

Hausarbeit im Rahmen des Lehrganges für Rechtsinformation und
Informationsrecht

Vorlesung: Grund- und Menschenrechte

Ass.- Prof. Dr. Hannes Tretter

Eingriffe in die Grundrechte von Betreibern und Konsumenten von
Telekommunikationsdiensten durch polizeiliche
Überwachungsmaßnahmen:

Zu Natur und Konsequenzen einer europäischen
Überwachungsverordnung
(ENFOPOL-98-Dokument)

Verfasst von:

Mag. Theresa Philippi, LL.M.
Mag. Petra Pracher

Einleitung

Gegenstand dieser Untersuchung ist das sogenannte „ENFOPOL-98-Dokument“ in seiner Fassung als Entwurf einer Entschließung des Rates der Europäischen Union über die rechtmäßige Überwachung des Telekommunikationsverkehrs in Bezug auf neue Technologien, welche der Ratsarbeitsgruppe „Polizeiliche Zusammenarbeit“ in ihrer Sitzung vom 3. und 4. September 1998 vorgelegt wurde.

Einbegleitend ist zu bemerken, dass das oben genannte Dokument, das den Gegenstand dieser Untersuchung darstellt, nach den Recherche-Ergebnissen der Verfasserinnen über den Status eines Entwurfes niemals hinausgekommen ist, aber dennoch Anlass für zahlreiche Berichte in Printmedien und im Internet sowie für ein rechtswissenschaftliches Gutachten im Auftrag des „Forum Mobilkommunikation“ wurde. Grund dafür ist sein überaus brisanter Inhalt, der, falls das Dokument einmal Rechtskraft erlangen sollte, wesentliche Auswirkungen auf Grundrechte der Anbieter von Telekommunikationsdiensten sowie auf die Nutzer der Telekommunikationsdiensten haben würde.

Das Basisdokument, die Entschließung des Rates über die rechtmäßige Überwachung des Telekommunikationsverkehrs vom 17.1.1995, wurde in der C-Serie des Amtsblattes der Europäischen Gemeinschaft veröffentlicht (ABl. C 329/01). In der C-Serie werden nicht-rechtsverbindliche Dokumente zur Information publiziert. Der erste Entwurf für die Überarbeitung, das ENFOPOL 98 - Dokument trägt jedoch die Klassifikation LIMITE, das heißt, dass er vertraulich zu behandeln und nur einem eingeschränkten Leserkreis zugänglich zu machen ist.

In der Folge soll die Entstehungsgeschichte, die europarechtliche Qualifikation und der Inhalt des ENFOPOL-98-Dokumentes dargestellt werden. Die Konzentration auf das ENFOPOL 98-Dokument erfolgt deshalb, weil die Nachfolgedokumente letztlich nur Versuche der jeweiligen Präsidentschaft waren, das Dokument endlich zur Abstimmung zu bringen, ohne den Inhalt wesentlich zu verändern. Der zweite Teil der Arbeit wird eine allfällige Umsetzung in österreichisches Recht und die daraus resultierenden Grundrechtseingriffe näher beleuchten.

Entstehungsgeschichte

Eine Studie des Europäischen Parlamentes¹ über die Technologien politischer Kontrolle zitiert einen Bericht der britischen Menschenrechtsüberwachungsorganisation Statewatch, in dem von einem Transatlantischen Gipfel zwischen den USA und der Europäischen Union in Madrid im Dezember 1995 berichtet wird. Gegenstand des Gipfeltreffens war laut „Statewatch“ eine Neudefinition der transatlantischen Zusammenarbeit nach dem Ende des Kalten Krieges und insbesondere die zunehmend polizeilichen Tätigkeiten interner Sicherheitsdienste im Sinne eines „Law and Order“-Staates im Rahmen eines „Joint Action Plan“.

Bereits im Jänner 1995 hatte der Rat der Europäischen Union im Rahmen der durch den Vertrag von Maastricht geschaffenen „Dritten Säule“ eine Entschließung über die rechtmäßige Überwachung des Telekommunikationsverkehrs angenommen, das weitreichende Überwachungsmöglichkeiten vorsah. Mit der vorgeschlagenen Überarbeitung

¹ www.europarl.eu.int/stoa: „An appraisal of the technologies of political control“, September 1998

durch eine EntschlieÙung im Jahr 1998 sollte der Rat den Anwendungsbereich insbesondere auf mobile satellitengestützte Dienste, mobile Telefonie, für die mit prepaid Karten bezahlt wird und das Internet ausdehnen.

