Soziologisches Seminar zur "Organisation im Zeitalter digitaler Medien"

Seminararbeit bei Prof. Dr. Katja Rost und Dr. Ernest Albert

(zus. mit Prof. Dr. em. Hans Geser) – HS 2013 / FS 2014, Soziologisches Institut, Universität Zürich

INDECT-Forschungsergebnisse der Europäischen Union

Chancen und Gefahren der Möglichkeiten zur zentralisierten und transnationalen Überwachung

Hernani Marques

Abgabedatum: 15.5.2014

Stufe: Master

Fachsemester: 2 (laufend)

Hauptfach: Computerlinguistik + Sprachtechnologie

1. Nebenfach: Soziologie

2. Nebenfach: Neuroinformatik

Inhaltsverzeichnis

1 Einleitung

> *Um ihre Herrschaft zu sichern, werden die Eliten frühzeitig den totalen Überwachungsstaat schaffen und eine weltweite Diktatur einführen.*
> (Carl Friedrich von Weizsäcker, 1994[1])

Das Jahr 2013 war gezeichnet von Enthüllungen[2], welche öffentliches Bewusstsein dafür geschafft haben, dass im Rahmen der zunehmenden Digitalisierung der Gesellschaft nicht bloss die globale kommunikative Vernetzung zugenommen hat, sondern auch die Möglichkeiten zur Überwachung der weltweiten Kommunikation.

Soziologisch stellt sich die Frage, inwiefern zentralisierte Überwachungsmöglichkeiten, die keinen Halt vor Staatsgrenzen machen, *einerseits* die Errungenschaften der digitalen Welt zunichte machen und *andererseits* – durch die massive Digitalisierung der Gesellschaft – Tür und Tor öffnen, den Weg für ein totalitäres System zu ebnen, das eben *nicht* auf den virtuellen Raum beschränkt bleibt, sondern in der "realen", physischen Welt spürbar wird.

Denn: Zusätzlich zur digitalen Überwachung durch Geheimdienste sind auch Entwicklungen auszumachen, die nicht unmittelbar mit der Kommunikation von Menschen über Telefonnetze oder das Internet zusammenhängen, sich dieser Technologien als Transportmedium aber bedienen, um zentralisiert Datensammlungen anzulegen, auf die immer mehr Personenkreise Zugriff erhalten.

In dieser Arbeit soll schwerpunktmässig auf ein mittlerweile abgeschlossenes EU-Forschungsprojekt eingangen werden, das sich "Intelligent information system support observation, searching and detection for security of citizens in urban environment" – kurzum: INDECT – nennt. Sektion 3 führt in dieses System, das ein umfassendes Überwachungssystem auf Basis von Video-, Ton- und Textdaten vorsieht, um strafbare Handlungen zu antizipieren.

Zunächst werden mit Sektion 2 soziologische Begriffe und Konzepte aufgewor-

[1] Zitat in: Weizsäcker, C. F. v. (1994): *Der bedrohte Friede – heute*. München: Hanser.
[2] Im besonderen Masse auf Basis von Quellen des ehemaligen Geheimdienstmitarbeiters Edward Joseph Snowden.

fen, die von einem praktischen INDECT-System berührt sind. Dies erlaubt es den betrachteten Gegenstand soziologisch klarer zu fassen.

Weitere Aspekte von INDECT werden in Sektion 4 diskutiert und kritisch hinterfragt. Zusätzlich wird INDECT in den Kontext mit weiterer (artverwandter) Forschung, die stattgefunden hat oder noch stattfinden wird, gestellt.

Abschliessend wird im Fazit (Sektion 5) die Arbeit rekapituliert und eine Einschätzung abgegeben.

2 Soziologische Verortung der Thematik

> *[...] [D]ie Kontrollgesellschaften operieren mit Maschinen der dritten Art, Informationsmaschinen und Computern, deren passive Gefahr in der Störung besteht und deren aktive Gefahr Computer-Hacker und elektronische Viren bilden.*
> (Gilles Deleuze, 1993[3])

Die hier eingeführten Begriffe und Konzepte sind hilfreich dabei, die von INDECT betroffenen Gesellschaftsbereiche besser zu verstehen und im Rahmen der Diskussion (vgl. Sektion 4) und der Schlussbetrachtungen in Sektion 5 zu einer Technikfolgenabschätzung zu gelangen.

2.1 Nominelle Freiheitsrechte und Alltagswirklichkeit

In zumindest westlichen Industriegesellschaften wird der individuellen Freiheit hohe Bedeutung zugemessen. Eingriffe im Sinne der (allgemeinen) Sicherheit oder zu ungunsten der (individuellen) Freiheit sind (nominell) nur eingeschränkt und auf gesetzlicher Grundlage vorgesehen.

Diese Normen drücken sich in der Schweizerischen Bundesverfassung BV an verschiedener Stelle (nicht-abschliessend) aus:

[3] Zitat in: Deleuze, G. (1993) [3]

- Art. 8 Abs. 2 BV “Rechtsgleichheit”: Ein Diskriminierungsverbot von Menschen, z. B. auf Grund der “Lebensform” oder der “politsichen Überzeugung”.[4]
- Art. 9 BV “Schutz vor Willkür und Wahrung von Treu und Glauben”: Es wird postuliert, dass Personen vor staatlichen Willkürhandlungen geschützt sind.[5]
- Art. 10 Abs. 2 BV “Recht auf Leben und auf persönliche Freiheit”: “Körperliche” und “geistige Unversehrtheit” wird garantiert, sowie das Recht auf “Bewegungsfreiheit”.[6]
- Art. 13 BV “Schutz der Privatsphäre”: Es wird für sowohl virtuelle als auch physische Räume das Recht auf Privatsphäre festgehalten.[7]
- Art. 32 Abs. 1 BV “Strafverfahren”: Die Unschuldsvermutung wird konstituiert.[8]

Doch: Beispiele von Vorgängen, die sich dieser Normen faktisch entziehen, sind zahlreich; es seien fünf Beispiele erwähnt, die viele der postulierten Rechte (alltagspraktisch) aushebeln:

- Apps von Smartphones können z. B. die GPS-Koordinaten oder via IP-Adresse den etwaigen Standort ihrer User nachvollziehen.
- Handyprovider müssen vielerorts – so auch in der Schweiz[9] – die Metadaten der Kommunikation[10] speichern. Unabhängig eines bewussten Kommunikationsvorgang kann der Provider nachvollziehen, wo sich das Gerät einer Person befindet. Dies geschieht für die Möglichkeit der “rückwirkenden Überwachung”; die Unschuldsvermutung wird ausgehebelt.

