KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 16.6.2004
KOM(2004) 429 endgültig

MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT

Betreffend den verbesserten Zugang zu Informationen für Strafverfolgungsbehörden

INHALTSVERZEICHNIS

MITTEILUNG DER KOMMISSION AN DEN RAT UND DAS EUROPÄISCHE PARLAMENT

**BETREFFEND DEN VERBESSERTEN ZUGANG ZU INFORMATIONEN FÜR STRAFVERFOLGUNGSBEHÖRDEN*
*(EU INFORMATIONSPOLITIK)***

KAPITEL I – EINFÜHRUNG, GRUNDPRINZIP UND POLITISCHER ZUSAMMENHANG

Die Erklärung des Europäischen Rates zum Terrorismus[1] weist den Rat an, gesetzgeberische Maßnahmen zur Vereinfachung des Austausches von Informationen und *Intelligence* zwischen den Strafverfolgungsbehörden der Mitgliedstaaten zu prüfen. Die Kommission wird aufgefordert, dem Europäischen Rat im Juni zum Zwecke der Terrorismusbekämpfung Vorschläge in Bezug auf den Austausch personenbezogener Informationen und die Nutzung von Passagierinformationen zu unterbreiten. Die Vorschläge der Kommission sollen auch Bestimmungen enthalten, die den nationalen Strafverfolgungsbehörden den Zugang zu den europäischen Informationssystemen ermöglichen.

Die vorliegende Mitteilung ist ein erster Beitrag der Kommission in Reaktion auf den Wunsch des Rates.

In dieser Mitteilung stellt die Kommission die Elemente dar, die für einen freien, besser als bisher strukturierten Verkehr von Informationen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten wesentlich sind. Gegenwärtig bestehen Hindernisse für den freien Verkehr von Informationen, die den Rat unter anderem dazu veranlassen, die dritte Runde gegenseitiger Evaluierungen der Überprüfung des „Austausches von Informationen und *Intelligence* zwischen Europol und den Mitgliedstaaten sowie zwischen den Mitgliedstaaten“ zu widmen. Die Aufsplitterung von Informationen und das Fehlen einer klaren Politik zu den Informationskanälen behindern den Informationsaustausch. Die Herausforderungen, die national bei der Überwindung der Informationszersplitterung auf verschiedene Ministerien bestehen, werden zwischen den Mitgliedstaaten durch rechtliche, technische und praktische, den Austausch behindernde Probleme verschärft. Die Kommission schlägt vor, eine vollständige Bestandsaufnahme über die Bedingungen für den Zugang zu Informationen und eine breit angelegte, offene Anhörung aller interessierten Parteien, insbesondere des Europäischen Datenschutzbeauftragten, vorzunehmen, um ein genaueres Bild von diesen Hindernissen zu erhalten. Die Mitteilung will auch die Mittel zur Vermeidung der Materialisierung der Hauptbedrohungen, wie zum Beispiel Terrorismus, aufzeigen, indem sie das Konzept

---

* Anmerkung zur Übersetzung: Für den in der englischen Originalfassung dieser Mitteilung verwendeten Begriff „law enforcement“ gibt es kein den Sinn genau widerspiegelndes, gebräuchliches deutsches Wort. Der Begriff wird hier mit „Strafverfolgung“ übersetzt, da dieser Begriff unter den gebräuchlichen deutschen Rechtstermini dem Begriff „law enforcement“ am nächsten kommt.

1 Europäischer Rat vom 25. März 2004 *Erklärung zur Bekämpfung des Terrorismus*.

Intelligence-gestützter Strafverfolgung auf EU-Ebene vorstellt. Sie legt anhand einer entsprechenden Planung dar, wie man dies erreicht, und kündigt gesetzgeberische Schritte zur Behebung spezifischer rechtlicher Probleme an. Der Schwerpunkt dieser Mitteilung liegt auf der Verbesserung des Zugangs zu erforderlichen und relevanten Informationen sowie auf den allgemeinen Konzepten für die Einführung *Intelligence*-gestützter Strafverfolgung auf der Ebene der EU. Dies wird auch Folgen für die internationale Rolle haben, die die EU einnehmen kann.

Diese zwei Elemente sind die Hauptbestandteile der EU-Informationspolitik für Strafverfolgungszwecke. Gemeinsame Maßnahmen auf diesen Gebieten werden den voranschreitenden Aufbau des Raumes der Freiheit, der Sicherheit und des Rechts unterstützen, in dem der freie Personenverkehr auch im Angesicht der neuen Sicherheitsherausforderungen sichergestellt bleibt, die Terrorismus sowie andere Formen schweren und organisierten Verbrechens für die Union als Ganzes darstellen. Die Effizienz der Strafverfolgungstätigkeit sollte auf der Beachtung der Menschenrechte und Grundfreiheiten aufbauen, die durch die internationalen und europäischen sowie allen Mitgliedstaaten gemeinsamen Verfassungstraditionen geschützt werden. Außerdem wird die Kommission bei der Realisierung dieser Politik sicherstellen, dass Gemeinschaftsrecht und –politiken gebührend berücksichtigt werden. Insbesondere darf solch eine Politik keine Rechtsunsicherheit erzeugen oder die Industrie keinen übermäßigen wirtschaftlichen Belastungen aussetzen.

Die Kommission ruft die Mitgliedstaaten und betroffenen Interessengruppen auf, sich der folgenden mutigen, kooperativen Maßnahmen anzunehmen:

Erstens müssen die unerlässlichen Schritte unternommen werden, damit die Strafverfolgungsbehörden in der EU Zugang zu allen erforderlichen und relevanten Daten und Informationen erhalten, um Terrorismus und andere Formen schweren oder organisierten Verbrechens sowie die davon ausgehenden Bedrohungen zu verhindern und zu bekämpfen. In diesem Zusammenhang muss berücksichtigt werden, dass kriminelle Handlungen oftmals nicht in die Kategorie „schwer oder organisiert“ zu fallen scheinen, jedoch hierzu führen oder damit verknüpft sein können.