Europarechtliche Qualifikation

Die Dritte Säule

Durch die mit dem Vertrag über die Europäische Union (Maastricht, 1992) geschaffene sogenannte Säulenstruktur wurden die davor im Rahmen der „Europäischen Politischen Zusammenarbeit“ (EPZ) diskutierten und nach den Regeln des Völkerrechtes Beschlüssen zugeführten Themen wie Außen- und Sicherheitspolitik aber auch Justiz und Innere Sicherheit an das institutionelle Gefüge der Europäischen Gemeinschaft herangeführt. Der Binnenmarkt und seine flankierenden Politiken blieben in der Ersten Säule, welche durch Beschlussfassung mit Mehrheitsentscheidung im Rat und die erhöhten Mitentscheidungsrechte des Europäischen Parlamentes am meisten „vergemeinschaftet“ ist. In der Dritten Säule (Zusammenarbeit im Bereich Justiz und Inneres), die im gegebenen Zusammenhang von Interesse ist, wurde die Beschlussfassung mit Einstimmigkeit beibehalten, aber ein gradueller Übergang zur Beschlussfassung mit Mehrheitsentscheidung und damit in die Supranationalität, die die Europäische Gemeinschaft charakterisiert, in Aussicht gestellt.

Mit dem Vertrag von Amsterdam wurde ein Teil der Inhalte der Dritten Säule vergemeinschaftet, nämlich die Zivilsachen und die Asyl- und Einwanderungsfragen.

Die polizeiliche und justitielle Zusammenarbeit in Strafsachen verblieb im Bereich der Dritten Säule. Die „Dritte Säule“ hat nunmehr eine stark strafrechtliche Akzentuierung. Die Lehre erblickt eine Rechtfertigung der Aufrechterhaltung der Sonderkonstruktion der Dritten Säule (sprich: der Beschlussfassung mit Einstimmigkeit), im einzelstaatlichen Gewaltmonopol, das sich im Strafgedanken ausdrückt.² Die Änderungen durch den Vertrag von Nizza interessieren im gegebenen Zusammenhang nicht, da die zu untersuchenden Dokumente nach den Regeln des Vertrages von Maastricht (Inkrafttreten 1993) und von Amsterdam (Inkrafttreten 1997) beschlossen wurden bzw. zu beschließen gewesen wären.

Die EntschlieÙung des Rates über die rechtmäßige Überwachung des Telekommunikationsverkehrs vom 17.1.1995 (ABl. C 329/01) als Grundlage von ENFOPOL 98

Die EntschlieÙung in ihrer Fassung vom 17.1.1995, welche durch ENFOPOL 98 auf die neuen Technologien, insbesondere auf das Internet und die satellitenunterstützte Mobiltelefonie ausgeweitet werden sollte, stützt sich auf Art K1.9 EUV. Eine EntschlieÙung ist jedoch kein nach Art K vorgesehenes Rechtsinstrument. Die in der Dritten Säule nach Maastricht vorgesehenen Instrumente sind die Gemeinsame Maßnahme, die Festlegung eines Gemeinsamen Standpunktes, die Empfehlung eines Übereinkommens zur Annahme sowie der sogenannte Passerelle - Beschluss. Im oben erwähnten Bericht des Europäischen Parlamentes wird die EntschlieÙung als „Memorandum of Understanding“ bezeichnet und diese Qualifikation trifft die Natur der EntschlieÙung wohl am besten. Eine europarechtliche

² Müller-Graff in Hummer: Die Europäische Union nach dem Vertrag von Amsterdam, Manz 1998, S. 264)

Verbindlichkeit ist somit auszuschließen³ und eine völkerrechtliche Verbindlichkeit kann wohl ebenso wenig konstruiert werden.