[4] Schweizerische Bundesverfassung Art. 8. Online: http://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a8 (Abruf: 14.5.2014)

[5] Schweizerische Bundesverfassung Art. 9. Online: http://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a9 (Abruf: 14.5.2014)

[6] Schweizerische Bundesverfassung Art. 10. Online: http://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a10 (Abruf: 14.5.2014)

[7] Schweizerische Bundesverfassung Art. 13. Online: http://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a13 (Abruf: 14.5.2014)

[8] Schweizerische Bundesverfassung Art. 32. Online: http://www.admin.ch/opc/de/classified-compilation/19995395/index.html#a32 (Abruf: 14.5.2014)

[9] In der Schweiz aktuell für sechs Monate; geplant ist die Verdoppelung der “Vorratsdatenspeicherung” auf 12 Monate.

[10] Es sind Antworten auf Fragen möglich, wer wann, wie lange, mit wem und wo telefoniert hat.

- Die Videoüberwachung im öffentlichen Raum ist in einigen Ländern, wie z. B. England, massiv vernetzt. An anderen Orten finden entsprechende Projekte statt. So bestehen Begehren, auch auf private Videoüberwachungsanlagen zugreifen zu können, etwa seitens des Schweizer Nachrichtendienstes – NDB.[11]
- Einkäufe, die bargeldlos stattfinden, erlauben eine umfassende Analyse des Kaufverhaltens und entsprechend der Präferenzen der entsprechenden Kundschaft. Zusätzlich bestehen Einkaufskarten mit Punktesystem, welche eine minutiöse Datensammlung darüber erlauben, wer, wann, was und wo gekauft hat.
- Digitale Krankenkassenkarten (mit Mikrochip) ermöglichen es, Einsicht in Krankheitsbilder von Personen zu erhalten – direkt auf dem Chip gespeichert. Dieses System soll u. a. den bis anhin unheitlichen Zugriff zu Informationen über den Gesundheitszustand einer Person vereinfachen.[12]

2.2 Deviantes Verhalten und Überwachungsdruck

Deviantes Verhalten bedeutet Verhalten, das von (geltenden) sozialen Normen in einer Gesellschaft abweicht. Ideellerweise spiegeln sich soziale Normen in gesetzlichen Normen wieder, d. h. die Gesellschaft verhält sich in aller Regel nach den gesetzlichen Vorgaben. Die in einer Gesellschaft zugrunde liegenden Normen haben sich durch repetitives Handeln ergeben und drücken sich schliesslich in Gesetze aus.

Für ihre Nicht-Einhaltung drohen je nach Gesellschaft verschiedene Formen von Sanktionen, die zur Funktion haben die geltende Ordnung zu erhalten. Giddens (vgl. 2009: 943ff.) weist darauf hin, dass praktisch alle Akteure einer Gesellschaft im Zuge ihrer Leben deviant handeln. Nicht jede Form von Normabweichung konstituiert allerdings eine derart "gravierende" Handlung, das dafür direkt strafrechtliche Konsequenzen drohen.

In vielen Fällen stellen Abweichungen der Norm auch nur eine Verletzung gegen guten Sitten oder kulturelle Vorstellungen dar. In solchen Fällen geraten die

[11] Vgl. VBS (2014: 57). [9]

[12] Vgl. "FAQ zur Versichertenkarte" (in der Schweiz) auf der Webseite vom Bundesamt für Gesundheit BAG. Online: http://www.bag.admin.ch/themen/krankenversicherung/04114/07062/index.html?lang=de (Abruf: 7.5.2014)

deviant handelnden Akteure nicht in Konflikt mit den Ordnungskräften einer Gesellschaft, sondern erfahren bestenfalls Sanktionen auf Ebene der Inklusion in Gruppen oder anderen Formen sozialer Exklusion

In Tremmels Arbeit (vgl. 2010: 10ff. [8]) mit Bezug auf Focaults Machttheorie wird der Begriff des "Überwachungsdrucks" geführt. Demnach führt eine Überwachung dazu, dass Akteure sich durch das Bewusstsein darüber überwacht zu werden, normkonformer verhalten und weniger dazu neigen, straffällig zu werden. Funktional betrachtet kann die Politik in einem Land zum Schluss gelangen, dass eine umfassende Überwachung der Gesellschaft das Ziel, straffälliges Verhalten zu reduzieren, begünstigen kann. Genau in diesem Bereich ist das INDECT-Projekt angelegt.

3 Übersicht INDECT-Forschungsergebnisse

3.1 Absicht von und Ressourcen zu INDECT

Beim "Intelligent information system supporting observation, searching and detection for security of citizens in urban environment" – INDECT – handelt es sich um ein europäisch angelegtes Forschungsprojekt, das im Zuge des 7. Forschungsrahmenprogramms der Europäischen Union FP7 gestartet wurde. Die Laufzeit des Projekts waren fünf Jahre – von 2009 bis 2013. Während dieser Zeit standen dem Projektteam ein Forschungsbudget von EUR 15 Millionen zur Verfügung – davon EUR 10 Millionen direkt aus der Europäichen Union.[13]

In insgesamt acht technischen Arbeitspaketen ("Work-Packages") besteht nach INDECT-eigenen Angaben das folgende, ambitionierte Projekt:[14]

> The aim of INDECT is to develop solutions to and tools for automatic threat detection through e.g. processing of CCTV camera data streams, standardization of video sequence quality for user applications, threat

[13] Webseite "Enterprise and Indusry" zum INDECT-Projekt der Europäischen Kommission. Online: http://ec.europa.eu/enterprise/policies/security/indect/index_en.htm (Abruf: 12.5.2014)

[14] Angaben aus den "Frequently Asked Questions" Q1.2 der INDECT-Projektwebseite. Online: http://www.indect-project.eu/faq#Q1.2 (Abruf: 11.5.2014)

> detection in computer networks as well as data and privacy protection. New techniques for intelligent analysis of data will allow recognizing such situations, and giving alert before it is too late. The objective is also to recognize events that could lead to terrorist attacks (e.g. left luggage at an airport, automatic recognition of dangerous tools).