Zweitens muss hochwertige verbrechensbezogene Informationsverarbeitung in der EU geschaffen und genutzt werden. Wissen, das in diesem Prozess verfügbar werden wird, wird die politische Ebene bei der konzertierten Festlegung von kriminalpolitischen Prioritäten der EU unterstützen und den Strafverfolgungsorganen dabei helfen, den Verbrechen und Bedrohungen wirksam zu begegnen, die das Leben, die körperliche Unversehrtheit und die Sicherheit unserer Bürger gefährden.

Drittens muss das Vertrauen zwischen Strafverfolgungsbehörden gestärkt werden. Die Einführung gemeinsamer Bedingungen etwa für den Zugang zu Datensystemen und die Weitergabe von *know how* wird zur Begründung einer gemeinsamen Informationspolitikplattform beitragen, insbesondere indem objektive Hindernisse für die effektive Weitergabe von Informationen und Informationsverarbeitungsergebnissen beseitigt werden.

Mehrere Überlegungen treiben die EU-Informationspolitik für Strafverfolgungszwecke an. Sie hängen zusammen mit dem wachsenden

Bewusstsein für die Verletzbarkeit der Union durch Bedrohungen, die etwa terroristische Aktivitäten für die Abhängigkeit der Union von Verbundnetzwerken darstellen; mit der Notwendigkeit, verstärkte Informationsflüsse zwischen den zuständigen Stellen einzurichten; mit den Vorteilen neuer Technologien und wissensgestützter Techniken bei der Förderung von Strafverfolgungsmaßnahmen und - gleichzeitig – verbessertem Datenschutz und erhöhter Sicherheit bei damit zusammenhängenden Überwachungs- und Aufsichtsmechanismen.

Diese Mitteilung bezweckt eine Verbesserung des Informationsaustausches zwischen allen Strafverfolgungsbehörden, d.h. nicht nur zwischen Polizeibehörden, sondern auch zwischen Zollbehörden, Meldestellen für Geldwäsche („Financial Intelligence Units"), den Gerichts- und sonstigen Strafverfolgungsbehörden und allen anderen öffentlichen Einrichtungen, die an einem Prozess teilnehmen, der von der frühen Aufdeckung von Sicherheitsbedrohungen und Straftaten bis zur Verurteilung und Bestrafung der Täter reicht. Die fundamentale Rolle, die staatliche Sicherheits- und nationale Aufklärungseinrichtungen hierbei spielen, ist unbestritten. Die zahlreichen, miteinander verbundenen Herausforderungen, denen die EU-Informationspolitik für Strafverfolgungszwecke begegnen soll, werden in den nachfolgenden Absätzen dargestellt.

Schließlich muss wegen des internationalen Wesens der Herausforderung des Terrorismus und des organisierten Verbrechens, der wir entgegenzutreten versuchen, die Außendimension in Betracht gezogen werden. Andere Länder haben ihre eigenen Informationspolitiken für Strafverfolgungszwecke entwickelt oder könnten dies in Zukunft tun, und es gab schon Fälle, in denen diese Politiken Auswirkungen auf EU-Bürger und -Unternehmer hatten. Gegenseitigkeitsaspekte können ebenfalls eine Rolle spielen, und spezialisierte Foren müssen unter Umständen nach multilateralen Lösungen suchen. Die Auswirkung, die die EU Politik auf Drittstaatsangehörige haben würde, muss auch hinreichend in Betracht gezogen werden, um sicherzustellen, dass die Strafverfolgungszusammenarbeit mit diesen Ländern nicht beeinträchtigt wird und dass die Rechte der Bürger ohne Diskriminierung respektiert werden.

Diese Politik wird erstens den Strafverfolgungsbehörden in der EU alle erforderlichen und relevanten Daten und Informationen zugänglich machen, um Terrorismus und andere Formen schweren oder organisierten Verbrechens sowie die davon ausgehenden Bedrohungen zu verhindern und zu bekämpfen[2]. Sie wird zweitens die Schaffung und Nutzung hochwertiger Kriminalaufklärungsarbeit vorantreiben, um die politische Entscheidungsfindung auf EU-Ebene zu unterstützen und den Strafverfolgungsorganen dabei zu helfen, diesen Verbrechen wirksam zu begegnen. Drittens wird der Vertrauensaufbau zwischen den zuständigen Stellen unterstützt. Bei der Realisierung dieser Politik werden auch die Gemeinschaftspolitiken und gemeinschaftlichen Rechtsinstrumente berücksichtigt; insbesondere wird diese Politik vollständig die Grundrechte achten.

Die Informationspolitik muss folgende Elemente berücksichtigen:

---

[2] Der Begriff "Daten" oder "Informationen" soll in dieser Mitteilung stets, falls nicht anders angegeben, "Daten, Information und Intelligence" bedeuten. Der Begriff „intelligence" bezieht sich auf kriminalistische „Intelligence".

- Die **Sicherheits**herausforderung erfordert zwingend eine bislang beispiellose gemeinsame und konzertierte Aktion; die nationalen Strafverfolgungsbehörden und die nationalen Regierungen, die europäische Exekutive und Legislative sowie andere Gremien auf europäischer und internationaler Ebene sind hier gefordert.

