BÜPF und Nachrichtendienstgesetz: Eine Betrachtung aus Grund- & Menschenrechtssicht

Gesetzesrevision I: BÜPF/StPO

*Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) regelt die Pflichten der Provider und die Aufgaben des Dienst ÜPF. Die Eidgenössische Strafprozessordnung (StPO) räumt den Behörden strafprozessuale Zwangsmassnahmen und damit den Zugriff auf die Kommunikationsdaten ein. Die beiden Gesetzen regeln die **Strafverfolgung** durch die Polizeibehörden im Rahmen von rechtsstaatlichen Strafverfahren mit Verteidigung und Recht auf Akteneinsicht durch die Betroffenen.*

Die **Vorratsdatenspeicherung** («Rückwirkende» Überwachung) und der damit mögliche **Antennensuchlauf** (Rasterfahndung) sind **unverhältnismässig**, da alle Menschen unterschiedslos betroffen sind. Eine entsprechende Beschwerde der Digitalen Gesellschaft ist am Bundesverwaltungsgericht hängig.

Der persönliche Geltungsbereich wird auf reine Diensteanbieter, Hostingprovider, Hotels, Spitäler, Schulen, Chatanbieter und selbst Vereine und Private, die ihr WLAN den Nachbarn zur Verfügung stellen, ausgeweitet. Die **private Mithilfe an der Strafverfolgung ist heikel**, da für die Beteiligten unklar ist, wen die Überwachung Betrifft (Familienmitglied, Arbeitskollegin, sich selber?).

Mit **Staatstrojanern** (Zugriff auf «Telekommunikationsdaten») lassen sich **keine forensisch gesicherten Beweise** erheben. Da technisch nicht verhindert werden kann, dass auf das ganze Gerät und dessen Sensoren zugegriffen werden kann, ist zudem der Kernbereich privater Lebensführung von einem Eingriff bedroht. Das **Recht auf (digitale) Intimsphäre gehört jedoch zum unantastbaren Bereich privater Lebensgestaltung**, das dem staatlichen Zugriff weitgehend verschlossen ist.

Mit **IMSI-Catchern** können nicht nur lokale Telefongespräche abhört werden, es lassen sich auch **unsichtbare Ausweiskontrollen** durch «Einfangen» von Mobiltelefonen durchführen.

Gesetzesrevision II: Nachrichtendienstgesetz

*Das neue Nachrichtendienstgesetz regelt die «präventive» Überwachung ohne konkreten Verdacht auf eine Straftat durch den **Geheimdienst**.*

Für die Verfolgung von Straftaten oder die Ermittlung bei einem Verdacht auf eine strafbare Handlung sind die Polizeibehörden zuständig. **Eine Überwachung ohne konkreten Verdacht ist unangemessen** – zumal kein Auskunftsrecht für Betroffene und nur eine eingeschränkte Mitteilungspflicht nach dem Abschluss der Überwachung vorgesehen sind.

Geheimdienstlich beschaffte Informationen dürf(t)en **vor Gericht nicht verwendet** werden. Gleichzeitige Spionage, Spionageabwehr und Zusammenarbeit mit fremden Geheimdiensten führen zudem zu einem **Zielkonflikt**.

Die **Entschädigungen für private Spitzel** und die **Mitwirkungspflicht für private Besitzer von Überwachungskameras** ist rechtsstaatlich bedenklich. Dasselbe gilt für ein Tätigkeitsverbot (bestehend) und ein Verbot von Organisationen ausserhalb von Strafverfahren.

Zu den neu möglichen besonderen (resp. bewilligungspflichtigen) Informationsbeschaffung gehören

- **Überwachung des Post- und Fernmeldeverkehrs** nach BÜPF
- **IMSI-Catcher** und GPS-Systeme zur Ortung
- **Kameras, Mikrofone und Wanzen** auch in Privaträumen
- **Staatstrojaner** inkl. Online-Durchsuchung und Eindringen via Sicherheitslücken. Der Geheimdienst hat dadurch Interesse am Bestehen von Sicherheitslücken und schwacher Antiviren-Software.
- **Eindringen in Computersysteme und -Netzwerke**
- **Geheime Hausdurchsuchungen**

Mit der **Kabelaufklärung** wird eine **unverhältnismässige Massenüberwachung** des «grenzüberschreitenden» Internetverkehrs nach Stichworten eingeführt. Das Überwachungsprogramm ist mit Tempora von GCHQ & NSA verwandt. Ausgeführt wird es durch das Zentrum für elektronische Operationen (ZEO) der Armee.

Dezember 2015, digitale-gesellschaft.ch

DIGITALE | GESELLSCHAFT