Erklärtes Ziel ist es, auffälliges Verhalten in der Bevölkerung, das sich aus Daten von Videoüberwachungsanlagen, doch auch aus anderen virtuellen Quellen in (semi-)öffentlichen[15] Sphären von z. B. Webforen oder Chats befindet, zu verknüpfen, um Gefahren für die Bevölkerung abzuwenden. Wichtiges Ziel sei, Straftaten vorzubeugen – im Sinne der präventiven Sicherheit sollen diese bereits in der Vorbereitung erkannt und folglich verhindert werden.

In diesem Zusammenhang wird in den verschiedenen Work-Packages nicht nur erforscht, was auffälliges Kommunikations- oder Bewegungsverhalten ist, sondern genauso ist Forschungsgegenstand, Methoden der (Neuro-)Informatik[16] oder Computerlinguistik[17] geschickt über taugliche Algorithmen dieser Bereiche so zu verknüpfen, dass ein umfassendes Gefahrenbild der Handlungen in der Bevölkerung möglich wird.

In der Science-Fiction ist das anvisierte Szenario am ehesten mit dem 2002 erschienenen US-amerikanischen Blockbuster-Film "Minority Report"[18] zu vergleichen. In der darin skizzierten Welt ist es möglich, Personen auf Schritt und Tritt – insbesondere dank umfassender Video-, doch auch Kommunikationsüberwachung – zu verfolgen und entsprechend polizeilich einzugreifen.

Ist dies übertrieben? Dass dieses Szenario greifbar ist, zeigen INDECT-Projektvideos bereits von 2010 auf YouTube. In einem Video wird exemplarisch illustriert, wie ein

[15] Obwohl viele Webdienste im Internet frei zugänglich sind, liegt deren entsprechendes Datenmaterial nicht ohne Anmeldung vor.

[16] Die Neuroinformatik beschäftigt sich mit neuronalen Netzen und Lernverfahren, die dem Gehirn von Menschen oder anderen biologischen Wesen, die Daten neuronal – auf Basis von Neuronen oder ähnlicher (virtueller) Prozessierungseinheiten – verarbeiten.

[17] im Englischen auch "Natural Language Processing" oder auch "Machine Learning", wenn es um maschinelle Lernverfahren aus dem Bereich der Informatik im Zusammenhang mit linguistischen Daten geht.

[18] Vgl. IMDB-Datenbank zu "Minority Report". Online: http://www.imdb.com/title/tt0181689/ (Abruf: 6.5.2014)

Raubüberfall zwischen zwei sich kreuzenden Personen erfolgreich erkannt wird.[19]

Ein zweites Projektvideo mutet eher harmlos an: Es handelt sich um die im Rahmen des Forschungsprogramms entwickelte Applikation "INSTREET", welche fähig ist, auf Basis eines Stadtbilds (z. B. eines Hauses), die entsprechende Lokalität in der Welt aufzuspüren.[20]

Das dritte Video, das stellvertretend für die facettenreiche Natur des INDECT-Projekt steht, beschäftigt sich mit der automatischen Erkennung (zu lange) liegengelassener Gepäcksstücke – nach einer zu definierten Zeitspanne wird ein derartiger Vorgang als verdächtig, somit als Sicherheitsrisiko eingeschätzt und entsprechend markiert.[21]

Vom INDECT-Projekt selber bestehen weitere Videos auf YouTube, die erkennen lassen, dass es im Bereich der Videoüberwachung ebenfalls um die Detektion verdächtiger "crowds" [22], oder um kryptografische Massnahmen geht, den Zugriff auf die sensiblen personenbezogenen Daten einzuschränken.[23]

Obwohl die vielen Einzelergebnisse des INDECT-Projekts teilweise harmlos anmuten, so darf nicht vergessen werden, dass das INDECT-Projekt ein systemisches Konzept verfolgt, wonach die verschiedenen Technologien ineinander integriert werden sollen. Zum anderen ist zu beachten, dass INDECT nur eines von vielen Projekten ist, das sich in diesem Bereich bewegt. Es ist – für sich genommen – das wohl umfassendste Projekt dieser Art, allerdings ist es durch Ergebnisse weiterer Forschung flexibel ausbaubar.

[19] Video "Automatic detection of threats based on video analysis for city security systems" des INDECT-Projekts auf YouTube. Online: https://www.youtube.com/watch?v=qvb-63DstTk (Abruf: 4.5.2014)

[20] Video "INSTREET Demo" des INDECT-Projekts auf YouTube. Online: http://www.youtube.com/watch?v=k4Y9_kdzcHw (Abruf: 4.5.2014)

[21] Video "Left luggage detection" des INDECT-Projekts auf YouTube. Online: https://www.youtube.com/watch?v=crhJ4oie9Ds (Abruf: 4.5.2014)

[22] Englisch für "Menschenansammlungen/-massen"

[23] Übersicht der INDECT-Videos auf YouTube. Online: https://www.youtube.com/user/INDECTproject/videos (Abruf: 4.5.2014)

3.2 Schematische Funktionsweise von INDECT

In verschiedenen Grafiken illustriert das INDECT-Projekt auf der eigenen Projektwebseite[24] die integrierte Natur des Systems.

