ARTIKEL 29-Datenschutzgruppe

/07/DE
WP129

Stellungnahme 1/2007 zum Grünbuch über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden

Angenommen am 9. Januar 2007

Die Datenschutzgruppe wurde durch Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG aufgeführt.

Das Sekretariat wird von der Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft) der Generaldirektion Justiz, Freiheit und Sicherheit der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro LX-46 01/43, gestellt.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie sowie auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14 -

hat folgende Stellungnahme angenommen:

1. Hintergrund

Die Europäische Kommission hat am 1. September 2006 ein Grünbuch über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden (KOM(2006) 474) angenommen („Grünbuch").

Ziel des Grünbuchs ist es, auf europäischer Ebene eine Diskussion über Detektionstechnologien anzuregen und *„konstruktive Beiträge und konkrete Vorschläge"* zu sammeln, um mit vereinten Kräften bei den Detektionstechnologien, die hier im weitesten Sinne zu verstehen sind, voranzukommen. Die Datenschutzgruppe ist zusammen mit anderen Interessierten eingeladen worden, sich an der Konsultation zu beteiligen.

Welche konkreten Schritte und Maßnahmen folgen werden, wird sich anhand der Antworten auf die im Grünbuch angesprochenen Fragen und der weiteren Beiträge zum Grünbuch entscheiden. Einzelne Schritte könnten schon beizeiten unternommen werden, je nachdem, welche Prioritäten sich im Laufe der Konsultation ergeben. So könnte eine Task Force eingesetzt werden, die Maßnahmen in bestimmten Bereichen ausarbeitet, falls die Konsultationsteilnehmer ein entsprechendes Interesse bekunden. Der Task Force könnten Vertreter aus verschiedenen mitgliedstaatlichen Behörden und Sachverständige aus dem Privatsektor angehören.

Die Datenschutzgruppe begrüßt, dass die Kommission in ihrem Grünbuch dem Umstand Rechnung getragen hat, dass politische Strategien, die sich mit Detektionstechnologien und ihrer Anwendung befassen, in vollem Umfang mit den bestehenden Rechtsvorschriften und den Datenschutzgrundsätzen vereinbar sein müssen. Sie will mit ihren nachstehenden Ausführungen zur Grünbuch-Diskussion beitragen.

2. Allgemeine Bemerkungen

Die Datenschutzgruppe hält es zum jetzigen Zeitpunkt für äußerst schwierig, ausführlich und detailliert zum Grünbuch Stellung zu nehmen, da das Grünbuch sehr allgemein gehalten ist. Zweckmäßiger wäre eine Stellungnahme zu einem späteren Zeitpunkt, wenn beispielsweise die im Grünbuch vorgeschlagenen Studien im Entwurf verfügbar sind und Informationen über konkrete Maßnahmen vorliegen.

Dessen ungeachtet befürwortet die Datenschutzgruppe die Idee, den Dialog zwischen Staat und Wirtschaft in Bezug auf die rechtlichen Anforderungen, insbesondere den Datenschutz, zu unterstützen und gleich zu Beginn bei der Planung und Entwicklung detektionstechnologischer Anwendungen zu berücksichtigen, dass möglichst wenig personenbezogene Daten verarbeitet werden[1].

Mit der Entwicklung der Detektionstechnologien geht die Entwicklung von Überwachungssystemen ungeahnten Ausmaßes einher. In diesem Zusammenhang möchte die Datenschutzgruppe daran erinnern, dass die Internationale Datenschutzkonferenz[2] unter dem Motto der „Überwachungsgesellschaft" stand und die Überwachungsproblematik ausführlich unter Datenschutzaspekten diskutiert wurde. Das folgende Zitat, das dem Abschlusskommunique der Konferenz entnommen ist, bringt die wesentlichen Bedenken treffend zum Ausdruck:

