Bern, den 18. August 2010

EJPD

Bundesamt für Justiz

Direktionsbereich Strafrecht

Bundesrain 20

3003 Bern

Totalrevision Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs,

Vernehmlassungsfrist 18. August 2010

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Gelegenheit, zur vorgeschlagenen Revision des BÜPF Stellung nehmen zu können. Die Vorlage ist aus unserer Sicht gesamthaft abzulehnen. Sie beinhaltet eine sehr weitgehende Ausdehnung der Eingriffe, die mit einer Überwachung der Kommunikation verbunden sind. **Einer Prüfung der Verhältnismässigkeit halten diese weiter gehenden Eingriffe nicht stand**. Die Notwendigkeit bzw. das Gewicht des öffentlichen Interesses erscheint fraglich. Der erläuternde Bericht bleibt hier sehr im Vagen, und es sind kaum Angaben greifbar, anhand derer sich die Notwendigkeit bestimmter Überwachungsmassnahmen überprüfen liesse. Manifest sind hingegen die gravierenden Auswirkungen auf die Grundrechte, namentlich das Recht persönliche Freiheit und Achtung der Privatsphäre, das Recht auf informationelle Selbstbestimmung und - wie es das Bundesverfassungsgericht zutreffend formuliert hat - das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Kommunikation ist ein zentraler Aspekt des menschlichen Daseins. Zu berücksichtigen ist zudem, dass es die Entwicklung der Kommunikation (Internet, mobile Kommunikation) mit sich bringt, dass immer mehr Daten anfallen, die aufbewahrt, mitgeschnitten und durchstöbert werden können, und sich immer mehr Bereiche des menschlichen Lebens in diesen Daten abbilden. **Die von der Vorlage angestrebte Erfassung neuer Bereiche der Telekommunikation bringt insoweit zwangsläufig schwerwiegendere Eingriffe mit sich als die Überwachung klassischer Kommunikationsformen.**

Der Gesetzgeber darf nicht der Verlockung erliegen, alle anfallenden Daten in der Kommunikation im Dienste der Bekämpfung von Verbrechen erfassen zu wollen. Genau in diese Richtung tendiert der Entwurf aber. Dies zeigt sich deutlich in der vorgesehenen Ausdehnung des Geltungsbereichs des BÜPF sowie der zeitlichen und sachlichen Ausweitung der Aufbewahrungspflicht, bei der zunehmend Daten gesammelt werden müssen, die nicht

ohnehin anfallen, sondern die speziell mit Blick auf die Überwachung der Kommunikation gesammelt werden müssen. **Was als Aufbewahrungspflicht für gewisse 'Randdaten' begann, mutiert so mehr und mehr zur Totalüberwachung aller Formen der Kommunikation**, bei denen Daten anfallen, die mitgeschnitten werden können, wobei sich aus den aufbewahrten Daten nicht nur Rückschlüsse auf den Inhalt der Kommunikation gewinnen lassen, sondern auch Bewegungsprofile der an der Kommunikation Beteiligten. Nach der Logik des Entwurfes sollen möglichst breit die Kommunikationsdaten aller BürgerInnen erfasst werden. Zwar nicht alle Inhalte der Kommunikation, und genutzt werden dürfen die Daten nur bei Verdacht der Begehung einer Katalogtat. Gleichwohl ist das Ergebnis aber, dass die Kommunikation aller BürgerInnen überwacht wird.

1.) Grundsätzliches

Die Technik im Bereich der Telekommunikation habe sich in den vergangenen Jahren rapide weiter entwickelt, so lautet auch die Rechtfertigung für den neusten Entwurf des BÜPF. Der erläuternde Bericht greift damit schon in den ersten Sätzen jene stereotype Argumentation auf, die seit mehreren jahrzehnten den Standard für verschärfte Formen der Telekommunikationsüberwachung darstellt. Diese Argumentation ist aus mehreren Gründen bedenklich:

Zum einen, weil sie im Kern totalitär ist: Zwar argumentiert auch der Vorentwurf, dass die meisten BürgerInnen und Unternehmen die neuen Techniken - hier: insbesondere die durch das Internet ermöglichten - gesetzestreu und mit «guten Absichten» nutzten. Sie dienten aber «auch Straftätern zu verwerflichen Zwecken». Weil dem so ist, soll nun praktisch sämtliche Telekommunikation unter den Vorbehalt staatlicher Kontrollierbarkeit gestellt werden. Technische Lücken der Überwachbarkeit sollen geschlossen werden. Sämtliche TeilnehmerInnen an der Telekommunikation sollen identifizierbar sein. Die Information, wann und von wo aus sie mit wem kommuniziert haben, sollen nunmehr für ein Jahr lang für den Abruf durch die Untersuchungsbehörden gespeichert werden. Damit das alles möglich ist, sollen die Anbieterfirmen stärker noch als bisher zu Hilfspolizisten gemacht werden.