Eine erste Grafik (vgl. Bild 3.2) präsentiert das INDECT-System in seinen drei Säulen:

- Die erste (blaue) Säule "Intelligent Monitoring for Threat Detection": In diesen Bereich fällt die Überwachung des öffentlichen Raums durch stationäre Videoüberwachungsanlagen oder Drohnen.
- Die zweite (rote) Säule "Threat Detection in Computer Networks" symbolisiert den virtuellen (semi-)öffentlichen Raum; betroffen sind z. B. Chat-Systeme, Foren, Webseiten usw.
- Die dritte (grüne) Säule "Data Protection and Privcacy Protection" verpflichtet sich dem Ziel, Personendaten im INDECT-System vor unbefugten Zugriff zu schützen; ideell soll im Rahmen dieser Säule auch verhindert werden, dass unbescholtene Bürger vom System (länger, missbräuchlich) erfasst werden.

Die zweite Grafik (vgl. Bild 3.2) zeigt schematisch Ziele und Ergebnisse des INDECT-Projekts auf.

Die im Rahmen des Ziels der Gefahrenerkennung[25] erfassten Personen werden gegen die INDECT-(Such-)Plattform abgeglichen; Ergebnisse können sein, dass (1) gefährliche Werkzeuge erkannt worden sind[26], (2) eine hilfesuchende Person detektiert oder gebrochenes Glas[27] festgestellt wurde[28], (3) liegengelassenes Gepäck festgestellt wurde[29] oder (4) Fahrzeuge ins Visier geraten sind, welche für kriminelle Aktivitäten zum Einsatz kommen dürften[30] – die Liste ist klarerweise unvollständig.

[24] INDECT-Projektwebseite. Online: http://www.indect-project.eu (Abruf: 2.5.2014)
[25] Englisch "Threat Detection"
[26] Englisch "Dangerous tools detection"
[27] Dies kann im Rahmen von Raubüberfällen oder Protesten der Fall sein.
[28] Englisch "Detection of crying for help, broken glass"
[29] Englisch "Detection of unattended luggage"
[30] Englisch "Monitoring of vehicles for crime"

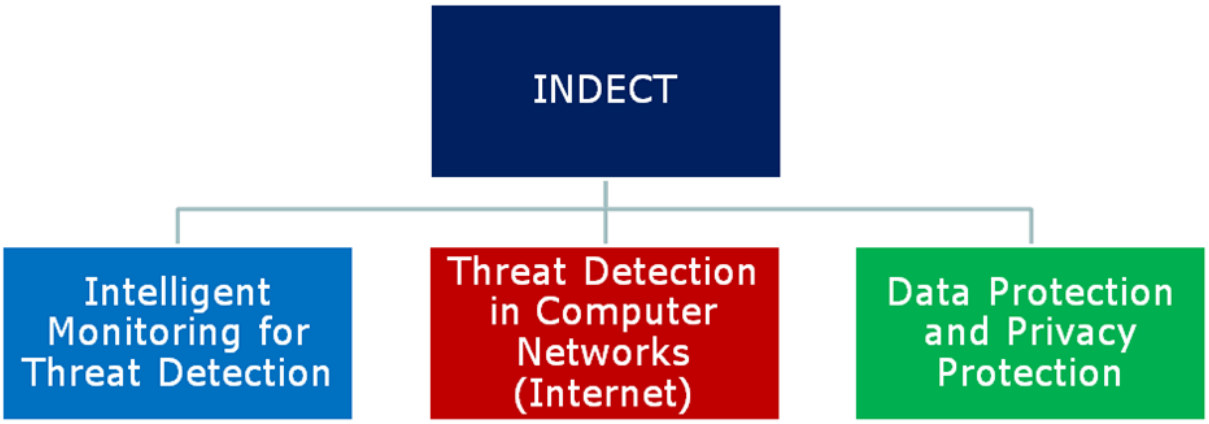

Abbildung 1: Illustration Säulen des INDECT-Forschungsprojekts.
[31]

3.3 Ausgewählte Ergebnisse der Work-Packages

Das INDECT-Projekt ist in acht[33] technischen Work-Packages gegliedert, für die auf der Open Access-Plattform der EU "OpenZaire" 131 Publikationen gelistet sind.[34] Grossmehrheitlich sind die Dokumente 2011[35] und 2012[36] publiziert worden.

Allerdings sind rund ein Viertel der Dokumente Closed Access[37]; dabei sind sechs Dokumente vom Zugangstyp "restricted", sind also nur projektintern verfügbar. Die rund 80 Open Access-Dokumente sind in übersichtlicher Form auch auf der INDECT-Projektwebseite verfügbar.[38]

Die Work-Packages gliedern sich wie folgt:

- Work-Package 1 "Intelligent Monitoring and Automatic Detection of Threats": Die Einspeisung von Audio- und Videoströmen von Kameras und Mikrofonen

[33] Vgl. Derkacz (2010: 12ff.) [2]
[34] INDECT-Projektseite auf der OpenZaire-Plattform der EU.
Online:
https://www.openaire.eu/index.php?option=com_openaire&view=project&Itemid=162&projectId=corda_____::f9c412f4928164da78a325c6bbf19972
(Abruf: 12.5.2014)
[35] 51 Publikationen
[36] 45 Publikationen
[37] INDECT-Projektseite auf der OpenZaire-Plattform der EU, die vom Typ Closed Access sind.
Online:
https://www.openaire.eu/index.php?option=com_openaire&view=browsepublications&Itemid=162&project=corda_____::f9c412f4928164da78a325c6bbf19972&accessMode=Closed+Access
(Abruf: 12.5.2014)
[38] "Public Deliverables"-Webseite des INDECT-Projekts mit allen Open Access-Dokumenten des Projekts. Online: http://www.indect-project.eu/public-deliverables (Abruf: 9.5.2014)