„Überwachungsaktivitäten können gut gemeint und nützlich sein. In demokratischen Gesellschaften haben sich diese Aktivitäten bislang relativ gutartig und in kleinen Schritten entwickelt – und nicht unbedingt deshalb, weil Regierungen oder Unternehmen auf ungerechtfertigte Weise in das Leben einzelner Bürger einzudringen beabsichtigen. Einige dieser Aktivitäten sind im Prinzip notwendig und wünschenswert – zum Beispiel zur Bekämpfung von Terrorismus und Schwerkriminalität, zur Verbesserung der Anspruchsberechtigung und des Zugriffs auf öffentliche Dienste sowie zur Verbesserung des Gesundheitswesens. Unkontrollierte oder übermäßige Überwachungsaktivitäten können jedoch unbemerkt zu Risiken führen, die wesentlich mehr als nur eine Beeinträchtigung der Privatsphäre nach sich ziehen. Sie können ein Klima voller Misstrauen hervorrufen und Vertrauen untergraben. Die Erfassung und Verwendung umfangreicher Personendaten durch öffentliche und private Organisationen führt zu Entscheidungen, die einen direkten Einfluss auf das Leben der Menschen haben. Durch eine automatische oder willkürliche Klassifizierung und Profilerstellung können Menschen auf eine Art und Weise stigmatisiert werden, die Gefahren für den Einzelnen mit sich bringen und deren Zugriffsmöglichkeiten auf Dienstleistungen beeinträchtigen. Insbesondere wird das Risiko einer sozialen Ausgrenzung immer größer."

Zur Definition der Detektionstechnologien im Grünbuch gibt die Datenschutzgruppe zu bedenken, dass diese Definition sehr umfassend ist, obwohl es sich um einen Sektor handelt, in dem Präzision und Bestimmbarkeit von großer Bedeutung sind. Dies dürfte jedoch zumindest teilweise auf den Aufbau des Grünbuchs selbst zurückzuführen sein. Von dieser allgemeinen Warte aus sei eingangs noch einmal betont, dass nicht alles, was technisch machbar ist, auch gesellschaftlich und politisch akzeptabel, ethisch vertretbar und rechtlich zulässig ist.

Alle einschlägigen Vorschriften und Garantien des europäischen Datenschutzrechts – wie die Europäische Menschenrechtskonvention[3], das Europäische Übereinkommen zum Schutz des

---

[1] Vgl. das Abschlusskommunique der 28. Internationalen Konferenz der Datenschutzbeauftragten, 2./3. November 2006, London (http://ico.crl.uk.com/files/FinalConf.pdf): „*Die Auswirkungen sollten systematisch bewertet werden. Derartige Bewertungen würden nicht nur eine Beurteilung der Beeinträchtigung unserer Privatsphäre beinhalten, sondern darüber hinaus auch die gesellschaftlichen Auswirkungen sowie die Möglichkeiten zur Minimierung unerwünschter Folgen für den Einzelnen und die Gesellschaft identifizieren."*

[2] 28. Internationale Konferenz der Datenschutzbeauftragten, 2./3. November 2006, London: http://ico.crl.uk.com.

[3] Es sei darauf hingewiesen, dass die Grundsätze der Europäischen Menschenrechtskonvention in der Empfehlung R(87)15 über die Nutzung personenbezogener Daten im Polizeibereich weiter konkretisiert worden sind. So heißt es in Artikel 1 Absatz 2 dieser Empfehlung: „*new technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation*" (neue technische Medien für die Verarbeitung von Daten dürfen erst eingeführt werden, wenn alle geeigneten Vorkehrungen getroffen wurden, um zu gewährleisten, dass ihr Einsatz mit dem geltenden Datenschutzrecht

Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV-Nr. 108), die Datenschutzrichtlinie sowie die Datenschutzrichtlinie für elektronische Kommunikation - sollten daher in die weiteren Diskussionen und Arbeiten zu den Detektionstechnologien einbezogen und beachtet werden.

Nach Auffassung der Datenschutzgruppe ist es für künftige Evaluierungen überdies unerlässlich, klar zwischen den verschiedenen Arten von Detektionstechnologien zu unterscheiden (d. h. CCTV, RFID-Tags, Biometrie usw.), um für jede Technik die geeignete Datenschutzlösung zu finden. Die Einführung von Überwachungssystemen mit den entsprechenden Vorschriften für die Datenverarbeitung muss mit einer klaren Zweckbestimmung der Datenverarbeitung einhergehen (Erhebung, Erfassung, Speicherung und Archivierung, Aufzeichnung und spätere Verwendung usw.). Auf diese Weise können die Datenschutzbehörden feststellen, ob die Erhebung der Daten für diese Zwecke geeignet, relevant und verhältnismäßig ist. Eine solche Prüfung ist notwendig, um sich zu vergewissern, dass Detektionstechnologien in einer bestimmten Situation nicht in die Privatsphäre eindringen und der Zweck nicht mit anderen, weniger einschneidenden Mitteln hätte erreicht werden können.