Zum zweiten, weil sie beliebig ist: Seit in den 90er Jahren neue technische Möglichkeiten der Telekommunikation - angefangen mit der Mobiltelefonie bis hin zu den neusten mit dem Internet verbundenen Techniken - entstanden sind und sich verbreitet haben, wird vor den Gefahren des Missbrauchs gewarnt. In diesem Vorentwurf werden sie in der Kinderpornographie, dem Organisierten Verbrechen und dem Drogenhandel geortet. Angesichts der Beliebigkeit der Argumentation ist es fast erstaunlich, dass der Terrorismus und dessen Finanzierung, die seit 2001 weltweit zur rechtspolitischen Allround-Legitimation für alles mögliche avanciert sind, nicht zur Begründung herangezogen werden.

Was insbesondere den Drogenhandel betrifft, so sind die technischen Vorkehrungen, welche Drogenhändler im Rahmen ihres illegalen Geschäfts ergreifen, erfahrungsgemäss aber eher minim. Geschäfte werden in der Regel nach wie vor über Mobiltelefone abgewickelt. Die Tatsache, dass Polizei und Strafverfolgungsbehörden regelmässig Erfolge durch traditionelle Telefonüberwachungen und andere Ermittlungsformen erzielen, zeugt davon, dass die Vorstellungen vom Organisationsgrad des Drogenhandels und der dort herrschenden technischen Konspiration doch reichlich überzogen sind. Die Schwierigkeiten der Verfolgung liegen vielmehr darin begründet, dass der Handel mit illegalen Drogen einen äusserst breiten (lukrativen) Markt mit einer grossen Konkurrenz darstellt**. Im Erläuternden Bericht finden sich daher bezeichnenderweise nicht einmal ungefähre Angaben über Fälle oder Fallkonstellationen, in denen das bisherige Instrumentarium der Überwachungen nicht ausgereicht hätte.**

Zum dritten finden sich generell nur sehr allgemeine statistische Angaben über die Überwachungspraxis. Der Dienst, der mittlerweile im EJPD angesiedelt ist, veröffentlicht nur die jährlichen Zahlen von Echtzeitüberwachungen einerseits und der rückwirkenden andererseits. Alle anderen Angaben sind nur «über den Daumen gepeilt».

Das gilt zunächst für die Art der überwachten Anschlüsse bzw. Geräte. Bekannt ist nur, dass die meisten Überwachungen sich auf Mobiltelefone beziehen. Unbekannt ist dabei aber die Zahl der technischen Sonderformen, die anhand der «Randdaten» möglich sind, etwa Zielwahlsuchläufe oder die Ermittlung sämtlicher Mobiltelefone, die zu einem bestimmten Zeitpunkt in einer Funkzelle präsent waren. Die E-Mail-Überwachung hat nach wie vor einen geringen Stellenwert, was kaum dafür spricht, dass die technischen Neuerungen für die Überwachungspraxis eine grössere Rolle hätten.

Unbekannt ist auch die jeweilige Dauer der Überwachung und die Zahl der Fälle, in denen Anordnungen über den Zeitraum von drei Monaten hinaus verlängert wurden.

Nur oberflächliche Angaben macht der Dienst zu den Anlassstraftaten.

Keine Informationen existieren darüber, ob und wenn ja zu welchem Ergebnis die Überwachung geführt hat. Dies würde voraussetzen, dass die Justizbehörden entsprechende Informationen zurückmelden.

Was schliesslich die Kosten anbetrifft, so finden sich allenfalls Angaben über die Gesamtsumme der Einnahmen des Dienstes aus den gebühren, die die Untersuchungsbehörden entrichten, sowie über die Summe der heute an die Provider gezahlten Entschädigungen. Allerdings muss davon ausgegangen werden, dass diese technische Seite nur der kleinere Teil der Gesamtkosten ist. Der überwiegende Teil dürfte bei den Untersuchungsbehörden für Transkriptionen und Übersetzungen anfallen.

Insgesamt bildet die Überwachungspraxis heute eine Blackbox und es scheint so, als hätten weder der Bund noch die Kantone ansatzweise ein Interesse, etwas Licht in diese Angelegenheit zu bringen. Eine Studie, wie sie in Deutschland vor einigen Jahren im Auftrag der Bundesregierung vom Freiburger Max-Planck-Institut für Strafrecht angefertigt würde, fehlt hierzulande gänzlich.

Vor diesem Hintergrund ist der vorliegende Gesetzentwurf eine schlichte Zumutung. Erneut wird hier ins Blaue hinein legiferiert - ohne Rücksicht auf die Rechte der BürgerInnen, auf den technischen und finanziellen Aufwand und die Effizienz, die die erweiterte Überwachung haben könnte.