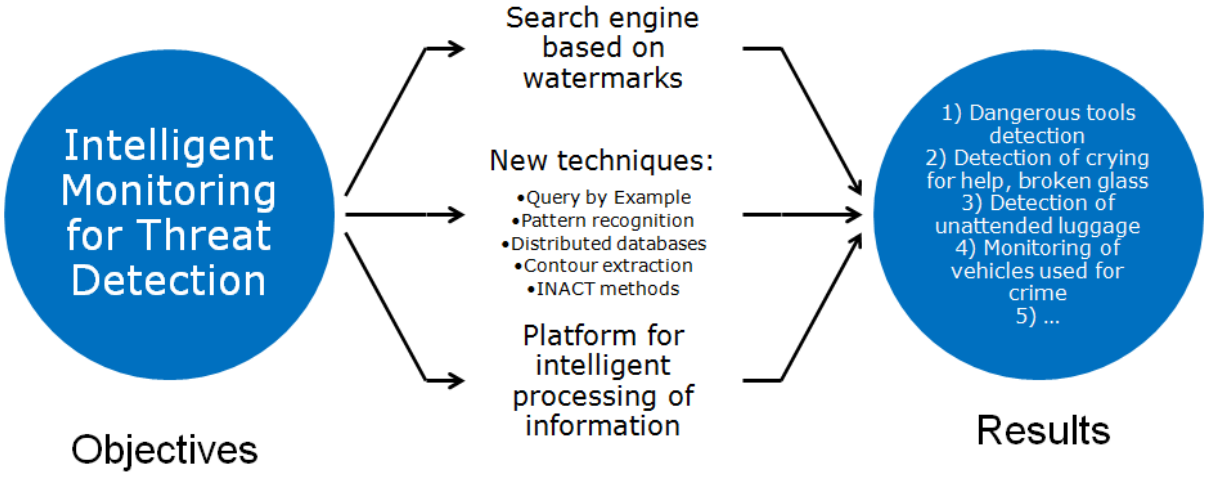

Abbildung 2: Illustration Ziele und (vorgesehene) Resultate eines (integrierten) INDECT-Systems.
[32]

sind hier Ziel, verknüpft mit der Fähigkeit in den Signalen Gefahren zu erkennen, etwa der Art: Schüsse, Glaszersplitterung, Hilferufe in den verschiedenen europäischen Sprachen usw.

- Work-Package 2 “Identification and Observation of Mobile Objects in Urban Environment”: Im Rahmen dieses Pakets sollen mobile Objekte erkannt werden können, darunter z. B. (kleine) Flugobjekte oder Fahrzeuge; zum Einsatz sollen auch Drohnen[39] kommen.

- Work-Package 3 “Intelligent integrated agent-based system supporting observation, analysis and detection of criminal activities and threats in complex real-virtual environments”: Eine Plattform, wo Informationen aus zahlreichen Internetquellen (z. B. Webseiten) Zusammenlaufen, wird erforscht.[40] Ebenfalls gehört die Entwicklung von Traffic-Analyse-Tools hinzu, um Kommunikation zu überwachen.[41]

- Work-Package 4 “Extraction of Information for Crime Prevention by Combining Web Derived Knowledge and Unstructured Data”: Dieses Arbeitspaket führt das “Relationship Mining” zum Ziel, das über Internetdatenquellen wie

[39] “UAV” für “Unmanned Aerial Vehicle” genannt
[40] Das System trägt den Namen “MAS” für “Multi Agent System”
[41] Es wird von einem “INDECT Lawful Interception tool” gesprochen.

Foren, Blogs oder sozialen Netzwerken gespiesen wird; es sollen Relationen ausgemacht werden, welche kriminelle Personen überführen.

- Work-Package 5 “Search Engine for Fast Detection of Person and Documents Based on Watermarking and Agent Technology”: In diesem Forschungspaket wird eine semantische Suchmaschine anvisiert, welche die Suche nach Beziehungen zwischen Personen in verschiedenen Datenquellen erlaubt und es z. B. auch ermöglicht, Personen auf Basis von Multimediamaterial aufzuspüren.
- Work-Package 6 “Interactive Multimedia Applications Portal for Intelligent Observation System”: Dieses Paket führt ein zentrales Zugriffssystem, das “INDECT Web Portal”, wobei der Zugrif nach Privilegien und Rollen eingeschränkt ist. Das Portal bietet ein Ablagesystem und ein Videokonferenzsystem zur Kommunikation.
- Work-Package 7 “Biometrics and Intelligent Methods for Extraction and Supplying Security Information”: In diesem Forschungsbereich wird die Technologie erarbeitet, um auf Grund von biometrischen Merkmalen Personen zu verfolgen, u. a. auf auditiver Basis.
- Work-Package 8 “Security and Privacy Management ”: Dieses Paket beschäftigt sich mit den kryptografischen Verfahren, um die erhobenen und zentralisierten Daten durch ausreichend sichere Verfahren vor fremden Zugriffen zu schützen. Diese Massnahmen sollen den Datenschutz der betroffenen Personen sichern.

Es fällt auf, dass für praktisch alle Work-Packages Open Access-Dokumente existieren. Im Bereich des Work-Package 3 allerdings bestehen keine öffentlich zugänglichen Dokumente. Dies mag mit der (vermeintlichen) Brisanz des darin erarbeiten Wissens zusammenhängen.

In einem Treffen des betreffenden Teams, das vom 24. bis 25. Juni in Grenoble stattgefunden hat, fallen Begriffe wie “WiFi-Monitoring” oder “Malware-Detection” mit welchen sich beschäftigt wurde.[42] Dabei handelt es sich um Massnahmen zur Überwachung von drahtlosen Netzwerken oder zur Erkennung von Schadsoftware im Internet. Es können nur Vermutungen angestellt werden, dass sich die Forschenden durch Nicht-Publikation entsprechender Ergebnisse Wissensvorsprünge

[42] Vgl. Webseite “WP3 Meeting in Grenoble on June 24-25, 2010” auf der INDECT-Projektwebseite. Online: http://www.indect-project.eu/events/wp3/wp3-meeting-in-grenoble-on-june-24-25-2010 (Abruf: 11.5.2014)

erhoffen. Einem weiteren Treffen in Warschau, das am 8. Mai 2011 stattgefunden hat,[43] sind keine inhaltlichen Informationen zu entnehmen.