- Die **menschenrechtliche** Herausforderung läuft hinaus auf die Herstellung eines angemessenen Gleichgewichts zwischen wirksamem Datenschutz und gebührender Achtung weiterer Grundrechte einerseits sowie intensiver Nutzung von Strafverfolgungsinformationen andererseits, die auf den Schutz wesentlicher öffentlicher Interessen wie der nationalen Sicherheit sowie der Verhinderung, Aufklärung und Verfolgung von Verbrechen abzielen.

- Was die **Technologie** betrifft, so bedarf es kompatibler, gegen unrechtmäßigen Zugang geschützter Informationssysteme, einschließlich der Überwachung und Beaufsichtigung der Datenverarbeitung sowie der Überprüfung von Untersuchungen. „Crime Proofing" von Informationstechnologien sollte deren Schwächen und Gelegenheiten für kriminelle Handlungen offen legen und sich auf die Datenanalyse, wie zum Beispiel Risikobewertung und „Profiling", konzentrieren.

- Zur Erleichterung effektiver **Zusammenarbeit** werden gemeinsame Normen für Sammlung, Speicherung, Analyse und Austausch von Informationen den Aufbau von Vertrauen zwischen den zuständigen Stellen sowohl auf nationaler als auch auf EU-Ebene entscheidend unterstützen.

- Zur **Umsetzung** eines mehrstufigen Ansatzes werden langfristige und nachhaltige kooperative Maßnahmen nötig sein.

KAPITEL II – ZU EINEM BESSEREN DATENZUGRIFF UND EINER EINFÜHRUNG „INTELLIGENCE"-GESTÜTZTER STRAFVERFOLGUNG AUF EU-EBENE

2.1. Strategische Ziele

Das Ziel dieser Mitteilung besteht darin, eine europäische Informationspolitik für Strafverfolgungszwecke zu schaffen, die zur Verwirklichung der Ziele des Art. 29 EUV beiträgt, indem bessere Informationen über sichere Kanäle für die **bestehende Strafverfolgungszusammenarbeit** verfügbar gemacht und - untermauert vom erforderlichen **Vertrauensaufbau -** die Grundlagen für die **Einrichtung einer effektiven „*Intelligence*-gestützten" Strafverfolgung** auf lokaler, nationaler und europäischer Ebene gelegt werden**.** Das politische Konzept umfasst gesetzliche, technische und organisatorische Maßnahmen, die in ihrer Gesamtheit den zuständigen Behörden einen Rahmen für die Zusammenarbeit bereitstellen, um den Zugang zu und die Verarbeitung von für die Strafverfolgung relevanten Daten und den Informationsverarbeitungsprozess zu erleichtern.

Bei detaillierterer Betrachtung der Informationspolitik stehen folgende Ziele im Vordergrund:

- optimierter Zugriff auf Informationen, um Kernanliegen der Strafverfolgung zu fördern und verbrechensbezogene Informationsverarbeitung zu ermöglichen;

- Gewährleistung, dass Daten, die für andere als Strafverfolgungszwecke erhoben wurden, verfügbar sind, solange dies im Hinblick auf die speziellen und legitimen Zwecke, die verfolgt werden, geeignet, erforderlich und verhältnismäßig ist[3];

- Festlegung oder, soweit horizontale Standards bereits bestehen, Förderung der effektiven Nutzung gemeinsamer horizontaler Standards für den Zugriff auf Daten, die Löschung, Vertraulichkeit von Informationen, Verlässlichkeit, Datensicherheit und –schutz sowie von Standards für die Interoperabilität von nationalen und internationalen Datenbanken;

- Festlegung gemeinsamer „*Intelligence*-Formate" zur Unterstützung politischer und operationeller Entscheidungsprozesse sowie Förderung der Entwicklung und Anwendung gleichwertiger Methoden der Analyse von z.B. kriminellen Netzwerken, Bedrohungspotentialen, -risiken und -profilen, zusätzlich unterstützt von wirtschaftlichen Schadenseinschätzungen;

- Schaffung einer Grundlage für die Prioritätensetzung bei der EU-weiten Sammlung und Analyse von Informationen sowie, im Anschluss daran, für die Bestimmung des besten Handlungsverlaufs, um im Rahmen der gesetzten Prioritäten Terrorismus und andere Formen schwerer oder organisierter Kriminalität sowie die dadurch verursachten Bedrohungen zu verhindern und zu bekämpfen;

- Erleichterung gemeinsamer koordinierter Strafverfolgungsmaßnahmen, um terroristische Aktivitäten und solche, die mit anderen Formen schweren oder organisierten Verbrechens zusammen hängen, wirkungsvoll und auf geeignete Art und Weise zu verhindern, zu ermitteln und zu unterbinden.

Verbesserter Zugang zu Daten, Informationen und „Intelligence" wird die Strafverfolgung in jedem Mitgliedstaat und auf europäischer Ebene unterstützen, um Terrorismus und andere Formen schweren oder organisierten Verbrechens sowie die dadurch verursachten Bedrohungen zu verhindern und zu bekämpfen. Durch die methodische Analyse von Daten zwecks Schaffung erstklassiger verbrechensbezogener „Intelligence" wird ein zusätzlicher Mehrwert erzielt werden. Zur Verstärkung der „Intelligence-gestützten" Strafverfolgung in der EU sollten gemeinsame Mindeststandards für die nationalen Informationsverarbeitungssysteme angenommen werden, die kompatible Bedrohungsanalysen auf der europäischen Ebene möglich machen.