2.) Zu den einzelnen Punkten

2.1) Geltungsbereich des BÜPF (Art. 2 u.a.)

Das Bestreben, möglichst alle Formen von Kommunikation unter den Vorbehalt der Überwachung zu stellen, kommt deutlich im wachsenden Umfang jenes Kreises von privaten Personen, Unternehmen und Organisationen zum Ausdruck, die in der einen oder anderen Form an der Überwachung mitzuwirken oder sie gar direkt vorzunehmen haben:

die **Post** und neu auch **Kurier- und Eildienste,** die sowohl «Randdaten» (rückwirkend) als auch Inhalte von Briefen oder Paketen (laufend) zu übermitteln haben;

die **Anbieter von Telefon** (Telefax u.a.)-Diensten, die ihre KundInnen identifizieren, sowie «Randdaten» und ebenfalls den Inhalt von Telefongesprächen offen legen müssen;

berufsmässige **Internet-Provider**. Dazu zählten bisher schon E-Mail-Service-Provider, die wie Post- und Telefon-Anbieter «Randdaten» und Inhalte übermitteln mussten. Die IPRichtlinie vom vergangenen Jahr zwingt Service-Provider, zusätzlich die Übermittlung des gesamten Internet-Verkehrs einer Person in Echtzeit (welche Websites wurden aufgerufen etc.) zu übermitteln. **Neu gehören auch reine «Hosting»-Provider** zum Kreis der Personen, die Überwachungen vorzunehmen haben: Dies beträfe u.a. Webmail-Dienste, Voice over Internet-Dienste, Chatrooms, Internet-Foren o.ä.m.

Händler von Prepaid-Sim-Karten, die die KäuferInnen zu identifizieren und die Daten für zwei Jahre aufzubewahren haben. Die Einführung dieser Registrierungspflicht hatte zur Folge, dass nicht nur Sans-Papiers, sondern auch vorläufig Aufgenommene und Asylsuchende praktisch vom Zugang zu einem Mobiltelefon ausgeschlossen wurden. Neu sollen nun auch Prepaid-Wireless-Karten registriert werden.

Betreiber von Internet-Cafés sowie Hotels, die ihren Gästen, oder Schulen, die ihren SchülerInnen Zugang zu einem WLAN gewähren, die Identität der TeilnehmerInnen feststellen; zu diesem Kreis zählen auch Privatpersonen, die anderen den Zugang zu ihrem WLAN ermöglichen. Sie müssen zwar nicht die Überwachung selbst durchführen, wohl aber die Überwachung durch den Provider dulden.

Ebenfalls den Zugang zur Überwachung ermöglichen müssen Betreiber von internen Telefonnetzen wie **Firmennetze oder Hauszentralen** sowie nicht berufsmässige Anbieter von Internet-Dienste (Vereine o.ä.).

Schon diese Auflistung macht deutlich, dass schon allein die Menge der Daten, die gegebenenfalls zur Identifizierung und zur rückwirkenden Erfassung von «Randdaten» aufbewahrt werden müssen, enorm ist. Schon allein vor diesem Hintergrund ist die neuerliche Ausdehnung der für die Überwachung in Dienst genommenen privaten Personen oder Orgnaisationen nicht hinzunehmen. Dies umso mehr, als gleichzeitig auch die Pflichten, Daten aufzubewahren und herauszugeben und bei der Überwachung mitzuwirken, deutlich ausgedehnt werden. Stattdessen fordern DJS und grundrechte.ch eine Überprüfung der Effizienz und Notwendigkeit einer solchen Mitwirkung.

2.2) Pflichten der Provider (Art.21)/Zertifizierung (Art. 18 und 24)/Kosten (Entschädigung) (Art. 30)

DJS und grundrechte.ch lehnen die Abschaffung der Entschädigung für diejenigen Personen (bzw. Firmen), die selbst die Überwachung vornehmen müssen, also die Provider von Post-, Telefon- und Internetdiensten, ab. **Das Argument, eine solche Entschädigung sei im Strafrecht „systemwidrig“, überzeugt nicht. Der dabei gezogene Vergleich mit der Editionspflicht der Banken ist abwegig.** Wenn der Vergleich zutreffend wäre, müssten nicht spezielle Aufbewahrungs- und sonstige Mitwirkungspflichten nur für den Bereich des BÜPF postuliert werden, sondern es würde genügen, den Providern gewöhnliche, auf die StPO gestützte Editionsbegehren zukommen zu lassen. Was von den Providern verlangt wird, ist mehr als die Herausgabe von ohnehin vorhandenen Daten oder Akten, sondern die **Rolle von Hilfspolizisten**, die mehr und mehr von vorneherein gegen die Interessen ihrer KundInnen agieren und Daten für eine potenzielle Überwachung im Falle einer Strafuntersuchung anhäufen und aufbewahren müssen. Die vorgesehene Hilfspolizistenrolle ist zumindest in Rechtsstaaten ebenfalls systemwidrig. Dies gilt umso mehr als der VE nun von den Providern

eine noch «aktivere Rolle» fordert - wenn es darum geht, **Schadsoftware in die Datenverarbeitung ihrer KundInnen einzuschleusen** (siehe unten). Spätestens an diesem Punkt stellt sich die Frage, ob die staatlich zugemutete Rolle noch mit dem Prinzip von Treu und Glauben vereinbar ist, der das schweizerische Wirtschaftssystem kennzeichnen soll.