Andererseits finden sich Hinweise zur hohen Datensensibilität bei Work-Package 3 bei Ciarkowski et al. (2012: 46ff. [1]) – in einem Papier des Work-Package 8. So liest sich dort:

> [...] Given the challenging nature of collecting so much data from so many Internet sources (web sites, discussion forums, social networks, etc), it has been agreed to partition the challenge into a number of small and feasible sub-problems, each addressed by simple and modular agents. [...]

U. a. sollen Korrelationen in sozialen Netzwerken erkannt werden, die dazu dienlich sind, Kriminelle zu überführen.

Über die konkrete Vorgehensweise bei der Detektion von Personen, die in "Terrorismus" oder "Hooliganismus" verwickelt sind, wird in D4.1 – einem Papier des Work-Package 4 – informiert, das von Klapaftis et al. (2009: 33ff. [6]) der University of York stammt. Am Beispiel eines Weblogs und von Newsmeldungen wird aufgezeigt, wie auf Basis von Methoden der Computerlinguistik, die entsprechenden Zusammenhänge hergestellt werden.

In einem weiteren Papier, das sich mit Verhaltensprofilierung[44] beschäftigt, ist eine Tabelle interessant, welche verschiedene (verdächtige) kriminelle Taten führt. (Vgl. Klapaftis (2010: 11ff. [7])

Nebst Diebstahl oder Vandalismus sind darin auch computerbezogene Handlungen aufgeführt, die von "denial of service", über "port scans" zu "monitoring network traffic" reichen. Letztere zwei Vorgänge erscheinen eigenartig, da diese Vorgänge in der IT-Security üblich sein können, um die Netzwerksicherheit zu gewährleisten.

[43] Vgl. Webseite "WP3 Meeting at The Police Headquarters in Warsaw". Online: http://www.indect-project.eu/events/wp3/wp3-meeting-at-the-police-headquarters-in-warsaw (Abruf: 11.5.2014)

[44] Auf Englisch "behavioural profiling"

4 Diskussion und Kritik der Erkenntnisse

Diese Sektion diskutiert die vorangegangene Recherchearbeit und diskutiert sie im Kontext (öffentlich) verfügbarer Kritik und den Verlautbarungen des INDECT-Projekts gegenüber (eben diesen) Vorwürfen. Zusätzlich wirft die Arbeit diverse Erkenntnisse – so z. B. Widersprüche – zur Diskussion auf oder beleuchtet Aspekte des INDECT-Projekts, welche bis dato nicht oder nur unzureichend beleuchtet wurden.

4.1 Datenschutzbestrebungen auf Invasionsgrundlage?

Das INDECT-Projekt behauptet in den FAQ[45] sich besonders um Datenschutzanliegen zu kümmern; so fallen darin folgende Aussagen:

> However, with INDECT solutions, the analysis of data is performed automatically and the access to the sensitive content is strictly registered (the date, time and the person who accessed), furthermore, even if there was a leakage, due to the watermarking techniques, it can be easily determined who is responsible for the abuse or negligence.

Demnach ist im INDECT-Verbund, unter der Voraussetzung es würde überhaupt entsprechend den vorgeschlagenen (strengen) Kriterien gemäss entwickelt werden, die Möglichkeit da, die Verantwortlichen dingfest zu machen, die für ein Leaking von Informationen verantwortlich wären.

Dies heisst aber nur, es könnte ausgemacht werden, welche polizeiliche oder (andere) Datenquelle für die Preisgabe der sensiblen Informationen verantwortlichen wären.

Denn: Es bleiben zumindest zwei Aspekte mit diesen Aussagen in den Dokumenten unbeantwortet und somit (soweit) ungelöst:

1. Gegen Angriffe von Dritten, z. B. bei unzureichend ungesicherten Systemen von aussen oder durch interne Infiltration könnte eine Veröffentlichung der

[45] Vgl. Q2.7 der "Frequently Asked Questions" auf der INDECT-Projektwebseite. Online: http://www.indect-project.eu/faq#Q2.7 (Abruf: 13.5.2014)

Daten in einer Art erfolgen, dass keine klare (personale) Verantwortlichkeit festzustellen ist.

2. Geraten sensible, personenbezogene Daten über überwachte Menschen in der einen oder anderen Weise nach aussen, so ist ihnen in keinem Fall geholfen, auch wenn Verantwortlichkeiten festgestellt werden können. Die massive Vernetzung, welche INDECT aus verschiedenen Datenquellen erlaubt, ist zugleich ihre datenschutzmässig betrachtet grosse Gefahr.

Somit wird deutlich: Sollte eine praktische INDECT-Installation verwundbar für Datenlecks werden, so "bezahlen die Zeche" zuletzt die Leute – bar mit ihren Daten. Eine Wiedergutmachung ist auf Grund der Natur des Netzes, Daten beliebig und praktisch ohne Kosten vervielfältigen zu können, nicht möglich.

Dadurch, dass INDECT – z. B. im Bereich der Überwachung im öffentlichen Raum oder in Foren – Daten ohne direkte Einwilligung sammeln möchte, besteht auch kein Konsens darüber, dass es der Bevölkerung nicht wichtig wäre, ihre Daten geschützt zu haben.

Es kann argumentiert werden, dass Internetuser darüber Bescheid wissen müssten und sich darauf einzustellen hätten, dass (technisch) jederzeit Daten von verschiedenen (dezentralen) Systemen an die Öffentlichkeit geraten können – dies nicht nur auf Grund des Inhalts der (sich verändernden) Allgemeinen Geschäftsbedingungen vieler Content-Provider, aber auch auf Grund von Leaks, welche durch Angriffe erbeutet werden.

Doch dieser mögliche Einwand ist verkürzt, denn ein wichtiger qualtiativer Unterschied besteht. Es existiert (gesichert) bisher kein System, das eine derart umfassende und zentralisierte Datensammlung aus verschiedener Datenquelle vornimmt. Zudem hat das INDECT-System aufzwingenden Charakter. Keine Person wird ihre Einwilligung geben können, ihre Textbeiträge mit Videobilddaten öffentlicher und gegebenfalls privater Videoüberwachungsanlagen zu verknüpfen und algorithmisch zu verarbeiten.