2.2. Kernelemente für effektiven Zugang zu sowie Sammlung, Speicherung, Analyse und Austausch von Daten und Informationen

2.2.1. Das Prinzip gleichberechtigten Zugangs zu Daten zwischen Strafverfolgungsbehörden

Das erste Kernziel der Informationspolitik für Strafverfolgungszwecke besteht darin, den freien Verkehr von Informationen zwischen den Strafverfolgungsbehörden,

[3] Ein Gesetzesvorschlag zu Datenzurückhaltung ist von vier Mitgliedstaaten dem JI-Rat im April 2004 vorgelegt worden. Die Kommission plant eine offene Anhörung.

einschließlich EUROPOL und EUROJUST, festzulegen. Gegenwärtig können die Strafverfolgungsbehörden national zugängliche Datenbanken abfragen. Der Zugang zu Informationen, die sich im Besitz der Strafverfolgungsbehörden anderer Mitgliedstaaten befinden, ist an Anforderungen geknüpft, die insgesamt dazu führen, dass jene praktisch unzugänglich sind.

Die Informationspolitik zielt darauf ab, diese Informationen in der Praxis allen Strafverfolgungsbehörden in der EU, einschließlich EUROPOL und EUROJUST, zugänglich zu machen, um diesen im Einklang mit dem Grundsatz der Rechtsstaatlichkeit bei der Ausübung ihrer Aufgaben zu helfen.

Das Prinzip, das die Informationspolitik einführt, um die Herausforderungen anzunehmen, die im vorherigen Kapitel beschrieben sind, ist **‚das Recht auf gleichberechtigten Zugang zu Daten'.** Dieses gäbe Strafverfolgungsbehörden und -beamten gleichbedeutende Rechte auf Zugang zu Daten und Datenbanken in anderen EU-Mitgliedstaaten unter vergleichbaren Bedingungen wie den Strafverfolgungsbehörden in diesem Mitgliedstaat. Die logische Folge dieses Rechts ist die Verpflichtung, Strafverfolgungsbeamten anderer Mitgliedstaaten Zugang unter denselben Bedingungen zu gewähren wie nationalen Strafverfolgungsbeamten.

Dies bedingt die Verpflichtung der Mitgliedstaaten auf ein EU-Modell, das Dinge wie die Synchronisation von Bedrohungsanalysen auf der Grundlage einer gemeinsamen Methodik und einer systematischen Untermauerung der Bedrohungsanalysen durch sektorale Verletzbarkeitsstudien umfasst.

Das Prinzip gleichberechtigten Zugangs erkennt an, dass:

– die Sicherheit der Union und ihrer Bürger eine gemeinsame Verantwortung ist;

– die Mitgliedstaaten bei der Strafverfolgung zur Verhinderung und Bekämpfung des Terrorismus und anderer Formen schweren oder organisierten Verbrechens sowie bei der Abwehr der davon ausgehenden Bedrohungen voneinander abhängen;

– die Strafverfolgungsbehörden in den einzelnen Mitgliedstaaten ähnliche Aufgaben erfüllen und gleichgelagerte Informationsbedürfnisse haben;

– die zuständigen Behörden rechtmäßig handeln, wenn sie in Erfüllung ihrer Aufgaben sowie innerhalb der durch gemeinsame Datenschutz- und Datensicherheitsstandards gezogenen Grenzen auf Daten zugreifen bzw. Datenbanken abfragen.

Das Recht auf gleichen Zugang sollte grundsätzlich nicht die Effektivität bestehender Instrumente gegenseitiger Rechtshilfe schmälern. Alle potentiellen gesetzlichen Auswirkungen werden sorgfältig geprüft werden müssen.

Auf der Grundlage gemeinsamer Standards, die Datenschutz und Datensicherheit einschließen, sollten für alle Strafverfolgungsbehörden in der EU verständliche und klare Voraussetzungen für den Zugriff auf alle erforderlichen, relevanten Informationen aufgestellt werden. Die Mitgliedstaaten werden für die Umsetzung dieser Bedingungen verantwortlich sein. Ein System zur Überwachung der

Umsetzung wird nach der Identifizierung der Zugriffsbedingungen im Zuge der Bestandsaufnahme eingerichtet werden (vgl. 2.2.2).

Den Kernhindernissen beim Austausch von Informationen zwischen den Strafverfolgungsbehörden kann nur dann wirksam entgegengetreten werden, wenn die Mitgliedstaaten sich ernsthaft verpflichten, konkrete Maßnahmen zur Festlegung eines Europäischen „Intelligence-Modells" festzulegen (vgl. 2.3).

Die Europäische Informationspolitik zielt auf die Einführung eines grundsätzlichen Rechts der Strafverfolgungsbehörden in der EU auf gleichberechtigten Zugang zu allen erforderlichen, relevanten Daten und Informationen ab. Die Kommission wird mit den Mitgliedstaaten prüfen, welche Hindernisse im Wege stehen, und auf dieser Grundlage beurteilen, ob es sinnvoll ist, dem Rat und dem Europäischen Parlament einen legislativen Vorschlag betreffend ihre Einführung auf europäischer Ebene vorzulegen.

2.2.2. „Scoping" der Zugangsbedingungen

Die Kommission schlägt vor, auf der Grundlage verfügbarer sowie solcher Informationen, die die Mitgliedstaaten zu diesem Zweck liefern, eine vollständige Bestandsaufnahme vorzunehmen, um Aufschluss über folgende Elemente zu erhalten:

- auf welche Daten oder Datenbanken die Strafverfolgungsbehörden in den Mitgliedstaaten der EU Zugriff haben, und auf welche im Ausland zugegriffen wird, einschließlich der Indexdatenbanken (*Inhalt*);
- was ist der Zweck der Datenbank *(Zweckbestimmung)*;
- welche Arten von Strafverfolgungsbehörden haben Zugang zu diesen Daten (*Benutzer*);
- unter welchen Bedingungen haben diese Behörden Zugang zu diesen Daten und Datenbanken (*Zugangsprotokoll*);
- welche technischen Anforderungen werden an den Zugang zu diesen Daten und Datenbanken gestellt (*technisches Protokolle*);
- wie häufig wird auf die Daten und Datenbanken zugegriffen (*Relevanz*);
- welche Daten oder Datenbanken sind von Interesse für die Strafverfolgungsbehörden, ihnen jedoch nicht zugänglich; welche Datenschutzbestimmungen finden Anwendung („*scoping" von Bedürfnissen*).

Die Kommission beabsichtigt:

- ***bis Ende 2004 eine Bestandsaufnahme in die Wege zu leiten, um Umfang, Bedarf und Beschränkungen des Zugriffes der Strafverfolgungsbehörden auf Daten und Datenbanken zu ermitteln.***
- ***eine Studie über die gesetzlichen Bestimmungen, Bedingungen, einschließlich IT-Lösungen für den Zugang zu (Nicht-)***

Strafverfolgungsdaten, sowie Datenschutzverfahren und Datensicherheitsbestimmungen zu veranlassen.

2.2.3. Datensammlung

Die Strafverfolgungsbehörden in der EU sammeln und kategorisieren Daten und Informationen nach unterschiedlichen Ansätzen. Zur Zeit existiert kein einheitliches Forum für die Einstufung der Vertraulichkeit verschiedener Informationsquellen.

Die erste und wichtigste Informationsquelle sind die Datenerhebungen der Strafverfolgungsbehörden. Der Zugang zu Daten, die nicht für Strafverfolgungszwecke gesammelt werden, ist eine weitere politische Frage. Sie bedarf angesichts ihrer möglichen Auswirkungen auf Unternehmer und Nutzer sowie auf Gemeinschaftsrecht und -politiken einer breiten und offenen Anhörung aller interessierten Kreise.

Ein System zur Verwaltung unterschiedlicher Zugriffsberechtigungen, zum Beispiel *europäische Standards für die Berechtigung zum Zugriff auf eingestufte Informationen,* ein gemeinsames System von *Benutzerprofilen* zur Verwaltung der zahlreichen Zugriffsrechte und ein authentifiziertes Verfahren zur Registrierung berechtigter Nutzer *(z.B. Benutzerkonten)* würden die Grundlage einer effektiven Zugangsverwaltung darstellen. Benutzerprofile könnten zur systematischen Überwachung und Überprüfung des Zugriffs auf und der Verarbeitung von Daten genutzt und in *„log files"* und *„audit trail"*-Systemen angelegt werden.

Die Kommission beabsichtigt die Veranlassung von Studien, um die Ausarbeitung legislativer und nicht-legislativer Initiativen zu untermauern, die sich beziehen auf: Mindestanforderungen für die Datenerhebung; gemeinsa Verfahrensnormen zur Einstufung der Vertraulichkeit und Zuverlässigkeit von Daten; gemeinsame Normen für die Genehmigung des Zugriffs auf eingestufte Informationen sowie Benutzerprofile. Die Kommission wird weiterhin Anhörungen und multidisziplinäre Workshops im Rahmen des EU-Forums für die Vorbeugung der organisierten Kriminalität organisieren, um öffentlich-private Partnerschaften und vor allem den Zugriff auf solche Daten zu diskutieren, die nicht für Strafverfolgungszwecke erhoben wurden.

2.2.4. Datenaustausch und -verarbeitung

Neben verschiedenen Wegen, auf Daten und Datenbanken auf der Grundlage des Prinzips gleichen Zugangs zuzugreifen, besteht eine weitere Option darin, bestehende Daten und Datenbanken zu vernetzen oder zentrale Datenbanken zu schaffen, um sie besser zugänglich zu machen. In diesem Zusammenhang forderte der Europäische Rat[4] die Kommission auf, "Vorschläge für eine verstärkte Interoperabilität zwischen europäischen Datenbanken zu unterbreiten (SISII, VIS und EURODAC), um ihren Mehrwert innerhalb ihres jeweiligen gesetzlichen und technischen Rahmens für die Verhütung und Bekämpfung des Terrorismus

[4] Europäischer Rat vom 25. März 2004 *Erklärung zur Bekämpfung des Terrorismus*

auszunutzen“[5]. Verstärkte Interoperabilität wird die einschlägigen gesetzlichen Bestimmungen zum Datenschutz berücksichtigen müssen.

Die Kommission vertritt die Auffassung, dass die einzig machbare Option in Zukunft die Schaffung dialogfähiger, miteinander verbundener Systeme in der EU ist. Eine konzeptionell angelegte, umfassende IT-Architektur, die nationale, europäische und internationale Systeme integriert, bietet langfristig beträchtliche Einsparungen, Synergien, politische Möglichkeiten und Chancen, und zwar sowohl auf dem Gebiet verbrechensbezogener „Intelligence“ als auch im breiteren Zusammenhang einer sich entwickelnden Europäischen Sicherheitsstrategie.

Ein stufenweiser Ansatz sollte verfolgt werden, der auf harmonisierten Dateiformaten und Zugangsregelungen für die unterschiedlichen Systeme basiert. Die durch die Europäische Kommission[6] im Vorfeld durchgeführten Anhörungen der betroffenen Parteien haben bereits einige mögliche Hindernisse für den Austausch von Informationen offen gelegt. Hierzu gehören mangelnde(s):

– gemeinsame Standards und Bedingungen für die Datenverarbeitung;

– gemeinsame Standards für den Zugang zu Daten;

– kompatible Verbrechensdefinitionen und Verbrechensstatistiken;

– kompatible, von den Strafverfolgungsbehörden eingesetzte IT-Technologien;

– kooperative Strafverfolgungskulturen jenseits institutioneller Grenzen;

– Zusammenarbeit zwischen den Akteuren des öffentlichen und privaten Sektors;

– Bewusstsein für gemeinsame Datenschutzregeln und ein fehlender Rahmen für die Datensicherheit.

Die Kommission beabsichtigt eine Mitteilung vorzulegen, die effektive Möglichkeiten zur Beseitigung von Kernhindernisse bei der Weitergabe von Daten erforscht und ggf. von entsprechenden Gesetzesinitiativen flankiert wird.

2.2.5. Forschung

Die aktuellen Europäischen Forschungsprogramme befassen sich mit der Sicherheit von Informations-/Kommunikationssystemen und -infrastrukturen. Die Kommission hat bereits berücksichtigt, dass die Vorbereitung eines Forschungsprogramms zur europäischen Sicherheit durch die Initiierung einer Vorbereitenden Maßnahme für Forschung im Bereich der Sicherheit[7] beschleunigt werden muss, um die Sicherheit der europäischen Bürger zu verbessern. Die Vorbereitende Maßnahme für Forschung im Bereich Sicherheit, die für die Jahre 2004 – 2006 vorgesehen ist (EUR 65 Mio.),

---

5 Eine getrennte Mitteilung der Kommission über dieses Thema wird vorbereitet werden.

6 Dubliner Erklärung und Schlussfolgerungen der Treffen des Forums zur Verhütung der organisierten Kriminalität

7 COM (2004) 72 endg.

würde Aktivitäten finanzieren und unterstützen, um Bedingungen für ein umfassendes Europäischen Sicherheitsforschungsprogramm ab 2007 auszuloten.

Terrorismus und organisiertes Verbrechen sind die beiden Spitzenreiter bei den Sorgen europäischer Staatsbürger (ungefähr 80% der EU-Bürger geben Terrorismus und organisiertes Verbrechen als ihre größten Befürchtungen an). Gegenwärtig werden Forschungsaktivitäten im Bereich der kriminalistischen *Intelligence*-Systeme und Strafverfolgung nicht in ausreichendem Maße von Forschungsprogrammen umfasst. Folglich müssten spezifische Forschungsmaßnahmen zusätzlich zu den existierenden Programmen definiert werden. Darüber hinaus ist die Ko-finanzierung von Forschungsaktivitäten auch im Rahmen des AGIS-Programms möglich.

- ***Förderung der Forschung bezüglich sicherer und vertraulicher Mitteilungskanäle durch das AGIS-Programm;***

- ***Initiierung der Entwicklung gemeinsamer Standards für den sicheren Informationsaustausch, insbesondere zwischen Strafverfolgungsbehörden;***

- ***Veranlassung spezieller Forschung zu Nutzung und Umsetzung eines europäischen kriminalistischen "Intelligence-Systems", einschließlich gemeinsamer Standards für so genannte Meta-Daten, sicheren Datenaustausch, stärkere Datenschutzinstrumente, automatisierte Analyse, Bedrohungs- und Risikopotentialeinschätzung und „Profiling-Methoden";***

2.3. Kernelemente einer effektiven "Intelligence-gestützten" Strafverfolgungsfähigkeit auf EU-Ebene

Das zweite Hauptziel dieser Informationspolitik besteht darin, Schritte zu einer *Intelligence*-gestützten" EU-Strafverfolgung vorzuschlagen. Kriminalistische "*Intelligence*" unterstützt die zuständigen Behörden in der Erfüllung ihrer strategischen oder operativen Aufgaben, damit Terrorismus und andere schwere oder organisierte Verbrechen sowie die davon ausgehenden Bedrohungen verhütet und bekämpft werden.[8] Die Einführung eines europäischen Modells für die kriminalistische „Intelligence" würde „Intelligence"-gestützte Strafverfolgung effektiv machen und verstärkte kooperative Maßnahmen erlauben. Sie würde Dinge wie die Synchronisation von Bedrohungsanalysen auf der Grundlage einer gemeinsamen Methodik, systematischer Untermauerung der Bedrohungsanalysen durch sektorale Verletzbarkeitsstudien sowie die Zuteilung der verlangten finanziellen und personellen Ressourcen umfassen.

Die EU-Informationspolitik für Strafverfolgungszwecke zielt darauf ab, **einem europäischen „Intelligence-Netzwerk" die nötigen Informationen verfügbar zu machen**, um erstklassige kriminalistische „*Intelligence*" zu schaffen, die dann in die periodische Produktion von EU-Strategien und operativen Bewertungen mündet. Die Verfügbarkeit des Europol-Informationssystems wird ebenfalls eine wichtige Rolle bei der Entwicklung einer derartigen „*Intelligence*"-Kapazität auf EU-Ebene spielen.

---

[8] Kriminalistische *Intelligence* unterteilt sich in strategische und operationelle (oder taktische) „Intelligence". Strategische *Intelligence* vermittelt einen Einblick in die Frage, wie die Bedrohungen und Verbrechen aussehen, die angegangen werden müssen. Operationelle *Intelligence* vermittelt taktische Anleitungen, wie man sie bewältigt und Schwerpunkte setzt.

Die nachfolgend umrissenen Schritte sollten zu einer Situation führen, in der strategische Bewertungen für die Entscheidungsträger leicht abgreifbar sind, um auf diese Weise Prioritäten für die Strafverfolgung so häufig wie nötig zu überarbeiten. Darüber hinaus würden operationelle Bewertungen für die "Polizeichefs- Task Force" (CPTF) verfügbar werden, sodass die besten taktischen Kenntnisse zur Anwendung kämen, um gemäß der Schwerpunktsetzung des Europäischen Rates Bedrohungen oder Verbrechen, einschließlich des Terrorismus, zu verhindern oder zu bekämpfen. Die Bewertungen sollten aktuell und qualitativ hochwertig sein.