Zwar sind die im Gesetz formulierten Pflichten der Provider seit der Einführung des BÜPF im Wesentlichen gleich geblieben. Praktisch haben sie mit den diversen Richtlinien – beispielsweise im letzten Jahr der IP-Richtlinie - ständig zugenommen. Dies war schon in der Vergangenheit vor allem für die kleineren Provider eine erhebliche Belastung. Bereits die Einführung der Vorratsspeicherung der «Randdaten» im E-Mail-Verkehr zwang zu grösseren finanziellen Aufwendungen. **Mit der in der IP-Richtlinie vorgesehenen Pflicht, den gesamten Internet-Verkehr einer Person in Echtzeit weiterzuleiten, wird ein neuer Schub an technischer Aufrüstung und damit an enormen Kosten auf die Provider zukommen.**

Das mag für die grossen Anbieterfirmen, die auch im Telefonbereich tätig sind, verkraftbar sein, auch wenn die bisherige Entschädigung wegfällt. Für die kleinen lokalen Provider stellen schon die für die Überwachung erforderlichen Investitionskosten ein Dilemma dar. Das Argument, sie würden ja auch Profit aus den neuen Techniken ziehen, ist vor allem auf dieser Ebene des Marktes unsinnig. Die Überwachung der Kommunikation für die Zwecke der Strafverfolgung ist eine staatliche Aufgabe, und es geht nicht an, von den Providern entschädigungslos derartige Sonderanstrengungen zu verlangen, damit diese staatliche Aufgabe erfüllt werden kann.

Auch eine Zertifizierung nach Art. 18 durch den Dienst bzw. von ihm beauftragte Dritte wird diese Situation nicht ändern. Zwar ist diese Überprüfung, ob der Provider über die für die Überwachung notwendigen technischen Voraussetzungen verfügt, zunächst freiwillig. Allerdings erfolgt sie auf Kosten der Provider. Zudem wird in Art. 24 mit Folgen gedroht, wenn die Überwachung durch Dritte vorgenommen wird und die Aufrüstung dann dennoch nachgeholt werden muss. Und schliesslich sieht Art. 31 Bussen bis zu 100 000 Franken für diejenigen vor, die vorsätzlich den Weisungen des Dienstes nicht nachkommen oder Randdaten nicht aufbewahren, und bis zu 40 000 für die fahrlässige Verletzung dieser Vorschriften. **Im Ergebnis weicht die Freiheit, moderne Formen der Kommunikation anbieten zu können - sei dies kommerziell oder nicht kommerziell - einem staatlichen Bewilligungs- und Kontrollsystem.**

Auf dieses Zwangssystem ist deshalb zu verzichten. Die Leistungen der Provider für die Überwachung sollten zudem weiterhin entschädigt werden bzw. es ist vorzusehen, dass alle Aufwendungen der Provider, die ohne die Pflichten, die ihnen mit dem BÜPF auferlegt werden, nicht angefallen wären, zu entschädigen sind.

2.3) Permanente Identifizierungspflicht (Art. 22)

Nach Art. 22 müssen die Provider dafür sorgen, dass alle Personen, die über ihre Vermittlung Zugang zum Internet erhalten, identifizierbar sind.

Nach Art. 2 VE sind Internetcafés, Schulen, Hotels, Spitäler oder andere, die zum Beispiel über ein WLAN Zugang zum Internet eröffnen zwar keine «Personen, die selbst Überwachungen durchführen» müssen. Nach Art. 22 sollen sie aber gemeinsam mit den Providern dafür sorgen, dass ihre KundInnen, Gäste etc. identifiziert werden. Dies gilt nach dem Wortlaut des Gesetzes und gemäss Bericht insbesondere auch für Privatpersonen und soll zum Beispiel dadurch geschehen, dass die Betroffenen erst nach Angabe einer Handy-Nummer Zugang zum WLAN erhalten. DJS und grundrechte.ch lehnen diese Regelung ab. Schliesslich setzt auch das Telefonieren in einer öffentlichen Telefonzelle nicht voraus, dass die betreffende

Person zunächst ihren Pass oder eine ID angibt und erst dann telefonieren darf.