Der Inhalt der Ratsentschließung vom 17. Jänner 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs⁴

Die aus zwei Punkten bestehende Entschließung stützt sich auf Art K 1.9 (nunmehr Art. 29 und Art K. 2.2 (nunmehr Art. 30) EUV und enthält in Punkt eins die Ankündigung einer Reihe von Anforderungen an die technische Umsetzung von legalen Überwachungsmöglichkeiten in Fernmeldeverkehr und Telekommunikation, welche die Mitgliedstaaten und ihre „kompetenten Behörden“ haben. Weiters wird in Punkt eins das Bedürfnis der Mitgliedstaaten und ihrer Behörden nach einer umfassenden Autorisierung zur Überwachung des Fernmeldeverkehrs ausgedrückt.

Punkt zwei bekräftigt die Ansicht des Rates, dass die oben erwähnten Anforderungen bei der Definition und Erlassung von Vorschriften, die die Telekommunikation betreffen, in Betracht gezogen werden sollen. Die zuständigen Minister für Telekommunikation sowie für Justiz und Inneres sollen informiert und dazu aufgefordert werden, diese Anforderungen ebenfalls zu beachten.

Die Anforderungen selbst sind in einem Anhang aufgelistet und beschreiben ein umfassendes Zugriffsrecht von (nationalen) Überwachungsbehörden auf telekommunikationsbezogenen Daten eines Teilnehmers am Fernmeldeverkehr, z. B. auch bei Rufumleitung und inklusive der Anfangs- und Endzeiten und der Dauer des Anrufes.

Der Text der Entschließung selbst deutet an, dass dem Rat durchaus bewusst ist, dass er mit einem derartigen Dokument seine Kompetenzen im Rahmen von Art K EUV überschreitet.

Das ENFOPOL-98-Dokument

Der Entwurf für die Überarbeitung der Entschließung aus 1995 war als Anhang zu dieser Entschließung konzipiert, der die einzelnen Anforderungen an die Netzbetreiber und Provider für die Zwecke der rechtmäßigen Überwachung des Telekommunikationsverkehrs im Hinblick auf neue Technologien erweitern sollte. Intendiert war wohl eine „Novelle“, wie sie auch bei verbindlichen Rechtsakten üblich ist. Auf dieses Dokument, von dem wir nicht zu 100% wissen, ob es jemals das Entwurfsstadium verlassen hat, ist nunmehr die Rechtslage nach dem Vertrag von Amsterdam anzuwenden. Hinsichtlich des Regelungsinstrumentariums gab es zwar einige Veränderungen, das Instrument der „Entschließung“ wurde jedoch nicht eingeführt.⁵ Von seiner Rechtsnatur her bleibt der Entwurf für die Überarbeitung daher ebenfalls in der Grauzone zwischen Unionsrecht und Völkerrecht.

³ Zu diesem Ergebnis kommt auch das Rechtsgutachten von Mayer/Pilz an das Forum Mobilkommunikation vom 24. September 1999.

⁴ Laut dem Abdruck in englischer Sprache auf www.statewatch.org/eufbi/eufbireq

⁵ Müller-Graff a.a.O. S. 271;

Was bedeutet die Abkürzung ENFOPOL?

Aus dem Deckblatt des Entwurfes für die Überarbeitung geht hervor, dass das Dokument von der Ratsarbeitsgruppe „Polizeiliche Zusammenarbeit“ erstellt wurde. Vermutlich trägt diese Ratsarbeitsgruppe intern das Acronym „Enfopol“.

Die Ratsarbeitsgruppe ist grundsätzlich ein Hilfsorgan des Rates. Institutionell besteht nur ein Rat, der in verschiedenen Zusammensetzungen (Binnenmarkt, Verkehr, Umwelt, oder eben Telekommunikation) zusammentreten kann. Seine Beschlüsse werden in den Hilfsorganen Ratsarbeitsgruppe (zusammengesetzt aus Experten aus den Verwaltungen der Mitgliedstaaten) und Ausschuss der Ständigen Vertreter (Botschafter bzw. stellvertretende Botschafter der Mitgliedstaaten bei der Europäischen Union⁶) soweit vorbereitet, dass eine Beschlussfassung auf Ebene der Minister möglich wird. Punkte, die bereits im Ausschuss der Ständigen Vertreter Einigung erzielt haben, werden als sogenannte A-Punkte nur mehr formell beschlossen und nicht mehr diskutiert.