4.2 Forschungsprojekt vs. Implementierungsarbeiten

Auf der INDECT-Projektwebseite[46] steht seit Neuestem:

> INDECT is not installing any cameras in the EU; nor is it filming people at random. It is not connected to any existing database or social network.

Dies stimmt natürlich für das Forschungsprojekt an und für sich, andererseits wurden im Rahmen der explorativen Arbeiten dermassen viele Werkzeuge produziert, dass es unwahrscheinlich erscheint, diese würden zuletzt gar nicht eingesetzt.

Ob es zumindest in der EU zum (vollen) Einsatz des INDECT-Systems kommen kann, sei zumindest aus rechtsstaatlicher Perspektive in Frage gestellt.

Auf der anderen Seite besteht die Gefahr, dass das System als Ganzes oder in (grösseren) Teilen in anderen Ländern als Exportware zum Einsatz kommen könnte, die der (allgemeinen) Sicherheit (auch nominell) mehr Wert beimessen als der (individuellen) Freiheit.

Durch die Beteiligung von Wirtschaftsunternehmungen verschiedener EU-Länder an dem Projekt ist diese Möglichkeiten real. Diese haben sich im Rahmen fünfjähriger Forschungsarbeiten reges Wissen und diverse Prototypen earbeitet, die einen Marktwert besitzen. Auch an Universitäten sind lauffähige Prototypen entstanden, die über Startups oder Joint-Ventures auf den Markt gelangen können.

4.3 INDECT im Kontext anderer FP7-Forschung

Im Rahmen des 7. Forschungsrahmenprogramms der EU FP7 sind insgesamt EUR 1.4 Milliarden zur Verfügung gestellt worden, um spezifisch im Bereich der Sicherheit – als "FP7-SECURITY" bezeichnet – zu forschen.[47]

Im Kontext der massiven Forschung in FP7-SECURITY stellt INDECT nur eines von über 100 Projekten dar. Diese sind in sieben Bereiche unterteilt, darunter

[46] Vgl. INDECT-Projektwebseite.
Online: http://www.indect-project.eu/ (Abruf: 13.5.2014)

[47] Webseite "FP7 - Research Theme: Security" auf der CORDIS-Plattform der EU.
Online: http://cordis.europa.eu/programme/rcn/861_en.html (Abruf: 13.5.2014)

"Security of the Citizens" und "Security of infrastructures and utilities". Auf der entsprechenden Webseite[48] des CORDIS-Portals[49] wird INDECT im Bereich "Security of the Citizens" geführt.

Es seien im Folgenden zwei weitere Projekte hervorgehoben und ihre Möglichkeiten skizziert, diese mit INDECT (praktisch) zu verbinden:[50]

- Das Projekt "Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces" (ADABTS) wurde mit insgesamt EUR 4.5 Millionen gefördert und erörtert insbesondere die Frage, was "abnormales" (von der sozialen Norm abweichendes) Verhalten im Rahmen (grösserer) Menschenansammlungen ist. Es steht in engem Zusammenhang mit Videoüberwachung, das bei INDECT selber ein Schwerpunktthema ist.[51]
- Es lief ein Projekt "Surveillance of unattended baggage and the identification and tracking of the owner" (subito), das mit fast EUR 4 Millionen gefördert wurde und das Ziel verfolgt hat, sich mit der Thematik der unbeaufsichtigten Gepäcksstücken zu beschäftigen; ein Thema, das bei INDECT ebenfalls wichtigen Rang hat.

4.4 INDECT im Kontext der Horizon 2020-Forschung

In Horizon 2020, dem 8. Forschungsrahmenprogramm der EU, das eine Laufzeit von 2013 bis 2020 aufweist, können weitere Forschungsprojekte durchgeführt werden, die sich – in ähnlicher Ausrichtung wie INDECT selber – der Kriminalitäts- und Terrorbekämpfung widmen. Dafür reserviert sind knapp EUR 57 Millionen an Forschungsgeldern.[52]

[48] Webseite "FP7 Security Research" auf der CORDIS-Plattform der EU.
Online: http://cordis.europa.eu/fp7/security/projects_en.html (Abruf: 13.5.2014)

[49] Informationsdienst "Community Research and Development Information Service" der EU zur Gemeinschaftsforschung.

[50] Auf eine nähere Betrachtung der konkreten Forschungsergebnisse muss im Rahmen dieser Ausarbeitung hingegen verzichtet werden.

[51] ADABTS-Seite auf der CORDIS-Plattform der EU. Online: http://cordis.europa.eu/projects/218197 (Abruf: 12.5.2014)

[52] Vgl. Horizon 2020-Webseite der Europäischen Kommission zum Bereich "Fight against crime and Terrorism".
Online:
http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-fct-2014.html (Abruf: 11.5.2014)

Noch ist keine abschliessende Liste der in diesem Bereich (bald) laufenden Projekte verfügbar, um abzuschätzen, ob Synergien zunehmen und Anknüpfungspunkte sichtbar werden, welche die INDECT-Systemidee weiter ausbauen.

Die folgende Auswahl von zwei der vorgesehen Topics in diesem Bereich aber machen deutlich, dass die Forschung an Überwachungsmöglichkeiten weiter betrieben wird – Systemintegration kann folglich konstruiert werden:

- Topic "Law enforcement capabilities topic 1: Develop novel monitoring systems and miniaturised sensors that improve Law Enforcement Agencies' evidence-gathering abilities" mit der Aufgabe den Strafverfolgungsbehörden[53] weitere Werkzeuge zur Überwachung zur Verfügung zu stellen.[54]
- Topic "Urban security topic 3: Minimum intrusion tools for de-escalation during mass gatherings improving citizens' protection" spricht von verbesserter und gezielter Sensorik im Rahmen von "crowd management instruments"[55], die es für die Polizei zu entwickeln gilt.[56]

5 Zusammenfassung und Schlussbetrachtungen

Diese Arbeit hat sich mit dem INDECT-Forschungsprojekt, das im Rahmen des 7. Forschungsprogramm der Europäischen Union von 2009-2013 durchgeführt wurde und das dabei mit rund EUR 15 Millionen gefördert wurde. Angesichts weiterer Projekte, die z. T. überschneidende oder anknüpfende Gegenstände zum Thema hatten oder im Rahmen des Horizon 2020-Forschungsprogramms noch haben werden, sind die skizzierten Möglichkeiten der umfassenden Überwachung der europäischen Gesellschaften immens.