Art. 22 bedeutet im Ergebnis, dass jede Person, die das Internet nutzt, egal wo und wie, sei dies über einen Heimanschluss, sei dies über ein Internetcafé, über einen Hotspot oder über das mobile Funknetz (welches ja ebenfalls Zugang zum Internet bietet) ihre Identifizierung ermöglichen muss, bevor sie surfen darf. Die Provider müssen gemeinsam mit ihren Kunden dafür sorgen, dass die lückenlose Identifizierbarkeit aller Internetnutzer sichergestellt wird. Damit müsste beispielsweise, wer einen Kollegen an seinen Computer oder an sein Smartphone lässt, damit dieser surfen kann, seinem Provider vorgängig die Identifizierung des Kollegen ermöglichen. Die Provider müssen die technischen Voraussetzungen dazu liefern und in Verträgen eine Pflicht zur Übermittlung der entsprechenden statuieren. **Die Vorschrift bedeutet im Übrigen auch, dass Provider ihren Nutzern verbieten müssten, nicht passwortgeschützte Netzwerke zu betreiben**. Der Aufwand für die Provider dürfte im Übrigen enorm sein. Schliesslich bedeutet die Vorschrift auch, **dass jede Person, die in einer solchen Situation nichts anzubieten hat, um ihre Identifikation zu ermöglichen, vom Zugang zum Internet ausgeschlossen sein soll:** Wer kein Mobiltelefon mit sich trägt, wird beispielsweise in vielen Fällen von der Nutzung des Internets ausgeschlossen sein, namentlich beim Zugang zu Hotspots oder wenn man einmal rasch den Computer einer Kollegin nutzen will, denn die Angabe einer funktionierenden, auf den eigenen Namen eingetragenen Mobiltelefonnummer wird oft die einzige Möglichkeit sein, um die Identifizierbarkeit herzustellen. Die genannten Auswirkungen zeigen allerdings gleichzeitig auch, dass sich die Vorschrift nie durchsetzen lassen wird. Die primären Kunden der Anbieter von Internetzugängen werden nicht dazu bereit sein, immer zu deklarieren, wer ihren Internetzugang benutzt. Zudem liesse sich die vorgesehene Identifizierbarkeit regelmässig leicht umgehen, namentlich durch die Verwendung eines fremden Mobiltelefons, um den Zugang zu erhalten. Insgesamt zeigt sich mit dieser absurden Vorschrift deutlich der totalitäre Ansatz der Vorlage.

2.4) Vorratsdatenspeicherung (Art. 23)

Bei den so genannten Randdaten handelt es sich um Angaben, die ursprünglich nur für Rechnungszwecke erforderlich waren. Die Anbieter von Telekommunikationsdiensten konnten die Daten ein halbes Jahr aufbewahren oder sie bereits früher löschen, wenn die Rechnung bezahlt war. Dieser Bezug auf den Zweck der Rechnungslegung hat im Laufe der Zeit gegenüber dem Überwachungsinteresse immer weniger Bedeutung erhalten. Zunächst wurde dem Überwachungsdienst bzw. den Untersuchungsbehörden die Möglichkeit eröffnet, auf die Rechnungsdaten zuzugreifen. **Mit Verabschiedung des BÜPF wurden die Anbieter von Telekommunikationsdiensten gezwungen, die Daten - unabhängig vom Rechnungszweck - in einer Art und Weise aufzubewahren, die nur der Überwachung diente.** Der Zweck der Rechnungslegung hat insbesondere im Bereich des Internets immer weniger Bedeutung, weil viele NutzerInnen ohnehin Pauschalbeträge bezahlen (ADSL-Anschlüsse). Dies ist ein treffendes Beispiel für die Zweckentfremdung von Daten, die sich bei der Telekommunikation notwendigerweise ergeben. **Ausweislich der mageren statistischen Angaben des Dienstes hat der rückwirkende und fortlaufende Zugriff auf die «Randdaten» mittlerweile eine grössere Bedeutung erhalten als die Überwachung des Inhalts der Kommunikation.**

Es geht hier offensichtlich um eine Vorratsdatenspeicherung. Die Anbieterfirmen werden gezwungen, Daten völlig unverdächtiger Personen aufzubewahren für den Fall, dass sie doch einmal verdächtig werden könnten. Dies war bereits bisher ein Skandal und wird es durch die mit dem Vorentwurf geplante Verdoppelung der Aufbewahrungsfrist um so mehr. Die verlängerte Aufbewahrungsdauer von neu 12 Monaten hat nicht nur für die TK-Unternehmen gravierende Auswirkungen, sondern auch für die Kommunizierenden selbst, deren Daten fortlaufend zweckentfremdet werden. DJS und grundrechte.ch lehnen diese Ausdehnung der

Aufbewahrungsfrist ab.