Bei der Eingabe des Suchbegriffes „ENFOPOL“ auf dem Website des Rates der Europäischen Union wurde allerdings nur der Jahresbericht über das Fußballrowdytum in den Mitgliedstaaten der EU angezeigt.⁷

Weiterentwicklung

Seit der Entschließung 1995 ist zu keiner neuerlichen Bestätigung auf EU-Ebene gekommen. Wie im zweiten Teil dieser Arbeit gezeigt wird, wurde das Ziel, nationale Behörden mit umfangreichen Überwachungsmaßnahmen auszustatten, auf innerstaatlicher Ebene im Falle Österreichs dennoch erreicht.

Seit der Entschließung 1995 sind insgesamt zehn Entwürfe⁸ für eine Überarbeitung (am bekanntesten ist der dieser Arbeit zugrundeliegende ENFOPOL 98-Entwurf) lanciert worden, zu einer Annahme ist es – wohl auch aufgrund der negativen Berichte in der Presse und die kritischen Stimmen u.a. der Menschenrechtsorganisation Statewatch nicht gekommen.

Zielkonflikte

Die Arbeitsgruppe „Polizeiliche Zusammenarbeit“ hat im November 2000 Kritik an der von der Europäischen Kommission vorgeschlagenen Richtlinie über die Datenverarbeitung und den Schutz der Privatsphäre (COM (2000) 385 vom 12. Juli 2000) geübt, da dieser Entwurf einer Richtlinie vorsieht, dass sämtliche personenbezogenen Verbindungsdaten nach erfolgter Übermittlung entweder gelöscht oder anonymisiert werden sollen. Die Arbeitsgruppe sieht darin eine Behinderung der Überwachungsarbeit und nimmt bezug auf den Entwurf der Cyber Crime Convention des Europarates, welche das Bedürfnis der ermittelnden Behörden, rasch auf die Übermittlungsdaten von Verdächtigen zugreifen zu können, anerkannt und als Vorbedingung für die erfolgreiche Verbrechensaufklärung bezeichnet hat.⁹

Die Charta der Grundrechte der Europäischen Union, welche als Teil des Vertrages von Nizza von den Mitgliedstaaten zu ratifizieren ist, sieht unter Kapitel II „Freiheiten“ in Artikel 8 vor,

⁶ Es wird allerdings nicht der Ausdruck „Botschaft“, sondern Ständige Vertretung bei der EU gebraucht.

⁷ <http://ue.eu.int/dynadoc/>

⁸ Alle Dokumente unter www.statewatch.org/News

⁹ ENFOPOL 71, 27. November 2000

dass jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat und dass Daten nur „... mit Einwilligung der betroffenen Person oder aufgrund einer sonstigen gesetzlich geregelten legitimen Grundlage“ verarbeitet werden dürfen. Ein ausdrücklicher Schutz des Brief- und Fernmeldegeheimnis fehlt in der Charta der Grundrechte. Allerdings beachtet der EuGH in ständiger Rechtsprechung sowohl die in den Verfassungen der Mitgliedstaaten geschützten Grundrechte als auch die Europäische Menschenrechtskonvention als Teil des Europarechts.

ENFOPOL und die Grundrechte

Wenn man davon ausgeht, dass ENFOPOL tatsächlich so umgesetzt wird, dass die zuständigen Behörden die darin vorgesehenen Möglichkeiten der Überwachung des Telekommunikationsverkehrs ohne weitere Voraussetzungen jederzeit in Anspruch nehmen können, würde das einen massiven Grundrechtseingriff in Österreich bewirken.