[53] In der englischen Projektausschreibung wird von "LEA" für Law Enforcement Agencie(s) gesprochen.

[54] Vgl. Seite zum Topic FCT-05-2014 auf der Horizon 2020-Webseite der Europäischen Kommission. Online: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1105-fct-05-2014.html#tab1 (Abruf: 11.5.2014)

[55] Wortwörtlich: Instrumente zur Verwaltung von Menschenansammlungen/-massen

[56] Vgl. Seite zum Topic FCT-12-2014 auf der Horizon 2020-Webseite der Europäischen Kommission. Online: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/1110-fct-12-2014.html#tab1 (Abruf: 11.5.2014)

Das INDECT-System erlaubt in einer praktischen Umsetzung ein Überwachungssystem wahr werden zu lassen, das Europa einem präventiven Sicherheitsstaat unterstellt. INDECT ist weit mehr als nur die Möglichkeit, die digitale Sphäre umfassend zu durchleuchten: Durch die europaweit vernetzte Videoüberwachung mit automatischer "Gefahrenerkennung" und den Einsatz von Drohnen zur mobilen Überwachung von Bereichen ohne bisherige Beobachtung des öffentlichen Raums droht ein praktischer INDECT-Einsatz konformes gesellschaftliches Verhalten zu erzwingen.

Politisch ist der Einsatz eines INDECT-Systems in Europa höchst fragwürdig: Tangiert sind praktisch alle Grundrechte, namentlich etwa das Recht auf Privatsphäre, der Komunikations- und Versammlungsfreiheit. INDECT hebelt zudem die Unschuldsvermutung auf, denn vorderhändig sind alle verdächtigt, kriminelle Handlungen auszuführen. INDECT soll diese verhindern, bevor sie geschehen.

Es ist nicht realistisch, den Personen nahe zu legen, sich sowohl in virtuellen (privaten) als auch physischen (öffentlichen) Räumen stärker zurückzuziehen, ohne einzuräumen, dass das INDECT-System den Lebensalltag der Menschen unter seiner Einflusssphäre massiv einschränkt. Denn: Nur durch eine massiv geringere Sichtbarkeit in allen Sphären, in denen INDECT "präsent" ist, könnten sich Einzelpersonen der kontinuierlichen Datenpreisgabe entziehen. Der Preis für die so gewonnene Privatsphäre aber ginge in bedeutendem Masse auf Kosten der Kommunikations- als auch Bewegungsfreiheit. Leiden dürfte insgesamt die Lebensqualität.

Literatur-/Bildverzeichnisse

Literatur

[1] Ciarkowski, A. et al (2012): *Specification of Requirements for Security and Confidentiality of the System (D8.1)*. Publikation im Rahmen des 7. EU-Forschungsrahmenprogramms FP7. Online: http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_D8.1_v20091223.pdf/at_download/file (Abruf: 12.5.2014)

[2] Derkacz, J. (2010): *D0.6 INDECT – Ethical Issues*. Publikation im Rahmen des 7. EU-Forschungsrahmenprogramms FP7. Online: http://www.indect-project.eu/files/deliverables/public/d0.6-indect-2013-ethical-issues-2013-2010/at_download/file (Abruf: 8.5.2014)

[3] Deleuze, G. (1993): *Postskriptum über die Kontrollgesellschaften*. In: Deleuze, G. (1972-1990): Unterhandlungen. 254-262. Frankfurt am Main: Suhrkamp. Online: https://www.nadir.org/nadir/archiv/netzkritik/postskriptum.html (Abruf: 14.5.2014)

[4] Hempel, L. (2008): *Die geschlossene Welt. Zur Politik der Überwachung am Beispiel von Videoüberwachung*. In: Gaycken, S. & Kurz, C. (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien: 79-100. Bielefeld: transcript Verlag.

[5] Giddens, A. (2009): *Sociology*. 6th edition. Cambridge/Malden: Polity Press.

[6] Klapaftis, I. et al. (2009): *XML Data Corpus: Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat. WP4*. D.4.1. Publikation im Rahmen des 7. EU-Forschungsrahmenprogramms FP7. Online: http://www.indect-project.eu/files/deliverables/public/INDECT_Deliverable_4.1_v20090630a.pdf/at_download/file (Abruf: 10.5.2014)

[7] Klapaftis, I. (2010): *D4.3. Report on current state-of-the-art of machine learning methods for behavioural profiling*. Publikation im Rahmen des 7. EU-Forschungsrahmenprogramms FP7. Online: http://www.indect-project.eu/files/deliverables/public/D4.3.pdf/view (Abruf: 10.5.2014)

[8] Tremmel, M. (2010): *Die Vorratsdatenspeicherung und der Panoptismus. Anwendbarkeit und Erkenntnisse aus der Analyse der Vorratsdatenspeicherung mit Foucaults Machttheorie*. Online: https://moritztremmel.de/files/2011/05/Moritz_Tremmel_-_Die_Vorratsdatenspeicherung_und_der_Panoptismus_-_2010-CC_BY.pdf (Abruf: 14.5.2014)

[9] Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (2014): *Botschaft zum Nachrichtendienstgesetz NDG*. Online: http://www.vbs.admin.ch/internet/vbs/de/home/themen/ndb/dokumente.parsys.44418.downloadList.23631.DownloadFile.tmp/ndgbotschaftd.pdf (Abruf: 4.5.2014)

Bilder