2.5) Postüberwachung (Art. 19)

Geradezu absurd erscheint die Übertragung der Definition von Randdaten auf die Postüberwachung. Die Zahl der Postüberwachungen hat ohnehin in dem Masse abgenommen, als die elektronischen Formen der Kommunikation zugenommen haben.

Für die Post galt die Pflicht zur Aufbewahrung der Information darüber, wer wem einen Brief oder ein Paket geschickt hat, schon bisher. **Es war und ist der Post offenbar aber nicht möglich, dieser Pflicht nachzukommen.** Anders als bei der elektronischen Kommunikation fallen bei der Post nicht automatisch Randdaten an, die die Identifizierung der Kommunikationsteilnehmer erlauben. **Die 15 Millionen Briefe, die sie täglich befördert, werden zwar in den Briefzentren maschinell sortiert und mit einer Codenummer versehen. Diese dient jedoch nur der korrekten Zustellung. Codenummern gibt es auch für die 500 000 täglich verschickten Pakete. Diese werden verwendet, um jede einzelne Sendung auf ihrem Weg zum Bestimmungsort zu identifizieren und zu verfolgen**. Die Adressen werden aber weder im Paket- noch im Briefverkehr eingescannt. Mit vernünftigen Aufwand wäre das gar nicht zu bewerkstelligen. Die Umsetzung der im BÜPF vorgesehenen Pflichten würde **Postdienstleistungen massiv verteuern.** Kommt hinzu, dass es für die Richtigkeit von Absenderangaben, sofern sie überhaupt auf dem Couvert stehen, keine Garantie gibt. Dafür müsste die Post von ihren KundInnen nämlich eine Identitätskarte verlangen - ein schwachsinniges Unterfangen. Die Post identifiziert daher nach eigenen Angaben nur die AbsenderInnen von eingeschriebenen Sendungen, was aber in der Praxis ebenfalls nicht grossflächig durchgesetzt wird Statt wie vorgesehen, die Aufbewahrungsdauer auch hier zu verdoppeln und auf Kurierdienste u.ä. auszudehnen, fordern DJS und grundrechte.ch die Abschaffung dieser gesetzlichen Vorschrift.

2.6) Informatiksystem (Art. 6 ff.)

Mit dem Vorentwurf soll auch das Informatiksystem eine Rechtsgrundlage erhalten, das bereits in der Ausschreibungsphase ist. Neu werden die, im Rahmen der Überwachung gewonnenen Daten nicht mehr an die anordnenden Behörden resp. die Polizei verschickt, sondern sollen für sie abrufbar sein.

grundrechte.ch und DJS kritisieren insbesondere die in Art. 11 vorgesehenen überlangen Aufbewahrungsfristen. Die Strafverfolgungsverjährung dürfte in den meisten Fällen erst nach 15 Jahren ablaufen. **Stattdessen fordern grundrechte.ch und DJS, dass die Daten spätestens nach Abschluss des Strafverfahrens auszugliedern sind und sie damit nicht mehr für den Abruf oder sonstigen Zugang der Strafverfolgungsbehörden vorzuhalten**. Die ausgegliederten Daten sollten nur noch für die Einsicht der Betroffenen aufbewahrt werden. Da das Verfahren abgeschlossen ist, steht auch der **vollständige Einsicht der Betroffenen** nichts im Wege. Sie sollte automatisch erfolgen und zwar in der Form, dass den Betroffenen sämtliche Aufzeichnungen in einem handelsüblichen Format ausgehändigt werden.

Das Verarbeitungssystem muss im Übrigen so eingerichtet sein, dass es nicht das Recht auf Akteneinsicht und den Datenschutz unterminiert, d. h. die Ausübung Einsichts- und Auskunftsrechts gewährleistet. Die Ausführungen in Ziff. 1.4.2 des erläuternden Berichts (immer grössere Datenmengen, rasche technische Entwicklung erschweren Lesbarkeit von Datenträgern über längere Zeit, schwer verfügbare Lesegeräte etc.) wecken hier gewisse Bedenken.

2.7) Einschleusung von «Informatikprogrammen», Online-Durchsuchung (Art. 270Bis StPO), sog. Trojaner

Die in der deutschen Diskussion unter dem Begriff «online-Durchsuchung» bekannte Methode soll mit dem Vorentwurf in der StPO verankert werden, im Büpf selbst wird zusätzlich die Mitwirkungspflicht der Provider statuiert. Die neue StPO ist noch nicht in Kraft getreten, da schlägt das EJPD also bereits eine Erweiterung der strafprozessualen Zwangsmassnahmen vor.