Dies vor allem deshalb, weil ENFOPOL vorsieht, dass entsprechende Voraussetzungen geschaffen werden, um den „*gesetzlich ermächtigten Behörden*“ den Zugriff und die Information über präzise beschriebenen Telekommunikationsvorgänge zu ermöglichen. Dabei versteht man unter „*gesetzlich ermächtigten Behörden*“ jene Behörden, die nach einzelstaatlichem Recht zur rechtmäßigen Überwachung des Telekommunikationsverkehrs autorisiert sind. Eine nähere Unterscheidung der Behörden in gerichtliche Institutionen, Sicherheitsbehörden oder andere Verwaltungsbehörden, wird im ENFOPOL Papier nicht getroffen. Im schlimmsten Fall würde das bedeuten, dass zB. eine Sicherheitsbehörde auch ohne richterlichen Beschluss jederzeit eine entsprechende Überwachung des Telekommunikationsverkehrs anordnen oder selbst durchführen könnte. Dadurch wären vor allem die Grundrechte des Privat- und Familienlebens wie Art. 8 MRK (Recht auf Achtung des Privatlebens), § 1 DSG (Recht auf Datenschutz) und Art. 10a StGG (Recht auf Achtung des Fernmeldegeheimnisses) massiv betroffen.

Nun zu den einzelnen betroffenen Grundrechten im Detail:

Art 8 MRK (Recht auf Achtung des Privatlebens)

Dieses Recht sichert dem Einzelnen einen privaten Bereich, in dem er seine Persönlichkeit frei entwickeln und entfalten kann. Der weite Schutzbereich des Privatlebens macht sehr unterschiedliche Eingriffsarten denkbar, sodass die tatsächlich geschützten Lebensbereiche erst im Einzelfall durch die Rechtsprechung konkretisiert wurden. Jedenfalls dazu zählt man jedoch den Bereich der informellen Selbstbestimmung, sodass ein Schutz vor Erstellung von Datenprofilen durch Datenverknüpfung und Rasterfahndung gegeben ist. Auch fällt jede Form der privaten Kommunikation, sei es ein persönliches Gespräch oder eine Kommunikation mittels moderner Kommunikationstechnik, darunter¹⁰. Da ENFOPOL die bestehenden Möglichkeiten der Überwachung des Telekommunikationsverkehrs konkretisiert, ist dieses Grundrecht davon sicherlich betroffen.

Ein Eingriff in den Schutzbereich des Art. 8 MRK ist nur zulässig, wenn er gesetzlich vorgesehen ist und in einer demokratischen Gesellschaft zur Erreichung einer der in Art. 8

¹⁰ Vgl. Hannes Tretter, Vorlesungsunterlage für den Lehrgang Informationsrecht, Grundrechte in Österreich, S 23f

Abs. 2 MRK taxativ aufgezählten Zwecke notwendig ist (materieller Gesetzesvorbehalt). Das bedeutet, dass jeder Eingriff dem Verhältnismäßigkeitsgrundsatz unterliegen muss.

Eine Überwachungsmaßnahme wird möglicherweise für die nationale Sicherheit, sowie für die Aufrechterhaltung der öffentlichen Ruhe und Ordnung, jedenfalls aber zur Verhinderung von strafbaren Handlungen im Einzelfall notwendig sein (Lauschangriff). In diesem Fall muss demnach eine Abwägung und Verhältnismäßigkeitsprüfung vorgenommen werden.

Derzeit regeln §§ 149a ff StPO die Voraussetzungen für eine Überwachung des Fernmeldeverkehrs. Eine solche ist insbesondere nur dann zulässig,

- wenn es einen richterlichen Befehl dazu gibt (Ratskammerbeschluss) und
- wenn die Überwachung an besondere Voraussetzungen, insbesondere die Schwere der Tat, die durch die Überwachung aufgeklärt werden soll, geknüpft ist.

Daher wird die Verhältnismäßigkeitsprüfung in Österreich derzeit bereits durch entsprechende Bestimmungen in der StPO vorweggenommen. Zumindest durch die Notwendigkeit eines Beschlusses eines verstärkten Gremiums (Ratskammer), kann man davon ausgehen, dass dieses ein Abwägung vornimmt, und sodann entscheidet, ob der geplante Grundrechtseingriff verhältnismäßig ist oder nicht.

Sollte nun aber das ENFOPOL Konzept nicht entsprechend in dieses nationale System der Verhältnismäßigkeitskontrolle übernommen werden, und jede Sicherheitsbehörde auch ohne weitere Voraussetzungen eine Überwachung anordnen können, so würde dies einen ganz krassen Eingriff in dieses Grundrecht bedeuten.