3. Anmerkungen zu einzelnen Kapiteln

Einleitung

Die Datenschutzgruppe begrüßt insbesondere den Hinweis auf Seite 6 des Grünbuchs, *„dass bei der Konzeption, der Realisierung und dem Einsatz solcher Technologien sowie bei den Rechtsvorschriften und Maßnahmen, mit denen diese Technologien gefördert und geregelt werden sollen, die Grundrechte, wie sie in der EU-Grundrechtscharta und in der Menschenrechtskonvention niedergelegt sind, uneingeschränkt zu beachten sind“* und dass der „S*chutz personenbezogener Daten und das Recht auf Achtung des Privatlebens […] besondere Beachtung [verdienen]“*. Diese Feststellung ist ein geeigneter Ausgangspunkt für die Ausführungen der Datenschutzgruppe. In diesem Zusammenhang sei auf die verschiedenen von der Datenschutzgruppe herausgegebenen Dokumente verwiesen, in denen betont wird, dass jede öffentliche Maßnahme, mit der Grundrechte eingeschränkt werden, in einer demokratischen Gesellschaft ausdrücklich im Gesetz vorgesehen und zum Schutz eines wichtigen öffentlichen Interesses notwendig sein muss (vgl. insbesondere die Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus[4]).

Die Gruppe weist ferner darauf hin, dass der Grundsatz der Verhältnismäßigkeit im Zusammenhang mit jeder Maßnahme zu beachten ist, die das Grundrecht auf Schutz der Privatsphäre gemäß Artikel 8 der Europäischen Menschenrechtskonvention und der einschlägigen Rechtsprechung beschneidet. Dies beinhaltet unter anderem die Verpflichtung nachzuweisen, dass die ergriffenen Maßnahmen einem „zwingenden gesellschaftlichen Bedarf“ entsprechen. Maßnahmen, die lediglich „nützlich“ oder „wünschenswert“ sind, dürfen die Grundrechte und –freiheiten nicht beschränken.

Diese Feststellung zieht gewisse Konsequenzen nach sich, die bei der Abfassung des Grünbuchs anscheinend nicht in vollem Umfang beherzigt wurden, was insbesondere aus der Liste der Vorschläge/Fragen deutlich wird. Dies gilt u. a. für die Notwendigkeit, dafür Sorge zu tragen, dass

---

inhaltlich vereinbar ist). Darüber hinaus ist die Möglichkeit einer Vorabüberprüfung durch die Aufsichtsbehörde vorgesehen.

[4] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53de.pdf.

bereits in die Entwicklung einer bestimmten Detektionstechnik zweckorientierte Datenschutzgrundsätze einfließen.

Eine weitere Überlegung gilt der im Grünbuch offensichtlich angestellten Gleichstellung zwischen „Terrorismus“ und „anderen Formen der Kriminalität“ (vgl. u. a. S. 4). Terrorismus sollte sehr genau definiert werden; beide Begriffe sind in jedem Fall voneinander zu trennen, da sie unterschiedliche Anforderungen sowohl an die Sicherheit und an die Detektionstechnologien als auch an entsprechende Forschungsarbeiten stellen.

Die folgenden Vorschläge und Bemerkungen betreffen Fragen, die aus datenschutzrechtlicher Sicht von besonderer Bedeutung sind.

I. Normung, Standardisierung und Sicherheitsforschung

Im Bereich der Forschung kommt es nach Auffassung der Datenschutzgruppe bei der Entwicklung technischer Standards und Normen vordringlich darauf an, dass die Verarbeitung personenbezogener Daten im Einklang mit geltendem Recht erfolgt. Dies ist ein Bereich, in dem die aktive Mitarbeit der Datenschutzbehörden gesucht werden könnte und sollte. Des Weiteren möchte die Datenschutzgruppe betonen, dass die Beachtung des Datenminimierungsprinzips hierzu unerlässlich ist. Anzustreben sind Lösungen, bei denen so wenig Personendaten wie möglich verarbeitet werden müssen. Wo immer dies möglich ist, sollten technologische Lösungen bevorzugt werden, bei denen sich das gewünschte Ziel auch ohne die Verarbeitung personenbezogener Daten erreichen lässt. Dies sollte bei allen künftigen Forschungs- und Entwicklungsarbeiten im Bereich der Detektionstechnologien als grundsätzliche Zielvorgabe festgeschrieben werden. Ferner ist zu überlegen, ob die Minimierung der Verarbeitung personenbezogener Daten nicht als Best Practice (Teil III.1 des Grünbuchs) gelten sollte.