Sowohl der Begriff «Online-Durchsuchung» als auch der im VE gewählte Terminus «Einschleusung von Informatikprogrammen» sind verharmlosend. **Es geht um Software, die Schaden anrichtet, um «Trojaner», vor denen ansonsten gewarnt wird und gegen die Anti-Viren- Programme empfohlen werden.**

Es geht hier nicht nur um eine besondere Form der Telekommunikationsüberwachung, sondern um einen schweren Eingriff in das Grundrecht des Post- und Fernmeldegeheimnisses. Nur lapidar hält der erläuternde Bericht fest: «Mit der betreffenden Überwachungsmethode kann auf das gesamte Datenverarbeitungssystem zugegriffen werden, in welches das Informatikprogramm eingeführt wird.» Die dadurch mögliche Ausforschung geht also erheblich weiter. Das deutsche Bundesverfassungsgericht hat deshalb in seinem Grundsatzurteil vom Februar 2008 festgestellt, dass **diese Methode das aus dem allgemeinen Persönlichkeitsrecht sich ergebende «Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme» verletzt.** Bezeichnenderweise nimmt der Bericht in seinem Rechtsvergleich keinen Bezug auf dieses Urteil, obwohl ein solches Grundrecht sich auch aus Art. 10 der schweizerischen Bundesverfassung ergibt. Dieses neue Grundrecht drängt sich auf, weil durch die neuere Informationstechnik «informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist», so das BVerfG. Für mehr und mehr Bürgerinnen und Bürger ist der mit dem Internet verbundene PC zu einem Medium geworden, worauf sie ihre Kontenführung und Terminplanung abwickeln, über das sie mit anderen kommunizieren und auch vergangene Kommunikation speichern, auf dem sie nicht nur private Bilder oder ähnliche Dinge speichern, sondern aus dem sich die gesamte Bandbreite ihrer Interessen und Informationsbedürfnisse ablesen lässt. Immer weitere Bereiche des Lebens bilden sich damit im PC ab. Ein heimlicher Eingriff in diese Sphäre müsste - wenn überhaupt - an besondere Eingriffsvoraussetzungen gebunden werden.

Das deutsche Bundesverfassungsgericht will diese «online-Durchsuchung» deshalb nur für den Schutz «überragend wichtiger Rechtsgüter» zulassen. «Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.»

Von solchen Überlegungen ist der Vorentwurf weit entfernt:

Dieser Zugriff auf die auf dem Computer gespeicherten Daten soll zwar dadurch begrenzt werden, dass bereits bei der Anordnung anzugeben ist, welche Daten denn gesucht werden. Das Ziel dieser Begrenzung ist laut Bericht aber nicht der Schutz der Privatsphäre oder der legitimen sozialen und politischen Aktivitäten des oder der Betroffenen, sondern die Aussonderung von irrelevanten Informationen. **Es ist auch nicht davon die Rede, dass die Durchsuchung des Computers auf bestimmte Programme - etwa das Mailprogramm - beschränkt werden soll.** Eine thematische Eingrenzung würde aber zunächst die Durchsuchung der gesamten Festplatte voraussetzen, um die angeblich relevanten Dateien zu finden. Darüber hinaus dürfte das Zwangsmassnahmengericht mehr noch als bei üblichen

Telekommunikationsüberwachungen von den Vorgaben der Staatsanwaltschaft und damit letztlich der Polizei abhängig sein.

Ansonsten soll nur die übliche Formulierung, dass die bisherigen Massnahmen erfolglos geblieben sind oder für aussichtslos gehalten werden, für eine Begrenzung sorgen. Der Bericht verkauft dies als «doppelte Subsidiarität», weil schon die übliche Telekommunikationsüberwachung an die Voraussetzung gebunden ist, dass andere Methoden erfolglos waren oder aussichtslos sind. **Tatsächlich heisst das aber nichts anderes, als dass die Untersuchungsbehörden und das genehmigende Gericht letztlich bei einem Fehlschlag der üblichen Telekommunikationsüberwachung fast automatisch die Grundlage für ein weiteres Eindringen in den jeweiligen Computer vorliegen haben.**

Einen b**esonderen Deliktkatalog will das EJPD nicht**, weil alle Delikte, die die «normale» Telefonüberwachung zulassen könnten, «geeignet sind, im konkreten Fall eine solche Schwere zu erreichen, welche die Anwendung der Überwachungsmassnahme rechtfertigt». Worin die hier geforderte besondere Schwere denn sonst bestehen soll, lässt der Bericht aber offen, und ist angesichts des doch sehr weit gefassten Deliktskatalogs (der beispielsweise die Verletzung von ausländerrechtlichen Strafbestimmungen enthält) nicht nachvollziehbar.

Die Phantasielosigkeit der UrheberInnen des Entwurfs, ihre mangelnde Bereitschaft auch nur ansatzweise über einen erhöhten Rechtsschutz nachzudenken, macht deutlich, dass es hier darum geht, eine möglichst leicht handhabbare Gesetzesgrundlage für eine Methode zu erhalten, die nun einmal technisch möglich ist.