Das Eintreten dieses „worst-case Szenarios“ ist jedoch insofern eher unwahrscheinlich, als auch sekundäres Unionsrecht wie die Entschließung ENFOPOL an Grundrechte wie die MRK gebunden ist. Durch das Gebot der primärrechtskonformen Interpretation von Sekundärrecht, ist ENFOPOL im Zweifel so zu interpretieren, dass es mit dem Primärrecht, und zwar in concreto mit Art 6 EUV (Union beruht auf dem Grundsatz der Achtung der Menschenrechte) konform geht.

Grundrecht auf Datenschutz (§ 1 Abs. 1 DSG)

Dieses Grundrecht gewährleistet allen natürlichen und juristischen Personen einen Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten. Jedermann hat demnach Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, sofern er daran ein schutzwürdiges Interesse, insbesondere im Hinblick auf Achtung seines Privat- und Familienlebens, hat.

Eingriffe in das Recht auf Geheimhaltung sind unter denselben Voraussetzungen zulässig, wie bereits oben beschrieben (Art. 8 Abs. 2 MRK, materieller Gesetzesvorbehalt). Eine Besonderheit dieses Grundrechtes ist die unmittelbare Drittwirkung, die es entfaltet. Es richtet sich daher nicht nur gegen den Staat, sondern gilt auch für Private untereinander¹¹.

¹¹ Vgl. Hannes Tretter, Vorlesungsunterlage für den Lehrgang Informationsrecht, Grundrechte in Österreich, S 25f

Schutzwürdig sind wie bereits erwähnt alle privaten, familiären, berufliche und geschäftliche personenbezogenen Daten, egal ob sie automationsunterstützt verarbeitet werden oder nicht. Bei automationsunterstützt verarbeiteten Daten hat der Betroffene unter bestimmten Voraussetzungen das Recht auf Auskunft, Richtigstellung und Löschung.

Daten im Zusammenhang mit einer Überwachung des Fernmeldeverkehrs (Gesprächsinhalte, beteiligte Rufnummern etc.) können in der Regel einer bestimmten Person zugeordnet werden und sind daher jedenfalls personenbezogen. Somit gelten für einen Eingriff in dieses Grundrecht dieselben Voraussetzungen und Verhältnismäßigkeitskriterien wie bereits oben bei Art. 8 MRK beschrieben.

Recht auf Achtung des Fernmeldegeheimnis (Art. 10a StGG, § 88 TKG)

Das Fernmeldegeheimnis ist in Art 88 TKG geregelt und besagt im Wesentlichen, dass das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen einer im Rahmen der Nutzung eines öffentlichen Telekommunikationsdienstes erfolgten Kommunikation, sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligte Benutzer unzulässig ist. Dem Fernmeldegeheimnis unterliegen sowohl die Inhaltsdaten und die näheren Umstände der Kommunikation, insbesondere die Tatsache ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, als auch die näheren Umstände von erfolglosen Verbindungsversuchen. Zur Wahrung des Fernmeldegeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet.

Art. 10a StGG bestimmt, dass Eingriffe in das Fernmeldegeheimnis nur aufgrund eines richterlichen und auf Gesetz beruhenden Befehls zulässig sind. Wie bereits oben erwähnt, regeln §§ 149a ff StPO die Voraussetzungen für die Erlassung eines solchen richterlichen Befehls. Die Überwachung des Fernmeldeverkehrs ist demnach nur zulässig, wenn die Aufklärung einer vorsätzlich begangenen, mit mehr als sechs monatigen Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann und der Inhaber der Anlage der Überwachung zustimmt. Ohne Zustimmung des Inhabers der Anlage muss die Strafdrohung entsprechend höher sein; dies ist auch der Fall bei Überwachung von Medienunternehmen.

Da der Begriff „Überwachung des Fernmeldeverkehr“ nicht näher definiert ist, kann man davon ausgehen, dass nicht nur Sprachverkehr sondern auch alle anderen denkbaren Übertragungsinhalte wie Daten, Töne, Bilder, Vermittlungsinformationen, etc. davon erfasst sind.

Wenn die Sicherheitsbehörden ohne weitere Voraussetzungen Überwachungsanordnungen treffen könnten, würde das gegen § 10a StGG verstoßen und wäre nach nationalem Recht schlicht als grundrechtswidrig zu beurteilen.

