht prüfen, ob Hintertüren für Regierungsorganisationen in den USA oder in anderen Staate bestehen. Sicherer dürfte beispielsweise Zfone von Phil Zimmermann sein: http://www.philzimmermann.com.
[12] Dieses Vorgehen wurde durch einen Artikel der SonntagsZeitung aufgedeckt und wird von den Strafverfolgungsbehörden bestätigt. Vgl. http://www.files-planet.ch/content/view/21/2/
[13] Beispielsweise gibt es viele sog. Live-CDs von Linux-Distributionen, beispielsweise: http://www.knopper.net/knoppix/
[14] Hersteller sind beispielsweise InfoGuard oder Rohde&Schwarz.
[15] Vgl. Art. 18l Überwachung des Post- und Fernmeldeverkehrs des Vorentwurfs fedpol vom 31.01.2006.

Anwälte, Ärzte und andere dem Berufsgeheimnis unterstehende Personen überwacht werden.

8. Kritische Beurteilung

Die Überwachung von Telefongesprächen stellt einen massiven Eingriff in die Privatsphäre und damit in auf Verfassungsstufe geschützte Rechte dar.. Dieser massive Eingriff ist bei einigen schweren Straftaten zwar gerechtfertigt. Der ausufernde, nicht auf Effizienz hin geprüfte und zunehmende Gebrauch dieses Mittels der Strafverfolgungsbehörden ist jedoch bedenklich. Mit den Worten von Benjamin Franklin: “Wer essentielle Freiheiten der zeitweiligen Sicherheit opfert, hat weder Freiheit noch Sicherheit verdient”[16].

9. Fragen und Informationen

Für Fragen und weitere Informationen stehen Ihnen die Datenschutzbeauftragten gerne zur Verfügung.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	+ 41 41 228 66 06
Fax:	+ 41 41 228 69 13
E-Mail:	dsb@lu.ch **WARNUNG**: Der E-Mail-Verkehr ist unsicher. Vertrauliches gehört deshalb nicht in E-Mails!
Internet:	http://www.datenschutz.lu.ch

Luzern, Juni 2006, Update Februar 2007

[16] In der Originalsprache: Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety.