





Ausarbeitung

INDECT



INDECT

Verfasser/in: 
Aktenzeichen: WD 3 – 3000 – 112/12
Abschluss der Arbeit: 29. Mai 2012
Fachbereich: WD 3: Verfassung und Verwaltung
Telefon: 

Inhaltsverzeichnis

1.	Einleitung	4
2.	Das Projekt „INDECT“	4
2.1.	Vorhaben	4
2.2.	Ziele	5
2.3.	Meinungsstand	7
3.	Grundrechtliche Implikationen	9
3.1.	Überwachungsmaßnahmen des Internets	10
3.1.1.	Post- und Fernmeldegeheimnis (Art.10 GG)	10
3.1.2.	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art.2 I i. V. m. Art.1 I GG)	12
4.	Die Finanzierung des Projektes durch die BRD als Spannungsverhältnis zum Grundrechtsschutz?	14

1. Einleitung

In den letzten Jahren gab es in verschiedenen Staaten konkrete Überlegungen, mögliche Gefahren für die öffentliche Sicherheit und Ordnung mittels Videoüberwachung und Vorratsdatenspeicherung abzuwehren. In diesen Rahmen ist auch das INDECT-Forschungsprogramm (Abkürzung für „**I**ntelligent Information System Supporting Observation, Searching and **D**etection for Security of Citizens in Urban Environment“, deutsch: Intelligentes Informationssystem zur Überwachung, Suche und Erkennung für die Sicherheit der Bürger in urbaner Umgebung) einzuordnen¹. Das Forschungsprojekt „INDECT“ und mögliche grundrechtliche Implikationen des Einsatzes der mit Hilfe des INDECT-Programms realisierten Technologien werden in dieser Ausarbeitung dargestellt.

2. Das Projekt „INDECT“

2.1. Vorhaben

INDECT wurde **von der polnischen Abteilung für Heimatschutz initiiert**². Siebzehn Partner versprachen, das Projekt zu unterstützen und zu begleiten, wobei sich die AGH Universität für Wissenschaft und Technik in Krakau bereit erklärte, INDECT zu führen. Projektkoordinator wurde Prof. Andrzej Dziech, der an der genannten Universität tätig ist. Die anderen sechzehn Partner sind elf Universitäten (u.a. Universität Wuppertal), vier (Sicherheits-)Firmen und zwei möglichen Endnutzern (u.a. Polizei von Polen bis April 2012)³. INDECT wurde der Europäischen Kommission im Rahmen des 7. Rahmenprogramms (FP7) unterbreitet. Die von ihr beauftragten Experten kamen nach eine Evaluation zu einem positiven Ergebnis hinsichtlich der Förderungswürdigkeit⁴. Das Projekt wird nun mit 14,86 Millionen Euro pro Jahr **durch die Europäische Union finanziert**⁵. INDECT startete am 01.01.2009 und ist auf fünf Jahre angelegt.⁶

Die Vereinbarkeit von INDECT mit europäischen und nationalen Regelungen zum Datenschutz soll durch einen **Ethikrat** sichergestellt werden⁷. Die Mitglieder des Ethikrats werden durch den Projektkoordinator des Programms aufgrund fachlicher Kompetenzen benannt. Derzeit besteht er aus neun Mitgliedern und setzt sich folgendermaßen zusammen: ein Anwalt für Menschenrechte, ein Professor für Ethik, zwei aktive und ein pensionierter Polizeibeamter, ein technischer Spezialist und drei Forscher auf dem Gebiet von Sicherheitstechnologien. Studentenvertreter können den Status von Beobachtern erhalten. Deren Äußerungen werden im Bedarfsfall vom Ethikrat bei

1 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Christine Buchholz, Dr. Dieter Dehm, weiterer Abgeordneter und der Fraktion DIE LINKE. „Forschung am EU-Projekt INDECT“, Drucksache 17/3940., <http://dip21.bundestag.de/dip21/btd/17/039/1703940.pdf>, S.1.

2 <http://www.indect-project.eu/>.

3 Sauerbrey, Anna, „Der Rechner als Polizist“, ZEIT ONLINE, 27.10.2010. <http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung> ; für weitere Informationen siehe <http://www.indect-project.eu/indect-partners>.

4 <http://www.indect-project.eu/faq#Q1.4>.

5 <http://jacobjung.wordpress.com/2011/05/23/der-einsatz-von-indect-in-europaischen-grosstadten-ist-nicht-auszuschliessen-roland-albert-piratenpartei-im-interview-mit-jacob-jung/>.

6 <http://www.indect-project.eu/>.

7 <http://www.indect-project.eu/faq#Q2.3>.

Entscheidungen bedacht. Ziel ist es, laut INDECT, eine möglichst breite Zusammensetzung anzustreben, um eine effektive Kontrolle des Projektes zu gewährleisten⁸.

Der Ethikrat trifft sich regelmäßig. Im Bedarfsfall können auch Telefonkonferenzen stattfinden⁹.

Die Hauptaufgabe des Rates besteht in der Rechtmäßigkeitskontrolle des Projektes. Insbesondere hat der Rat folgende Befugnisse¹⁰:

- Erstellen von Anordnungen, die aktuelle Entwicklung des Projekts der aktuellen Rechtslage anzupassen, insbesondere im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention (EMRK) und der EU-Grundrechtecharta
- Schaffung von Kontrollverfahren zum Schutz der Testpersonen des Projektes
- Koordinierung der Projekte zur Video- und Internetüberwachung mit europäischen und nationalen Datenschutzbeauftragten
- Organisation regelmäßiger Treffen zur Information des Fachpublikums
- Jährlicher Bericht an die Europäische Kommission über den Datenschutz im Rahmen von INDECT

Neben dem Ethikrat gibt es einen Ethical Issue Manager (EIM), der die Einhaltung von Datenschutzregelungen sicherstellen soll¹¹.

2.2. Ziele

INDECT kann als „integriertes netzwerkzentriertes System zur Unterstützung der operativen Aktivitäten von Polizisten unter Bereitstellung von Techniken und Instrumenten zur Beobachtung verschiedener beweglicher Objekte charakterisiert werden. Neben angeschlossenen Polizeidatenbanken und dem Internet sollen Daten auch von fliegenden Kameras verarbeitet werden.“¹²

INDECT bezeichnet sich selbst als **reines Forschungsprojekt**.¹³ Es gehe nicht um eine globale Überwachung. Die Daten, die benützt würden, seien entweder fiktiv oder mit dem schriftlichen Einverständnis der beteiligten Personen erhoben worden¹⁴. Das Oberziel von INDECT bestehe in der Erhöhung der Sicherheit der Bürgerinnen und Bürger, insbesondere in städtischer Umgebung. Vor allem Terrorismus, aber auch andere kriminelle Aktivitäten (z.B. organisierte Krimina-

8 <http://www.indect-project.eu/faq#Q2.5>.

9 <http://www.indect-project.eu/faq#Q2.4>.

10 <http://www.indect-project.eu/faq#Q2.3>.

11 <http://www.indect-project.eu/faq#Q2.2>.

12 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Christine Buchholz, Dr. Dieter Dehm, weiterer Abgeordneter und der Fraktion DIE LINKE. „Forschung am EU-Projekt INDECT“, Drucksache 17/3940., <http://dip21.bundestag.de/dip21/btd/17/039/1703940.pdf>, S.1.

13 <http://www.indect-project.eu/faq#Q3.1>.

14 Mansmann, Urs, „INDECT auf dem Prüfstand“, Magazin für Computer und Technik vom 25.10.2012, S. 52

lität) sollen mittels der neuen Technologien verhindert werden. Der Ansatz von INDECT sei somit präventiver Natur, nicht repressiver Natur.¹⁵

INDECT arbeitet auf Basis existierender Technologien; sie sollen in einem automatischen System zusammenfasst werden. INDECT verfolgt vor allem zwei Stränge¹⁶:

Zum einen sollen Verbrechen, die im Internet geplant oder begangen werden, verhindert werden. Dies soll durch **Suchmaschinen** geschehen, die mithilfe digitaler Wassermarken **Bilder und Videos auf Internetseiten auffinden¹⁷ und die Nutzer identifizieren**. Sie werden dann der Polizei gemeldet. Die INDECT-Technologie im Internet basiert auf **digitalen Wasserzeichen**. Mit diesen soll u.a. nachvollzogen werden, wie sich die entsprechend markierte Nachricht im Internet verbreitet hat und welcher Internetnutzer zu welchem Zeitpunkt auf die Nachricht zugegriffen hat. Die erworbenen Informationen werden dem gesammelten Datensatz zugefügt¹⁸.

Zum anderen ist die **Entwicklung intelligenter Kameras** Gegenstand von INDECT. Diese Kameras sollen automatisch terroristische Bedrohungen oder „nicht normale Verhaltensweisen“ erkennen. Die zuständige Polizeidienststelle wird informiert, die sodann anhand des Bildmaterials ein Eingreifen abschätzt. Die Definition von „nicht normalen Verhaltensweisen“ bezieht sich laut INDECT auf „Verhalten, das mit terroristischen Akten, ernsthaften kriminellen Aktivitäten in der realen und virtuellen Welt (z.B. Mord, Bankraub, Bomben in Gepäckstücken)“¹⁹ verbunden ist. Zum Begriff des „unnormalen Verhaltens“ wurden beispielsweise 2009 über 100 polnische Polizisten befragt. Die Antworten reichten von Rennen auf öffentlichen Straßen bis hin zum Vergessen eines Gepäckstücks in öffentlichen Räumen²⁰. Fällt den Kameras ein „unnormales Verhalten“ auf, kann zur Identifizierung auf die biometrische Personenerkennung zurück gegriffen werden. Der Einsatz von Drohnen mit integrierten Kameras ist ebenso denkbar. Die Entscheidung zum Eingreifen treffe letztlich aber, betont INDECT, grundsätzlich ein Mensch, kein Computer. Die automatische Datenerfassung schaffe keine „Orwellschen Zustände“, sondern würde lediglich der effizienteren Polizeiarbeit und der Vermeidung menschlicher Fehler, z.B. bei der Weitergabe von Daten, dienen²¹.

Zusammenfassend stellen sich die wichtigsten Ziele von INDECT u.a. wie folgt dar:²²

- 1) die Testinstallation eines Überwachungssystems an verschiedenen Orten eines städtischen Ballungsraums und Erprobung eines Prototyps des Systems mit 15 Knotenpunkten,

15 <http://www.indect-project.eu/>

16 <http://www.indect-project.eu/>.

17 http://www.stopp-indect.info/?page_id=2&lang=de.

18 http://de.wikinews.org/wiki/EU_will_Internet_und_Mobiltelefone_anzapfen.

19 <http://www.indect-project.eu/faq#Q1.3>.

20 Hoferer, Dominik, „Geplante Überwachung mit INDECT- Jeder Bürger steht unter Generalverdacht“, Focus Online vom 16.03.2012, http://www.focus.de/digital/computer/chip-exklusiv/tid-25266/ueberwachung-jeder-steht-unter-verdacht_aid_724007.html.

21 <http://www.indect-project.eu/approach-to-ethical-issues>.

22 http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=1&CAT=PROJ&RCN=89374, hier in der Übersetzung ins Deutsche aus: Berliner Beauftragter für Datenschutz, Datenschutz und Informationsfreiheit, Bericht 2011, abzurufen unter: <http://www.datenschutz-berlin.de/content/veroeffentlichungen/jahresberichte>. S. 23 f.

- 2) die Implementierung eines verteilten Computersystems, welches die Erfassung, Speicherung, nach Aufforderung effektive Verteilung und intelligente Verarbeitung von Daten ermöglicht,
- 3) die Herstellung einer Reihe von Prototypen von Geräten für die Verfolgung mobiler Objekte,
- 4) die Entwicklung einer Suchmaschine für die schnelle Erkennung von Personen und Dokumenten anhand von digitalen Wasserzeichen,
- 5) die Durchführung umfassender Forschung an der digitalen Wasserzeichentechnologie für die semantische Suche im Internet,
- 6) die Entwicklung von Agentensystemen zur ständigen und automatischen Kontrolle öffentlicher Quellen wie Webseiten, Diskussionsforen, Usenet-Gruppen, Fileservern, Peer-to-Peer-(P2P-)Netzwerke und privater Computer,
- 7) der Aufbau eines Internet-basierten intelligenten (aktiven und passiven) Datensammelsystems und der messbare Nachweis seiner Effizienz.

2.3. Meinungsstand

INDECT ist innerhalb der EU-Staaten seit Bekanntwerden **heftig umstritten**. Es gibt nur **wenige Befürworter** des Projekts. Die Mehrheit erkennt die Entwicklung neuer Technologien im Sicherheitsbereich zwar an, sieht in INDECT aber eine **Gefahr für die Bürgerrechte**²³.

Befürworter des Projekts sehen in INDECT ein „**zukunftsweisendes Instrument bei der Bekämpfung von Kriminalität, insbesondere Terrorismus**“²⁴. Sie sehen in INDECT keine Gefahr für die Bürgerrechte der EU-Bürger. INDECT selbst versichere immer wieder, dass eine ausreichende Abwägung zwischen individuellen Rechten und dem öffentlichen Interesse stattfinde. Dies werde durch den Ethikrat sichergestellt²⁵. INDECT sei mit Art. 2 EMRK²⁶ (Recht auf Leben), Art. 3 EMRK (Verbot der Folter), Art.5 EMRK (Recht auf Freiheit und Sicherheit), Art.6 EMRK (Recht auf ein faires Verfahren), Art.8 EMRK (Recht auf Achtung des Privat- und Familienlebens), Art.9 EMRK (Gedanken-, Gewissens- und Religionsfreiheit), Art. 10 EMRK (Freiheit der Meinungsäußerung) und Art. 11 EMRK (Versammlungs- und Vereinigungsfreiheit), Art. 8 GR-Charta²⁷ (Schutz personenbezogener Daten) und Art. 3 UN-Kinderrechtskonvention²⁸ (Wohl des Kindes) vereinbar²⁹.

23 Salter, Thomas, „Europäisches Sicherheitsprojekt INDECT-Die moderne Verbrecherjagd“, TAZ.de, 24.12.2009, <http://www.taz.de/!45893/>.

24 MMR-Aktuell 2010, 301674, <http://beck-online.beck.de/Default.aspx?words=MMR-Aktuell+2010%2C301674&btsearch.x=42&btsearch.x=0&btsearch.y=0>.

25 <http://www.indect-project.eu/>.

26 Europarat- Europäische Menschenrechtskonvention vom 04.11.1950, zuletzt geändert durch Protokoll Nr.14 vom 13.05.2004 m. W. v. 01.06.2010, <http://dejure.org/gesetze/MRK>.

27 Charta der Grundrechte der Europäischen Union (2000/C 364/01), http://www.europarl.europa.eu/charter/pdf/text_de.pdf.

28 Übereinkommen über die Rechte des Kindes vom 20. November 1989, http://www.unicef.de/fileadmin/content_media/Aktionen/Kinderrechte18/UN-Kinderrechtskonvention.pdf, S.12.

29 <http://www.indect-project.eu/faq#Q2.6>.

Gegner kritisieren INDECT aus zwei Gründen:

Erstens werden die Ziele des Projektes **aus datenschutzrechtlichen Gründen abgelehnt**. INDECT führe zu einer „Totalüberwachung“³⁰ des Bürgers und greife unverhältnismäßig in europäische und deutsche Grundrechte ein. Die Datenschutzbeauftragten des Bundes und der Länder kamen auf ihrer Konferenz am 21./22. März 2012 zu dem Schluss, bei der automatischen Mustererkennung werde völlig unverdächtiges Verhalten registriert und ausgewertet. Dadurch entstünde die Gefahr der Erzeugung eines Anpassungsdrucks, wodurch die Persönlichkeitsrechte der Betroffenen verletzt werden würden³¹. Der EU-Datenschutzbeauftragte Peter Hustinx kritisiert, dass schon in der Planungsphase eines Projektes nicht der Schutz der Bürgerrechte in den Hintergrund treten dürfte und eine ausgewogene Abwägung zwischen privaten und öffentlichen Belangen stattfinden müsste³². Thilo Weichert, Leiter des unabhängigen Datenschutzzentrums Schleswig-Holstein sieht schon im Konzept von INDECT eine Unvereinbarkeit mit europäischem und deutschem Datenschutzrecht³³. Zudem lehnten die INDECT-Beteiligten jede gesellschaftliche Verantwortung mit der Begründung ab, es handele sich nur um ein Forschungsprojekt und sie gäben die Verantwortung für ethische Grundsätze an die potenziellen Endnutzer ab³⁴. Zudem gehe INDECT über die Vorratsdatenspeicherung hinaus, da INDECT Telefon- und Chatgespräche grundsätzlich protokollieren würde³⁵. Zudem sei die Entscheidung, wann ein Verhalten „normal“ und wann es „nicht normal“ ist, sehr problematisch. Techniker von Sicherheitssystemen weisen immer wieder daraufhin, dass die Erkennung menschlichen Verhaltens für Computer sehr schwierig sei, da menschliche Verhaltensweisen und Bewegungsabläufe sehr komplex seien³⁶. Dies könne dazu führen, dass normale Alltagssituationen (z.B. Suchen nach dem Autoschlüssel in der Handtasche über einen längeren Zeitraum) vom Videosystem als verdächtig eingestuft werden könnten und der zuständigen Polizeistelle gemeldet würden. Das Argument des Ethikrates „Wer nichts getan hat, muss auch nichts befürchten“³⁷ sei aus den genannten Gründen somit nicht nachvollziehbar.

Zweitens wird die **Informationspolitik von INDECT** und dessen Ethikrat kritisiert. Je lauter die Kritik von Datenschützern werde, desto weniger erfahre man über INDECT. Abgeordnete des Europäischen Parlaments wiesen in den vergangenen Jahren immer wieder darauf hin, sie würden über zu wenig Informationen über das Projekt verfügen, einige Informationen seien widersprüch-

-
- 30 Meier, Albrecht, „Angst vor der Mega-Suchmaschine“, Der Tagesspiegel, 08.02.2011, www.tagesspiegel.de/politik/ueberwachungssysteme-angst-vor-der-mega-suchmaschine/3798484.html.
- 31 <http://www.datenschutzbeauftragter-info.de/datenschutzkonferenz-aeussert-sich-zu-indect-acta-facebook-fahndung-und-co/>.
- 32 INDECT: EU-Überwachungsprojekt in der Diskussion, Beck-Online, MMR-Aktuell 2010, 301674, <http://beck-online.beck.de/Default.aspx?vpath=bibdata\zeits\mmraktuell\2010\301674.htm&pos=0&hlwords=INDECT#xhlhit>.
- 33 Salter, Thomas, „Europäisches Sicherheitsprojekt INDECT-Die moderne Verbrecherjagd“, TAZ.de, 24.12.2009, <http://www.taz.de/!45893/>
- 34 <http://jacobjung.wordpress.com/2011/05/23/der-einsatz-von-indect-in-europaischen-grosstadten-ist-nicht-auszuschliessen-roland-albert-piratenpartei-im-interview-mit-jacob-jung/>.
- 35 Monroy, Mattias, „Polnische Polizei steigt aus INDECT aus“, Telepolis, 16.04.2012, <http://www.heise.de/tp/artikel/36/36763/1.html>.
- 36 Sauerbrey, Anna, „Der Rechner als Polizist“, ZEIT ONLINE, 27.10.2010, <http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung>.
- 37 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Christine Buchholz, Dr. Dieter Dehm, weiterer Abgeordneter und der Fraktion DIE LINKE. „Forschung am EU-Projekt INDECT“, Drucksache 17/3940., <http://dip21.bundestag.de/dip21/btd/17/039/1703940.pdf>, S.1.

lich und eine Klärung der Widersprüche würde nicht ermöglicht werden³⁸. Selbst die Bundesregierung demonstriere Unkenntnis über das INDECT-Projekt. Mit dieser Kritik konfrontiert, verweist INDECT auf die jährlichen Fachmessen, auf denen sich Interessierte über die Ziele und den Fortgang des Projektes informieren können³⁹. Dies reicht EU-Abgeordneten und Datenschützern aber nicht aus.

Auch die **Zusammensetzung und die Arbeit des Ethikrates** wird **kritisiert**. Die Zusammensetzung des Ethikrates spreche nicht dafür, dass bei INDECT Bürgerrechte im Vordergrund stünden. Der Ethikrat setze sich nur aus nur Mitgliedern zusammen, die in das Projekt eingebunden seien. Eine unbefangene, auch kritische Kontrolle sei deshalb nicht möglich, das Projekt werde vielmehr nur geschützt⁴⁰. Statt mehr Transparenz seitens der Projektbetreuer zu fordern, fungiere der Ethikrat als „Veröffentlichungsfilter“, der nur die Publikation harmloser Erklärungen zulasse und bei Nachfragen der Öffentlichkeit abblocke⁴¹.

Erwähnenswert ist des Weiteren in Bezug auf Deutschland die **Position des Bundeskriminalamtes (BKA)**. Hierzu hat das BKA in einer Pressemitteilung von Oktober 2011⁴² darauf hingewiesen, dass dem BKA 2007 von Seiten der University of Science and Technology in Krakau, die mit der Leitung des INDECT-Projektes betraut sei, eine Partnerschaft angeboten worden sei. Diese habe das BKA **aufgrund des umfassenden Überwachungsgedankens** des Projektes abgelehnt. Seine Ablehnung habe es seit 2007 mehrfach schriftlich zum Ausdruck gebracht, sowohl gegenüber der beauftragenden EU-Kommission als auch der Projektleitung von INDECT. Auf Bitten der Projektleitung habe das BKA im Jahr 2009 INDECT-Beteiligten das BKA-eigene Projekt "Foto-Fahndung" vorgestellt. Dieses Projekt sei 2007 mit überwiegend negativen Forschungsergebnissen vom BKA eingestellt worden. Dies sei der alleinige und einmalige Beitrag des BKA zum INDECT-Projekt gewesen.

3. Grundrechtliche Implikationen

Da es sich bei INDECT um ein Forschungsprojekt handelt, dessen Umsetzung weder auf der Ebene der Europäischen Union (EU) noch auf der nationalen Ebene Anwendung findet, unterstellt die folgende Analyse die Realisierung der von INDECT erfassten Technologien. Zugrundegelegt werden dabei insbesondere die bereits aufgezählten wichtigsten Ziele 1 bis 7 des Programms (siehe 1.2, nachfolgend als „Ziel x“ bezeichnet). Denn **Einzelheiten zu den konkreten Maßnahmen**

38 Hoferer, Dominik, „Geplante Überwachung mit INDECT- Jeder Bürger steht unter Generalverdacht“, Focus Online vom 16.03.2012, http://www.focus.de/digital/computer/chip-exklusiv/tid-25266/ueberwachung-jeder-steht-unter-verdacht_aid_724007.html.

39 Monroy, Mattias, „Polnische Polizei steigt aus INDECT aus“, Telepolis, 16.04.2012, <http://www.heise.de/tp/artikel/36/36763/1.html>.

40 Hoferer, Dominik, „Geplante Überwachung mit INDECT- Jeder Bürger steht unter Generalverdacht“, Focus Online vom 16.03.2012, http://www.focus.de/digital/computer/chip-exklusiv/tid-25266/ueberwachung-jeder-steht-unter-verdacht_aid_724007.html.

41 Hoferer, Dominik, „Geplante Überwachung mit INDECT- Jeder Bürger steht unter Generalverdacht“, Focus Online vom 16.03.2012, http://www.focus.de/digital/computer/chip-exklusiv/tid-25266/ueberwachung-jeder-steht-unter-verdacht_aid_724007.html.

42 Siehe <http://www.presseportal.de/polizeipresse/pm/7/2129265/bka-das-bundeskriminalamt-teilt-mit-keine-beteiligung-am-eu-forschungsprojekt-indect-intelligent>.

men sind **nicht bekannt** sind. Daher kann nachfolgend auch nur eine **grobskizzenhafte Betrachtung** der möglichen grundrechtlichen Probleme erfolgen.

3.1. Überwachungsmaßnahmen des Internets

3.1.1. Post- und Fernmeldegeheimnis (Art.10 GG)

Es kommt im Hinblick auf die von INDECT ggf. entwickelten Systeme zur Überwachung des Internets eine Verletzung des **Fernmeldegeheimnisses** aus **Art. 10 Abs. 1 GG** in Betracht.

Der sachliche **Schutzbereich** des Fernmeldegeheimnisses umfasst alle „unkörperlichen Übermittlungen von Informationen...Dabei schützt das Fernmeldegeheimnis in erster Linie die Vertraulichkeit der ausgetauschten Information“⁴³, **den Inhalt der individuellen Kommunikation**.⁴⁴ Danach fällt die E-Mail grundsätzlich in den Schutzbereich des Art. 10 Abs. 1 GG. Dies gilt allerdings nicht, wenn der Zugriff durch entsprechende Zugangsregelung oder vom Informationseingebenden (offene Mailinglist) oder durch Einwilligung eines Kommunikationspartners gestattet ist.⁴⁵ Es ist also im Einzelfall Individual- von Massenkommunikation abzugrenzen, wobei der Inhalt letzterer nicht durch Art. 10 Abs. 1 GG geschützt wird.⁴⁶ Sollen durch die von INDECT entwickelten Agentensysteme tatsächlich ständig und automatisch auch private Computer kontrolliert werden können (Ziel 6) und würde dies z. B. auch den Inhalt von E-Mails betreffen, wäre ein Eingriff in den Schutzbereich zu bejahen.

Unter das Fernmeldegeheimnis fällt – ungeachtet der Frage, ob es um Massen- oder Individualkommunikation geht - zudem auch, ob jemand an einem **Kommunikationsvorgang** beteiligt war oder nicht. Somit sind die „Spuren“, die der Netzbenutzer im System hinterlässt, unabhängig vom „Grund“ der Nutzungsspur vom Schutzbereich des Art. 10 Abs.1 GG erfasst.⁴⁷ Der sachliche Schutzbereich endet allerdings dort, wo der Übertragungsvorgang beendet worden ist und die Kommunikation auf einem Endgerät verfügbar ist.⁴⁸

Sofern etwa die angesprochenen Agentensysteme die ständige und automatische Kontrolle öffentlicher Quellen wie z. B. Diskussionsforen, Usenet-Gruppen etc. verfolgen (Ziel 6), d. h. ob und wer an einem Kommunikationsvorgang beteiligt war, liegt ein Eingriff in Art. 10 Abs.1 GG vor. Er scheidet aus, wenn die Behörde nur allgemein zugängliche Inhalte erhebt, etwa indem sie die offenen Diskussionsforen oder nicht Zugangsgesicherte Webseiten einsieht und sich zur Effektivierung der Arbeit eines Agentensystems bedient.

43 BVerfGE „E-Mail- Postgeheimnis“, 2 BvR 2099/04 vom 2.3.2006, http://www.bverfg.de/entscheidungen/rs20060302_2bvr209904.html, Rn. 73-81.

44 Löwer, in: v. Münch/Kunig, Grundgesetz Kommentar, Bd. 1 , 6. Aufl., 2012, Art. 10 Rn. 18.

45 Löwer, in: v. Münch/Kunig, Art. 10 Rn. 20.

46 Löwer, in: v. Münch/Kunig, Art. 10 Rn. 20.

47 Löwer, in: v. Münch/Kunig, Art. 10 Rn. 20.

48 BVerfGE „E-Mail- Postgeheimnis“, 2 BvR 2099/04 vom 2.3.2006, http://www.bverfg.de/entscheidungen/rs20060302_2bvr209904.html, Rn. 73-81.

Ein Eingriff in das Fernmeldegeheimnis ist nur durch ein **formelles Gesetz** möglich.⁴⁹ Bei dem für die Umsetzung notwendigen formellem Gesetz, muss nach der ständigen Rechtsprechung des **BVerfG** außerdem das **Kriterium der Normenklarheit** erfüllt sein. Dies bedeutet, dass Anlass, Zweck und Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festgestellt werden müssen, um die geeignete Rechtssicherheit für den Bürger sicherzustellen.⁵⁰

Die Rechtmäßigkeit von Eingriffen in Art. 10 Abs. 1 GG ist zu bejahen, wenn sie **legitimen Gemeinwohlzwecken dienen** und im Übrigen **verhältnismäßig** sind.⁵¹ Die Verfassungsmäßigkeit im weiteren Sinne umfasst allgemein folgende Anforderungen: Legitimer Zweck, Geeignetheit, Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne.

Ein legitimer Zweck ist in Bezug auf Eingriffe in das Recht auf informationelle Selbstbestimmung dann zu bejahen, wenn dadurch Grundrechte Dritter oder andere Güter von Verfassungsrang geschützt werden. Die beabsichtigten Maßnahmen von INDECT sollen der Gefahrenabwehr dienen und die Verletzung der öffentlichen Sicherheit und Ordnung auch in der virtuellen Welt verhindern⁵². Ein legitimer Zweck könnte sich somit bejahen lassen.

Geeignet ist ein Eingriff immer dann, wenn er zumindest zur Erreichung des legitimen Zwecks förderlich ist. Dies könnte hier die Straftatenprävention und ggf. Strafverfolgung sein.

Die Maßnahmen von INDECT müssten aber auch erforderlich sein, d.h. es darf kein gleich geeigneteres, milderes Mittel geben. INDECT betont, die Suche nach für die Allgemeinheit gefährdenden Taten effektivieren und die Gefahrenprävention verbessern zu wollen. Gegenüber einer ständigen und automatischen Kontrolle privater Computer durch Agentensysteme (Ziel 6) dürften anlassbezogene Prüfungen als milderes Mittel erscheinen. Neben den Zweifeln an der Erforderlichkeit ist aber weiter zu bedenken: Die Verhältnismäßigkeit im engeren Sinne verlangt eine Abwägung zwischen dem Allgemeininteresse und dem individuellen Interesse der Grundrechtsträger. Bei der Überwachung des virtuellen Raumes handelt es sich um **verdachtslose Eingriffe mit großer Streubreite**, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden sollen, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen.⁵³ Es besteht eine **hohen Eingriffsintensität**, die streng am Verhältnismäßigkeitsgrundsatz gemessen werden muss. Zwar ist es legitim, Internetkriminalität und die Planung von Straftaten zu bekämpfen, ob dafür allerdings eine so große Streubreite notwendig ist, ist fraglich. Die Realisierung etwa von Ziel 6 dürfte somit wohl gegen den Grundsatz der Verhältnismäßigkeit verstoßen.

Sollte mit den von INDECT entwickelten Agentensystemen eine ständige und automatische Kontrolle sozialer Netzwerke im Internet tatsächlich in dieser Allgemeinheit beabsichtigt sein, so

49 Jarass, in: Jarass/Pieroth, GG, 9. Aufl. 2007, Art. 10 Rn. 16.

50 BVerfGE „Vorratsdatenspeicherung“, 1 BvR 256/08 vom 2.3.2010, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html, Rn. 328.

51 BVerfGE „Vorratsdatenspeicherung“, 1 BvR 256/08 vom 2.3.2010, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html, Rn. 204.

52 <http://www.indect-project.eu/>.

53 Hornung, Gerrit, „Smart Cameras“ und automatische Verhaltensanalyse“, Kommunikation & Recht, 2011, S. 155, <http://www.juris.de/jportal/portal/t/u8s/page/jurisw.psml?doc.hl=1&doc.id=jzs-KuR-1103A-153-1%3Ajuris-zs00&documentnumber=2&numberofresults=7&showdoccase=1&doc.part=A¶mfromHL=true#focuspoint>.

dürfte dies eine unverhältnismäßige Maßnahme darstellen, die als Verstoß gegen das Fernmeldegeheimnis nach Art. 10 Abs.1 GG zu werten wäre.

3.1.2. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art.2 Abs. 1 i. V. m. Art.1 Abs. 1 GG)

Das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** ist **subsidiär** gegenüber dem Fernmeldegeheimnis aus Art. 10 GG und stellt eine besondere Ausprägung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs.1 GG i. V. m. Art. 1 Abs. 1 GG dar.⁵⁴

Soweit es um Maßnahmen geht, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen.⁵⁵ Der Grundrechtsschutz des Art. 10 Abs. 1 GG erfasst dagegen nicht den Fall, dass eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solches überwacht oder die Speichermedien des Systems durchsucht.⁵⁶ Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt kein Eingriff in Art. 10 Abs. 1 GG. Dies gilt auch dann, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall.⁵⁷ Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist einschlägig, wenn es um Systeme geht, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.

Ein Eingriff in den Schutzbereich ist danach zu bejahen, wenn durch einen „heimlichen Zugriff die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können, sowohl am Arbeitsspeicher als auch bei den temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten.“⁵⁸ Sofern INDECT z. B. beabsichtigt, eine Suchmaschine für die schnelle Erkennung von Personen und Dokumenten anhand von digitalen Wasserzeichen zu entwickeln (Ziel 4), so dürfte im staatlichen Einsatz solcher Mittel eine Überwachung der Nutzung eines informationstechnischen Systems liegen. Gleiches ist wohl auch für eine mittels eines verteilten Computersystems Datenerhebung, -speicherung und -verwendung (Ziel 2), für Agentensysteme zur ständigen Kontrolle von öffentlichen Quellen im Internet und privaten Computern (Ziel 6), sofern dies nicht schon unter Art. 10 Abs. 1 GG gefasst wird (siehe oben 3.1.1), und im Falle eines internetbasierten intelligenten Datensammelsystems (Ziel 7) anzuneh-

54 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Rn. 168.

55 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Rn. 184.

56 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Rn. 186.

57 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Rn. 186

58 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Rn. 205.

men. Dies stellt einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar.

Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind grundsätzlich zu präventiven Zwecken und zur Strafverfolgung zulässig, müssen aber auf einem verfassungsmäßigen gesetzlichen Grundlage beruhen.⁵⁹ Im Hinblick auf die Verhältnismäßigkeit gilt, dass ein Eingriff nur gerechtfertigt ist, wenn tatsächliche Anhaltspunkte für eine **konkrete Gefahr für ein überragend wichtiges Rechtsgut** (z.B. Leib, Leben und Freiheit einer Person, Güter der Allgemeinheit) sprechen. Allerdings kann die Maßnahme schon dann rechtmäßig sein, „wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern **bestimmte Tatsachen auf eine im Einzelfall durch bestimmte** Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.“⁶⁰

2.3 Videoüberwachung im öffentlichen Raum

Die **automatische Videoüberwachung** kann als neue Stufe der Videoüberwachung angesehen werden, da sie „normales“ und „unnormales“ Verhalten erfasst und über eine verbesserte Technologie verfügt. Dies führt zu neuen Rechtsfragen im Bereich der Grundrechte und des Datenschutzes.