Zusammenfassung dieser Grundrechtsbetrachtung

Nachdem, wie bereits erwähnt, Sekundärrecht primärrechtskonform auszulegen ist, wird man wohl davon ausgehen können, dass ENFOPOL keine weitergehenden Grundrechtseingriffe als die bereits bestehenden im Zusammenhang mit Überwachungsmaßnahmen beabsichtigt, sondern lediglich anordnet, welche technischen Überwachungsmöglichkeiten von den Mitgliedsstaaten bereitgestellt werden müssen. Wie letztlich von diesen technischen

Möglichkeiten der Überwachung Gebrauch gemacht werden darf, bestimmt sich aber weiterhin nach dem nationalen Recht der Mitgliedsstaaten.

Somit bedeutet ENFOPOL vor allem eine Verpflichtung des österreichischen Staates, diese technischen Möglichkeiten bereitzustellen. Im Wesentlichen wird es auf eine Verpflichtung der Provider zur Implementierung von diversen Überwachungsmöglichkeiten in ihren Netzen hinauslaufen. Die Durchführung der konkreten Überwachungsmaßnahmen richtet sich aber weiterhin nach den bestehenden grundrechtlichen Bestimmungen des nationalen Rechtes, sodass auch keine Änderung des nationalen Rechtes dadurch notwendig wird.

Umsetzung von ENFOPOL in nationales Recht

Durch eine entsprechend Regelung wäre anzuordnen, dass Provider die geforderten technischen Möglichkeiten zur Überwachung einrichten und zur Verfügung stellen. Diese Pflicht befindet sich eigentlich schon in Art. 89 Abs. 1 TKG, wonach der Betreiber nach Maßgabe einer gemäß Abs. 3 erlassenen Verordnung verpflichtet ist, alle Einrichtungen bereitzustellen, die zur Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO erforderlich sind. Bis dato ist jedoch aufgrund massiver Proteste der Betreiber und Öffentlichkeit noch keine diesbezügliche Verordnung erlassen worden, sodass es derzeit noch keine verpflichtenden näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Gewährleistung der Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO gibt. Daher ist dies nach wie vor ein Graubereich, und sind die Behörden teilweise auf den „good will“ der Betreiber und deren bisher implementierten technische Systeme angewiesen.

Durch die Erlassung einer Verordnung gemäß § 89 Abs. 3 TKG könnte ENFOPOL in nationales Recht umgesetzt werden. Allerdings wurden alle bisherigen Verordnungsentwürfe einer „Überwachungsverordnung“ vor allem von den Betreibern, aber auch von der breiten Öffentlichkeit strikt abgelehnt. Der letzte Entwurf sah vor, dass die Telekommunikationsbetreiber eine Schnittstelle in ihre Netze installieren müssen, durch die die Behörden via Standleitung Zugriff auf Verbindungs- und Inhaltsdaten von Handy- und Festnetztelefonaten haben. Verschlüsselte Informationen sollen dabei dechiffriert zur Verfügung gestellt werden. Der Entwurf war so formuliert, dass neben dem Telefonverkehr über ISDN bis GSM, auch Internet-Überwachung unter die Verordnung fallen kann.

Die Arbeiterkammer sowie sonstige Verbraucherschutzverbände führten massive Datenschutzbedenken gegen den Verordnungsentwurf ins Treffen. Die Telekom-Industrie kritisierte am Entwurf vor allem die unklaren Formulierungen und die immensen Kosten für die technische Bereitstellung der Schnittstellen (mehr als vier Milliarden Schilling). Vor allem die Verpflichtung für Betreiber, nach Maßgabe der Verordnung auf eigene Kosten alle Einrichtungen zur Überwachung des Fernmeldeverkehrs bereitzustellen, stellt einen schwerwiegenden **Eingriff in das Grundrecht der Freiheit des Eigentums** dar (Art. 5 StGG) und entspricht auch nicht dem Prinzip der Verhältnismäßigkeit, das im Rahmen eines Grundrechtseingriffes zu beachten wäre. Durch § 89 TKG werden Kosten von Kernaufgaben des Staates, wie etwa Wahrung der öffentlichen Sicherheit, auf private Telekommunikationsbetreiber überwältzt. Diese Belastung kann weder als Gegenleistung für eine besondere Inanspruchnahme der Verwaltung noch als Abgeltung eines adäquaten Vorteiles gelten und verstößt somit möglicherweise auch **gegen den Gleichheitsgrundsatz** (Art. 2 StGG).