Jenseits der Frage des Rechtsschutzes müsste auch die Frage nach der erwartbaren Effizienz dieses Mittels gestellt werden. Spätestens dann, wenn die zu überwachende Person nicht von ihrem eigenen Computer, sondern in einem Internet-Café ins Netz geht, laufen die Bestrebungen, eine Verschlüsselung durch die Einschleusung von Schad-Software zu knacken, ins Leere. Schwierig kann es beispielsweise auch werden, wenn die im Bericht beschriebenen Kommunikationsformen wie Internettelefonie über ein Smartphone laufen, wenn ein Computer konsequent über Hotspots oder über wechselnde Mobilfunkzugänge - etwa über die Verbindung mit einem Smartphone (Tethering) - genutzt werden. Schliesslich gibt es auch Methoden, um anonymes Surfen zu ermöglichen (z. B. TOR), deren konsequente Nutzung es erheblich erschweren bis verunmöglichen können, einen Computer überhaupt für die Einschleusung des Trojaners anzupeilen. **Die Massnahme träfe also insbesondere diejenigen, die keine entsprechenden Vorsichtsmassnahmen ergreifen.**

2.8) IMSI-Catcher Art. 270ter StPO

Der IMSI-Catcher ist ein Gerät, das - verkürzt ausgedrückt - den im Umkreis befindlichen Mobiltelefonen «vorgaukelt», es sei eine Mobilfunkantenne. Da der Mobiltelefonverkehr immer über die nächst gelegene Antenne gesteuert wird, zieht dieses Gerät automatisch sämtliche Handys auf sich und erlaubt damit, sie anhand der IMEI- und SIM-Kartennummer zu identifizieren. Der Mobiltelefonverkehr wird entweder weitergeleitet oder einfach durch die Fake-Antenne gestört. **Die Massnahme betrifft nicht nur einen bestimmten Mobilfunkteilnehmer, wie das im Bericht behauptet wird, sondern immer alle Personen, die sich im Umkreis aufhalten - unabhängig davon, ob sie verdächtig sind oder die Massnahme auf sie gezielt ist. Schon aus diesem Grund ist der Einsatz solcher Geräte abzulehnen.**

Auch beim Einsatz des IMSI-Catchers handelt es sich um eine Regelung, die noch kurzfristig vor dem Inkrafttreten in die StPO eingefügt werden soll. Allerdings stellt sich die Frage, ob der Einsatz dieses Geräts überhaupt in den Rahmen des Strafprozessrechts gehört. Laut Bericht

soll die Polizei nämlich zwar auf Anordnung der Staatsanwaltschaft solche Geräte einsetzen dürfen - jedoch mit dem Ziel, «die öffentliche Sicherheit zu gewährleisten». Letzteres ist aber eindeutig eine polizeirechtliche Aufgabe, für die der Bund keine Gesetzgebungskompetenz hat. **Bezeichnenderweise ist im Text des neuen Artikels selbst überhaupt keine Zweckbestimmung angegeben - weder polizeirechtlicher noch strafprozessualer Natur.** Der Artikel gibt weder Kriterien dafür an, wann ein solcher Einsatz gerechtfertigt wäre, noch formuliert er Eingriffsvoraussetzungen, die über die Genehmigung durch das Zwangsmassnahmengericht hinausgehen würden. Das Gericht hat damit auch keine Leitlinien, anhand derer es den Einsatz genehmigen oder untersagen könnte. Ausländische Erfahrungen mit dem IMSI-Catcher zeigen, dass das Gerät vor allem dazu geeignet ist, um in bestimmten Situationen «spontan» zu erfahren, wer sich an einem bestimmten Ort aufhält, oder um gezielt den Telefonverkehr zu stören. Vor diesem Hintergrund wäre auch die Zeit, die dem Gericht für die Prüfung von Akten und Informationen und seine Entscheidung bleiben würde, eng bemessen. Eine solche Regelung kann nicht akzeptiert werden.

Insgesamt kommen grundrechte.ch und die DJS zum Schluss, dass diese Gesetzesvorlage so nicht dem Parlament vorgelegt werden kann und darf. Vielmehr muss zuerst umfassende Transparenz über die bisherige Überwachungspraxis gestützt auf die bestehende gesetzliche Grundlage geschaffen werden. Und es braucht unmissverständlich klare gesetzliche Vorschriften, die dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Rechnung trägt und vom Gedanken der pauschalen Verdächtigung aller Bürgerinnen und Bürger absieht.

Wir hoffen, dass unsere hier dargelegten Überlegungen in die weitere Diskussion einfliessen können und namentlich der Bundesrat die Vorlage zur vollständigen Überarbeitung zurückzieht.

Mit freundlichen Grüssen

Für grundrechte.ch: RA Viktor Györfffy, Präsident

Für die DJS: Catherine Weber, Geschäftsführerin