Zur Sicherheitsforschung enthält der im Grünbuch erwähnte Bericht des Europäischen Beirats für Sicherheitsforschung (ESRAB) interessante Hinweise für künftige Forschungsarbeiten in diesem Bereich. Nach Ansicht der Datenschutzgruppe ist es aufschlussreich, dass in dem Bericht als ein wesentliches Ergebnis festgestellt wird, dass Leitprinzip des Programms die Achtung der Privatsphäre und der bürgerlichen Freiheiten sein sollte. Die Gruppe schließt sich dieser Auffassung voll und ganz an.

Selbstverständlich wäre die Datenschutzgruppe daran interessiert, *„bewährte Praktiken für den Einsatz und den Umgang mit Daten und Informationen […] zu ermitteln und auszutauschen, um auf diese Weise den einschlägigen Rechtsvorschriften und Regeln in vollem Umfang genügen zu können“*. Hier sei ergänzend angemerkt, dass dies sowohl für die Vorschriften auf europäischer Ebene als auch für die Vorschriften auf nationaler Ebene gilt.

II. Bedarf und Lösungen

<u>Bedarf und Lösungen aus technologischer Sicht</u>
Es sollte geklärt werden, wie die abrufbare EU-Liste/-Datenbank, die Aufschluss über den konkreten Bedarf der Sicherheitsbehörden und gleichzeitig über das Angebot des privaten Sektors geben soll, funktionieren soll. Die Datenschutzgruppe weist darauf hin, dass ausreichende Vorkehrungen getroffen werden müssen, damit gewährleistet ist, dass Entscheidungen über Sicherheitslösungen in völlig transparenter Weise getroffen werden.

<u>Tragbare, mobile Lösungen/Interoperabilität der Systeme</u>

Die Datenschutzgruppe ist durchaus bereit, die von der Kommission angeführten „rechtlichen und sonstigen Grenzen“ für die Interoperabilität der Systeme in der EU genauer zu beleuchten. Sie teilt die Einschätzung des Europäischen Datenschutzbeauftragten (EDSB) in seiner Stellungnahme[5] zu der Kommissionsmitteilung über die Interoperabilität der europäischen Datenbanken, dass Interoperabilität bedeutende rechtliche Auswirkungen hat: „*Es liegt natürlich auf der Hand, dass dadurch, dass der Zugang zu oder der Austausch von Daten technisch ermöglicht wird, der tatsächliche Zugang zu diesen Daten bzw. ihr Austausch in vielen Fällen beträchtlich stimuliert wird“*. Unterschiedliche Arten der Interoperabilität (allgemeine Nutzung großer IT-Systeme, Zusammenführung von Datenbanken, Möglichkeiten des Zugangs zu oder des Austauschs von Daten), so der Datenschutzbeauftragte, erfordern unterschiedliche Sicherheitsmechanismen und Bedingungen. Die Interoperabilität der Systeme ist unter gebührender Beachtung der Datenschutzgrundsätze und insbesondere des Grundsatzes der Eingrenzung des Verwendungszwecks umzusetzen. Dies ist jedoch nicht als Einschränkung zu verstehen, sondern eher als vernünftiger Weg, wie vorab mit grundlegenden Fragen umzugehen ist.

Die Datenschutzgruppe möchte in diesbezügliche Initiativen auf EU-Ebene einbezogen werden.

[5] http://www.edps.europa.eu/legislation/Comments/06-03-10_Comments_interoperability_DE.pdf.

Integration von Informationen und Verbesserung der Datenanalyse

Es sollte deutlich gemacht werden, dass eine Verbesserung der Datenanalyse nicht bedeuten darf, dass unbeschränkt Daten abgeglichen werden oder eine Datenbank nach der anderen abgefragt wird. Datensparsamkeit und Zweckbestimmung sollten als Vorgaben in die Datenanalysesysteme integriert werden. Die Datenschutzgruppe verweist auf die Vorkehrungen und Leitlinien, die im Zusammenhang mit Europols Analysedateien entwickelt wurden und als Vorbild für die Einhaltung der Datenschutzgrundsätze in diesem Bereich dienen können.