Das Infrastrukturministerium will daher in weiteren Arbeitssitzungen mit dem Innen- und Justizministerium den Entwurf nochmals überarbeiten, sodass ein Inkrafttreten am 01.07.2001 wie ursprünglich geplant nicht mehr zu halten sein wird.

Zusammenfassung und Ausblick in die Zukunft

Die ENFOPOL - Papiere und die Existenz der Gruppe „polizeiliche Zusammenarbeit“ wurden 1998 bekannt. Die damit zusammenhängenden Lauschpläne sorgten für großes Aufsehen und wurden nach massiven Protesten der Datenschützer offiziell wieder ad acta gelegt.

Dennoch ist die Richtung klar. Am 29.05.2000 unterzeichneten die Justizminister der EU-Mitgliedsstaaten ein Rechtshilfeübereinkommen, das den Informationsaustausch und die Vernetzung bei Ermittlungen vereinfachen soll.¹² In der Praxis werden im Rechtshilfe-Übereinkommen den ermächtigten Behörden Freiheiten eingeräumt, die in der Geschichte der modernen Kommunikation einmalig sind. Beispielsweise wird es den Polizeibehörden ermöglicht, eine Zielperson (und alle ihre Telefonate) auf fremden Hoheitsgebiet bis zu 12 Tage legal abzuhören, ohne dass ein ordentliches Gericht im Zielland dies genehmigt hätte.

Auch an der Fortsetzung des ENFOPOL Papiers wird zur Zeit in einer Arbeitsgruppe genannt „Lawful Interception“ des European Telecom Standards Institutes (ETSI) gerade gearbeitet. In den sogenannten „ETSI Dossiers“ werden weitere Definitionen von Schnittstellen zur Überwachung ausgearbeitet. Wenn man aktuellen Zeitungsberichten Glauben schenkt, existiert bereits ein neues Dokument, das sogenannte ENFOPOL 38 Geheimpapier, wonach zB. Vermittlungsdaten jedenfalls sieben Jahre hindurch vom Betreiber gespeichert werden sollen. Eine internationale Seilschaft von Polizeibehörden und Geheimdiensten im Verbund mit den Herstellerfirmen strickt also fleißig weiter am einem weltweiten Standard zum Abhören von digitalen Netzen.

Die Akte ENFOPOL ist nicht nur aus grundrechtlicher Sicht und aus der operativen Sicht der Betreiber, denen umfassende Mitwirkungspflichten und daraus entstehende Kosten auferlegt werden sollen, interessant. Sie bildet auch ein anschauliches Beispiel für eine nicht mehr durchhaltbare Informationspolitik, die durch einen mangelnden informationsrechtlichen Zugang geprägt ist. Grund dafür ist die juristische Grauzone, in der das Dokument seiner Rechtsnatur nach angesiedelt ist. Aus dem Zusammenspiel zwischen Rat und Mitgliedstaaten entsteht durch die Veröffentlichung der Dokumente im Internet durch eine NGO auf einmal ein Dreieck der Akteure. Überdies ist die Akte ENFOPOL Teil eines Zielkonfliktes zwischen dem aus rechtsstaatlicher Sicht anerkennenswerten Bemühen um eine erfolgreiche Verbrechensbekämpfung und dem aus rechtsstaatlicher Sicht ebenso schützenswerten Interesse des Einzelnen an der Wahrung seiner Privatsphäre und der Vertraulichkeit seiner (legalen) Geschäftsverbindungen.

Diese Arbeit beruht auf einem Gutachten über ENFOPOL, das Mag. Michael Pilz für das Forum Mobilkommunikation und damit für österreichische Telekombetreiber erstellt hat. Im Übrigen enthält die Arbeit auch Anregungen und Diskussionsstoff aus diversen Arbeitsgruppen zu diesem Thema, an denen die Verfasser selbst teilgenommen haben.

¹² <http://www.statewatch.org/eufbi/enfo19.htm>