Gegenwärtig werden die Strafverfolgungsbehörden in der EU nicht von kriminalistischer „*Intelligence*" geleitet, die ganzheitlich auf die europäische Sicherheit abzielt. Gleichzeitig besteht die dringende Notwendigkeit, die EU-Bürger vor neuen Risiken und Bedrohungen zu schützen. Daher ist es zwingend erforderlich, dass die strategischen und operationellen Bewertungen auf EU-Ebene schnellstmöglich verfügbar sind. Der Austausch von „*Intelligence*" muss gleichermaßen die Rechtsstaatlichkeit und die Grundrechte des Einzelnen beachten.

Daher wird der folgende zweiphasige Ansatz angestrebt:

- Kurzfristig sollten die für kriminalistische „Intelligence" zuständigen Behörden der Mitgliedstaaten, möglichst unter der Ägide von Europol, monatliche Treffen abhalten, um ihre nationalen strategischen und operationellen Bewertungen zu besprechen. Europol sollte hierzu seinerseits mit aller verfügbaren „*Intelligence*" beitragen. Alle hieraus folgenden Erkenntnisse sollten zusammengetragen werden, um auf EU-Ebene zweimal jährlich eine strategische sowie einmal monatlich eine operationelle Bewertung zu erstellen. Die strategischen Bewertungen auf EU-Ebene würden es dem Rat erlauben, Prioritäten für die Strafverfolgung zu setzen. Die CPTF sollte die operationellen Bewertungen an die Arbeitsebene in den Mitgliedstaaten weitergeben.

  All dies sollte in einem ersten Schritt auf Informationen beruhen, auf die die kriminalistische „Intelligence" der Mitgliedstaaten und Europol aufgrund bestehender Rechtsgrundlagen rechtmäßig zugreifen und die sie mit vorhandenen Analysewerkzeugen auswerten können.

- Längerfristig können die nationalen "*Intelligence*-Behörden" damit beginnen, auf der Grundlage EU-weit zugänglicher Strafverfolgungsinformationen und mithilfe standardisierter Analyseinstrumente „*Intelligence*" zu schaffen.

  Die Bedeutung von Europol würde gewichtiger werden, da Daten und Verfahren europäischer werden würden. Das würde „*Intelligence*" von höherer Qualität schaffen, die standardisierter wäre und auf breiterer Basis verstanden würde. Das Verhältnis zwischen Europol, dem Rat und der CPTF muss den veränderten Verhältnissen angepasst werden. Von diesem Moment an wird die EU in der Lage sein, sich als Partner mit eigenem Wesen und besonderer Qualität bei der Strafverfolgung im internationalen Rahmen behaupten zu können.

Die Kommission beabsichtigt, die für die zeitlich angemessene Entwicklung verlässlicher „*Intelligence*" notwendigen Schritte zu untersuchen und dem Rat bis Ende 2005 einen entsprechenden Bericht vorzulegen.

Der Rat wird auf der Grundlage strategischer und taktischer Lagebewertungen, die von der „*Intelligence Group*“ ausgearbeitet wurden, Prioritäten setzen. Solch eine operationelle Bewertung sollte die Möglichkeit bieten, spezielle Ergebnisse zu erreichen, zum Beispiel Festnahmen, Beschlagnahmen oder Verwirkungen von Vermögenswerten, die aus Straftaten resultieren, oder die Vornahme zielgerichteter Versuche, kriminelle Gruppierungen aufzubrechen.

Allgemein verwendete „*Intelligence*-Methoden“ sollten so vereinheitlicht werden, dass sie nicht nur für den Gebrauch auf EU-Ebene geeignet sind, sondern auch für die Behandlung spezifischer transnationaler oder regionaler Fragen (z.B. im Rahmen der Ostsee-TaskForce). Die Kommission und Europol könnten eine Studie über die verschiedenen, bei den zuständigen „*Intelligence*-Einheiten“ der Mitgliedstaaten gebräuchlichen Methoden durchführen und bis Ende 2005 eine gemeinsame europäische Analysemethodik für kriminalistische *Intelligence* vorschlagen. In Verbindung damit könnte CEPOL aufgefordert werden, einen Lehrplan für die Schulung von Kriminalanalytikern zu erstellen, sowie diese Methoden und ihre Anwendung auf Führungsebene bekannt zu machen, um eine bestmögliche Verwertung von operativen Lageeinschätzungen zu gewährleisten. Die analytischen Methoden, die allgemein angewendet werden[9] sollten so angepasst werden, dass Ergebnisse erzeugt werden können, die strategische und operationelle Bewertungen ermöglichen.

- ***Die Ideen dieser Mitteilung könnten vom Rat im Hinblick auf die Ergreifung geeigneter Maßnahmen zu ihrer Umsetzung gebilligt werden.***
- ***Unter der Ägide von Europol könnten die Vertreter der zuständigen „Intelligence-Einheiten“ der Mitgliedstaaten nationale strategische und operationelle Bewertungen sammeln.***
- ***Der Rat könnte die Mitgliedstaaten ersuchen, Europol „Intelligence“ zur Verfügung zu stellen und Europol das Mandat für eine umfassende Bewertung der Bedrohungslage erteilen. Zoll- und Grenzkontrollbehörden könnten angewiesen werden, die Erstellung ihrer „Intelligence“ mit Europol zu koordinieren.***
- ***Gemeinsame Verbrechenstatistikdefinitionen und Normen für die Berichterstattung sollten entwickelt werden.***
- ***Gemeinsame Analysemethoden für die Erstellung von „Intelligence“ auf EU-Ebene sollten möglichst unter der Ägide von Europol entwickelt werden.***

2.4. Vertrauensbildung

Das dritte Hauptziel der europäischen Informationspolitik besteht darin zum Aufbau eines Vertrauensverhältnisses zwischen den Strafverfolgungsbehörden, -beamten und -partnern beizutragen, indem ein Fundament gemeinsamer Werte, Standards und Politikorientierungen in diesem Bereich geschaffen wird.