2.3.1 Recht auf informationelle Selbstbestimmung (Art.2 Abs. 1 i. V. m. Art.1 Abs. 1 GG)

Der sachliche Schutzbereich des **Rechts auf informationelle Selbstbestimmung** umfasst die **Freiheit jeder Person selbst zu entscheiden, was er von sich preisgeben möchte**, z.B. wann und wo sie an welchem Ort war, welche Kleidung sie getragen hat und mit wem er sich getroffen hat. Diese Freiheit kann durch die Videoüberwachung eingeschränkt werden. Ein **Eingriff** in den Schutzbereich läge bei der Videoüberwachung praktisch immer vor, dieser würde **bei der automatischen Videoüberwachung**, z.B. durch eine verbesserte Kameraoptik, noch **verschärft**. Die Streubreite und Intensität des Eingriffs erhöhe sich zunehmend⁶¹. Der Schutzbereich ist somit im Hinblick auf eine Testinstallation eines Überwachungssystems an verschiedenen Orten eines städtischen Ballungsraums und Erprobung eines Prototyps des Systems mit 15 Knotenpunkten (Ziel 1 von INDECT) eröffnet.

Es bedürfte eines legitimen Zweckes für eine solche Maßnahme. Der legitime Zweck ist die Gefahrenprävention, die durch die Videoüberwachung im öffentlichen Raum erreicht werden kann.

Auch müsste die Videoüberwachung des öffentlichen Raum geeignet sein, d.h. zumindest dem legitimen Zweck förderlich. Mittels intelligenter Kameras im öffentlichen Raum, können Gefahren schon vor ihrem Auftreten erkannt werden.

59 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Rn. 207.

60 BVerfG „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, BVerfG, 1 BvR 370/07 vom 27.2.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html, Leitsatz 2.

61 Hornung, Gerrit, „Smart Cameras“ und automatische Verhaltensanalyse“, Kommunikation & Recht, 2011, S. 155, <http://www.juris.de/jportal/portal/t/u8s/page/jurisw.psml?doc.hl=1&doc.id=jzs-KuR-1103A-153-1%3Ajuris-zs00&documentnumber=2&numberofresults=7&showdoccase=1&doc.part=A¶mfromHL=true#focuspoint>.

Diese INDECT-Maßnahme müsste auch erforderlich sein, d.h. es kann kein milderes, gleichsam wirksames Mittel geben. INDECT betont, automatische Videosysteme würden die Polizei entlasten und menschliche Fehler, insbesondere bei der Weitergabe von Daten, verhindern. Es ist dementsprechend zu prüfen, ob es keine Alternativen zu automatischen Überwachungssystemen gibt, z.B. eine Aufstockung des Personals der Sicherheitsbehörden, um Gefahren rechtzeitig erkennen zu können.

In Bezug auf die Angemessenheit wird vor allem die generelle Videoüberwachung im öffentlichen Raum aufgrund ihrer **hohen Eingriffsintensität** bemängelt. Die Polizeigesetze des Bundes und der Länder enthalten Befugnisnormen zur offenen Erhebung und Aufzeichnung von Bild- und Tondaten.⁶² Sofern mit Ziel 1 von INDECT eine großflächige Videoüberwachung beabsichtigt ist, könnte dies problematisch sein, weil jedenfalls die **generelle Videoüberwachung** wegen Verstoßes gegen das **Übermaßverbot** abgelehnt wird.⁶³ Sie wird daher allenfalls an „Kriminalitätsschwerpunkten“, d. h. an Orten, wo aufgrund von Tatsachen vermehrt Straftaten zu erwarten sind, oder in der Nähe wichtiger öffentlicher Gebäuden für mit dem Verhältnismäßigkeitsgrundsatz vereinbar gehalten. In diesem Sinne seien auch die gesetzlichen Ermächtigungsnormen zu interpretieren.⁶⁴ Weiterhin müssen zur Wahrung der Verhältnismäßigkeit die von der Videoüberwachung betroffenen Bürger auf die Überwachung hingewiesen werden, wenn dadurch der Zweck der Maßnahme nicht vereitelt wird⁶⁵. Eine Ausweitung der Videoüberwachung, sofern dies mit Ziel 1 von INDECT intendiert ist, stellt sich nach alledem im Hinblick auf die Verhältnismäßigkeit als ein problematischer Eingriff im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung dar.

4. Die Finanzierung des Projektes durch die BRD als Spannungsverhältnis zum Grundrechtsschutz?

Da sich INDECT in der Entwicklung bisher nur auf dem Stand eines Forschungsprojektes befindet und es bisher in der Bundesrepublik keinerlei konkrete Umsetzungsvorhaben gibt, steht auch das Ausmaß des Spannungsverhältnisses zwischen dem grundgesetzmäßigen Schutz der Bürgerinnen und Bürger und der Mitfinanzierung durch Deutschland im Rahmen der EU nicht fest.

62 Siehe hierzu: Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 4. Aufl., 2007, H 197.

63 Siehe hierzu: Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 4. Aufl., 2007, H 201.

64 Siehe hierzu: Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 4. Aufl., 2007, H 201.

65 [REDACTED], „Videoüberwachung- Vergleich der Gesetzeslage in Deutschland und dem Vereinigten Königreich“, Wissenschaftliche Dienste des Deutschen Bundestages (WD 3-473/07), 2007, S.4.