III. Verwendung und Zertifizierung von Instrumenten und Ausrüstungen

Einsatz von Data- und Textminingsystemen

Die Datenschutzgruppe unterstützt nachdrücklich die Forderung, dass die Grundrechte und Datenschutzgrundsätze einzuhalten sind, und betont insbesondere die Notwendigkeit, dass Detektionssysteme bereits entsprechend auszulegen sind.

Zwar könnte sich die Gruppe der Auffassung anschließen, dass bewährte Praktiken und Informationen über den Einsatz von Data- und Textminingsystemen ausgetauscht werden sollten, doch wäre zuvor zu klären, was mit dem Hinweis auf die *„ungenutzten Kapazitäten*" der Mitgliedstaaten oder europäischen Einrichtungen gemeint ist, *„um den Mitgliedstaaten, die nicht über diese Technologie verfügen, bei der Bearbeitung ihrer Dokumente zu helfen"*. Hier muss deutlich gemacht werden, dass jeder Einsatz dieser Systeme auf einer geeigneten Rechtsgrundlage basieren muss. Zu klären ist auch, was unter einem *„europäischen oder regionalen Zentrum für Data- und Textmining*" zu verstehen ist. Ein solches Zentrum sollte nicht auf eine Art ‚Clearinghouse' für Datenextraktionstechniken beschränkt sein.

Die Datenschutzgruppe bedauert, dass im Zusammenhang mit den bewährten Praktiken für Data- und Textmining ein Hinweis auf den Datenschutz fehlt. Es ist lediglich davon die Rede, dass Informationen und Best Practices auszutauschen sind. Bewährte Praktiken müssen nach Auffassung der Gruppe neben anderen Sicherheitsvorkehrungen auch eine obligatorische Schulung aller Beteiligten in Datenschutzfragen enthalten.

Nützlich wäre eine Untersuchung, inwieweit Datamining-Systeme einen Beitrag zur Terrorismusbekämpfung leisten könnten, da u. U. auch andere Techniken hierfür geeignet sein könnten. Systeme, die weniger stark in die Privatsphäre eindringen, sollten stets Vorrang vor Systemen erhalten, die eine große Menge von Personendaten verarbeiten.

Was die Vertraulichkeit der Kommunikation anbelangt, so möchte die Datenschutzgruppe an die Anwendung der Datenschutzrichtlinie für die elektronische Kommunikation erinnern sowie an ihre Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post[6] und die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zur Überwachung des Brief- und Telefonverkehrs[7].

Die Datenschutzgruppe erinnert ferner an ihre Stellungnahme 3/99[8] betreffend die Informationen des öffentlichen Sektors und den Schutz personenbezogener Daten (Konsultationsbeitrag zum

[6] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_de.pdf .

[7] Z. B. EGMR, *Klass/Deutschland*, 6. September 1978, EGMR, *Malone/Frankreich*, 2. August 1984, *Kruslin/Frankreich*, 24. April 1990, *Huvig/Frankreich*, 24. April 1990, *A/Frankreich*, 23. November 1993, *Halford/Vereinigtes Königreich*, 25. Juni 1997, *Kopp/Schweiz*, 25. März 1998, *Amann/Schweiz*, 16. Februar 2000.

[8] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp20de.pdf.

Grünbuch „Informationen des öffentlichen Sektors - Eine Schlüsselressource für Europa“ KOM(1998) 585). Darin führte die Gruppe aus: *„Die Digitalisierung der Information und der Volltextabruf gestatten eine unendliche Vervielfältigung der Möglichkeiten, Daten abzufragen und zu sichten, wobei die Verbreitung über Internet die Gefahren der Datenpiraterie und -zweckentfremdung vergrößert. Darüber hinaus wird die Verknüpfung von Daten, die aus unterschiedlichen Quellen öffentlich zugänglich gemacht werden, mit Hilfe der Digitalisierung sehr erleichtert. Auf diese Weise lassen sich vor allem Profile über die Situation und das Verhalten von Einzelpersonen erstellen. Ferner muß der Tatsache besondere Aufmerksamkeit geschenkt werden, daß die neuen Technologien des „data warehousing“ und des „data mining“, wenn der Öffentlichkeit personenbezogene Daten zur Verfügung gestellt werden, starke Impulse erfahren. Sie ermöglichen es, Daten ohne jede vorherige Spezifikation der Zweckbestimmung zu sammeln und die Zweckbestimmung erst bei der Auswertung zu definieren. So muß also alles berücksichtigt werden, was im Datenbereich technisch möglich ist.”*

Prüfung und Zertifizierung der Qualität von Instrumenten und Ausrüstungen
Das „Netzwerk nationaler Zertifizierungsstellen“ könnte eine brauchbare Lösung sein, doch müssten auch die Datenschutzbehörden und entsprechende Fachleute einbezogen werden.