Die Einführung gemeinsamer Standards ist entscheidend für die Schaffung einer vertrauensvollen Umgebung für die Erhebung von, den Zugriff auf und den Austausch von Informationen (siehe insbesondere 2.2). Gemeinsame Standards für den Datenzugriff und die

[9] Die Methoden sind Analysen zu Ergebnissen, Verbrechensmustern, Verbrechensmärkten, Verbrechensnetzwerken, Risiken (was wiederum als Managementwerkzeug genutzt wird), Zielprofilen (oft „profiling genannt), verbrecherischen Wirtschaftsprofilen, sowie demographischen und sozialen Trends.

Datenverarbeitung werden genauso unabdingbare Grundlagen sein, wie kompatible Methodologien bezüglich der Bedrohungs-, Risiko- und Profilbewertung, um Informationen und „Intelligence“ auf strategischer und operativer Ebene effektiv weiterzugeben. Diese Maßnahmen werden nur dann effektiv sein, wenn sie von nachhaltiger politischer Unterstützung für einen **gemeinsamen Raum der Strafverfolgung** in der EU begleitet werden, der auf kompatiblen nationalen „*Intelligence*-Systemen“ basiert, die zusammen wiederum ein integriertes europäisches „*Intelligence*-Modell“ bilden.

Formelle und informelle Arbeitsbeziehungen müssen entwickelt werden, um ein funktionsfähiges System zu bilden. Schulungsmaßnahmen zur Vermittlung eines gemeinsamen Verständnisses von „*Intelligence*“ bei dem eingesetzten Personal werden zu dieser Entwicklung beitragen. CEPOL sollte eine wichtige Rolle in diesem Zusammenhang spielen, insbesondere durch:

– Aufstellung regelmäßiger Ausbildungskurse für potentielle zukünftige politische Entscheidungsträger und Führungskräfte;

– Ausarbeitung eines Musterlehrplans für die Schulung der mittleren Führungsebene in Bezug auf europäische „*Intelligence*-Angelegenheiten“ auf nationaler Ebene;

– Durchführung von Ausbildungsmaßnahmen bezüglich aller Elemente der EU Informationspolitik

Andere Maßnahmen würden Vernetzungsbemühungen einschließlich jener verstärken, die auf schon bestehenden Instrumentarien beruhen, wie zum Beispiel gegenseitige Bewertungen, gezielte Projekte im Rahmen des AGIS-Programms oder Maßnahmen, die unter dem Forum für die Verhütung des organisierten Verbrechens ergriffen werden.

Schließlich sollte die Rolle der nationalen Datenaufsichtsbehörden gebührend berücksichtigt werden, da sie dazu beitragen, dass die notwendigen Sicherheitsmaßnahmen zur Aufrechterhaltung der Rechtsstaatlichkeit festgelegt und effektive demokratische Kontrolle vorgesehen wird.

Vertrauensbildende Maßnahmen und Methoden sind von fundamentaler Bedeutung (gemeinsame Standards und Methodologien). Die Kommission beabsichtigt, entsprechende Vorschläge bis Ende 2005 vorzulegen.

PARALLEL DAZU KÖNNTE DER RAT CEPOL ERSUCHEN, EINEN GEMEINSAMEN LEHRPLAN FÜR DIE SCHULUNG VON „INTELLIGENCE-BEAMTEN“ ZU ENTWICKELN.

KAPITEL III – GESETZGEBUNGSINITIATIVEN, DIE MIT DIESER MITTEILUNG VERBUNDEN SIND

Die Kommission wird die Entwicklung dieser Politik fortsetzen, einschließlich gesetzgeberischer Initiativen in den verwandten Gebieten des Schutzes personenbezogener Daten im dritten Pfeiler und der Nutzung von Passagierinformationen für

Strafverfolgungszwecke, letzteres in Übereinstimmung mit den in der Kommissionsmitteilung vom Dezember 2003[10] festgelegten Grundsätzen.

Der Vorschlag für einen Rahmenbeschluss zum Datenschutz wird gemeinsame Standards für die Verarbeitung personenbezogener Daten aufstellen, die gemäß Titel VI des Vertrages über die Europäische Union ausgetauscht werden, um die Polizei- und Justizbehörden im Einklang mit den Grundrechten zum Zugriff auf alle für die Strafverfolgung relevanten Daten zu ermächtigen. Dieser Rahmenbeschluss soll einen einzigen allgemeinen Rahmen für den Datenschutz zum Zwecke der Zusammenarbeit bei der Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verbrechen und Sicherheitsbedrohungen schaffen. Er wird einen Rahmen für spezifischere Bestimmungen bilden, die in verschiedenen, auf EU-Ebene angenommenen Rechtsinstrumenten enthalten sind, die praktischen Unterschiede beim Informationsaustausch zwischen den Mitgliedstaaten einerseits sowie den Mitgliedstaaten und Drittstaaten andererseits weiter reduzieren und in einen Mechanismus eingebettet sein, der den Schutz der Grundrechte sicherstellt.

10 COM (2003) 826 endg. vom 16.12.03 betreffend die Übermittlung von Fluggastdatensätzen (PNR): Ein sektorübergreifendes EU-Konzept