IV. Studien

Die Datenschutzgruppe kann sich dem vorgeschlagenen Vorgehen anschließen, doch sollte bei jeder neuen Detektionstechnologie eine Datenschutz-Folgenabschätzung erstellt werden, um den Bedarf dieser neuen Technologie zu beurteilen und sich ein klares Bild von den gesellschaftlichen wie finanziellen Kosten zu verschaffen.

Durchaus von Nutzen wären einige der in Kapitel IV genannten Studien mit datenschutzrechtlichem Bezug: 3) Rechtsvorschriften für die Verwendung bestimmter Detektionstechnologien, 4) Einsatz bestimmter Detektionstechnologien in der Praxis, 5) Rechtsvorschriften für den Einsatz von Personendetektionssystemen (einschließlich Personenüberwachung) in der EU und 6) Akzeptanz der Personendetektion (einschließlich Personenüberwachung und Einsatz von Biometrie) in der EU.

V. Umsetzung der Konsultationsergebnisse

Die Datenschutzgruppe hält es für wichtig, sich an den Folgearbeiten im Anschluss an die Konsultation zu beteiligen. Hier wäre ein Aktionsplan hilfreich.

4. Fazit

Die Datenschutzgruppe hat die Aufforderung begrüßt, zum Grünbuch über Detektionstechnologien Stellung zu nehmen und sich am Konsultationsprozess zu beteiligen. Es ist zum jetzigen Zeitpunkt jedoch sehr schwierig, eine eingehende datenschutzrechtliche Analyse der Detektionstechnologien vorzunehmen, da das Grünbuch eher vage abgefasst ist und sich sehr allgemein mit Detektionstechnologien befasst.

Die Formulierung bewährter Praktiken kann zwar insofern hilfreich sein, als hierdurch eine Verbindung hergestellt wird zwischen den rechtlichen Vorgaben (z. B. Datenschutzbestimmungen und Richtlinie über elektronische Kommunikation) und der Anwendung einer Technologie, doch lassen sich diese Praktiken nur anhand recht konkreter Beispiele beurteilen, die die besonderen Folgen erkennen lassen, die sich aus dem Einsatz einer bestimmten Technologie ergeben. Es sei

allerdings darauf hingewiesen, dass die Datenschutzrichtlinie immer dann Anwendung findet, wenn es um die Erhebung oder Verarbeitung personenbezogener Daten geht *(„alle Informationen über eine bestimmte oder bestimmbare natürliche Person“*) und deren Verwendung durch Gemeinschaftsrecht geregelt ist.

Zusammenfassend lassen sich der Richtlinie mehrere Grundprinzipien entnehmen:

i) Der Zweck der Erhebung personenbezogener Daten sollte von Anfang an genau bestimmt werden, und die Daten sollten nicht auf eine Weise weiterverarbeitet werden, die mit diesem Zweck unvereinbar ist.

ii) Eine Technologie an sich ist nicht unbedingt problematisch, doch muss die Erhebung und Verwendung personenbezogener Daten rechtmäßig sein. Dies bedeutet, dass auf den Einsatz einer bestimmten Technologie sowie auf die Erhebung und Verwendung der Daten hingewiesen werden sollte (z. B. in dem bereits gut dokumentierten Fall der CCTV-Überwachung).

iii) Es sollten keine personenbezogenen Daten erhoben werden, die für den Erhebungszweck irrelevant sind. Auch sollten personenbezogene Daten nicht länger als nötig aufbewahrt werden. Der Entwicklung von Technologien, die der Erkennung von Stoffen und nicht von Personen dienen, sollte mehr Bedeutung als bisher beigemessen werden.

Die Datenschutzgruppe behält sich vor, zu künftigen Arbeiten in diesem Bereich Stellung zu nehmen.

Für die Datenschutzgruppe
Der Vorsitzende
Peter Schaar