INDECT – ein weiterer Schritt zum Orwellschen Überwachungsstaat?
von Sylvia Johnigk und Kai Nothdurft, Februar 2010,
Erstveröffentlichung in FIfF-Kommunikation 2/2010

Das EU-Projekt INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment) wurde Anfang 2009 mit einem Budget von 14,86 Millionen Euro bei einer Laufzeit von 5 Jahren gestartet. Es ist Teil eines Gesamtrahmens der EU für die Erforschung von Sicherheitsthemen mit einem Budget von 1,4 Milliarden.

Inhalte und Zielsetzung und Beteiligte

IDECT hat die Entwicklung einer ganzen Palette von neuen Werkzeugen zum Ziel, die die polizeiliche Überwachung effektivieren sollen. Die Projektziele auf der offiziellen Homepage wirken im englischen Original etwas gestelzt formuliert und lauten übersetzt:[1]

- Entwicklung einer Plattform für die Erfassung und den Austausch von Betriebsdaten, Sammlung von Multimedia Inhalten, intelligente Verarbeitung von allen Informationen und automatisches Entdecken von Bedrohungen und Erkennung von abnormalem Verhalten oder Gewalt

- Entwicklung eines Prototyps für ein integriertes, netzwerkzentriertes System, das die operative Polizeiarbeit unterstützt, zur Verfügung stellen von Techniken und Werkzeugen zur Überwachung verschiedener mobiler Objekte

- Entwicklung eines Suchmaschinentypus, der die direkte Suche nach mit Wassserzeichen markierten Bildern und Videos verbindet mit der Speicherung von Metadaten in Form von digitalen Wasserzeichen.

Als Ergebnisse werden dort erwartet:

- Realisierung eines Prototyps für das Beobachtungs- und Überwachungssystem in verschiedenen Ballungsräumen und Demonstration des Prototypen mit 15 Knoten

- Implementierung eines verteilten Systems, das in der Lage sein soll, bei Bedarf Daten zu sammeln, zu speichern, effektiv zur Verfügung zu stellen und zu verarbeiten

- Konstruktion einer „Familie von Prototypen“ von Geräten zur Nachverfolgung mobiler Objekte

- Konstruktion einer Suchmaschine für die schnelle Entdeckung von Personen und Dokumenten basierend auf Wasserzeichentechnologie und für Nutzung umfassender Erforschung (Tiefenanalyse), die Wasserzeichen für semantische Suche nutzt.

- Konstruktion von Agenten zur fortlaufenden und automatischen Beobachtung von öffentlichen Ressourcen wie: Webseiten, Diskussionsforen, UseNet, File Server, p2p Netzwerken ebenso wie individueller Computersysteme.[2]

---

1 http://www.indect-project.eu

2 Bemerkenswert ist, dass hier Privatrechner als öffentliche Ressourcen betrachtet werden. Nachdem der Bundestrojaner politisch gescheitert ist, kommt jetzt der EU-Trojaner.

- Erarbeitung eines Internet-basierten Systems, das sowohl aktiv als auch passiv Informationen sammelt

Zusammengefasst sollen hier Technologien entwickelt werden, die die polizeiliche Überwachung effektiver als bisher gestalten, indem schon vorhandene Systeme und Informationsquellen vernetzt und aneinander gekoppelt werden. Die Auswertung der erhobenen Daten soll durch das Erkennen von abnormalem Verhalten und Gewaltbedrohungen automatisiert und Reaktionen darauf beschleunigt werden.

An dem Projekt beteiligen sich mehrere europäische Universitäten, Privatfirmen mit dem Fokus Überwachungstechnologien und die Polizei von Polen und Nordirland. Aus Deutschland sind die Uni Wuppertal, InnoTec DATA und PSI Transcom beteiligt.

INDECT im Kontext der europäischen Sicherheitspolitik

Das INDECT Projekt ist nur eines von vielen Puzzleteilen, das zu einer neuen europäischen Sicherheitspolitik gehört, die in einem all um fassenden Überwachungsstaat beziehungsweise in einem totalitären Staat mit einer Null-Toleranz-Politik münden kann. Insgesamt umfasst der europäische Forschungsrahmen zur Sicherheitspolitik 45 Projekte.

Das neue, geänderte EUROPOL Gesetz trat am 1.1.2010 in Kraft. Es wurde, genau wie das SWIFT Abkommen, im letzten Augenblick kurz vor Inkrafttreten des Lissabon Vertrages durch gewunken. Damit wurden die neuen Mitspracherechte des EU-Parlaments umgangen. Mit dieser Gesetzesänderung werden nicht nur Kompetenzen und Möglichkeiten der Zusammenarbeit der europäischen Polizeien auf Kosten des europäischen Datenschutzes erweitert werden. Jörg Leichtfried, SPÖ Abgeordneter im EU Parlament, kritisierte, „die Formulierungen seien "so schwammig", dass sie die Weitergabe polizeilicher Informationen an nicht genauer definierte "Körperschaften" in Nicht-EU-Staaten erlaubten.“ [3] Das EU Parlament hat dies scharf kritisiert und gefodert die Umsetzung auszusetzen. [4] Strittig ist u.a., inwieweit EUROPOL den im Lissabon vereinbarten Grundsatz der Offenheit gewährleisten, und wie EUROPOL durch das Europäische Parlament kontrolliert werden kann.
Das EUROPOL Gesetzt und das Projekt INDECT ergänzen sich perfekt. Indect liefert die Technik, das Europol Gesetz den rechtlichen Rahmen für eine umfassende Überwachung der EU Bürger durch nahezu beliebige staatliche Institutionen auch außerhalb der EU.

Datenschutz, Ethik und Selbstkontrolle

Bezogen auf die Ziele des Projekts sagte Thilo Weichert in der TAZ vom 24.12.2009: „Das Projekt steht konzeptionell mit europäischem und deutschem Datenschutz- und Verfassungsrecht im Widerspruch.“ Er kritisiert, dass die Datenerhebung heimlich sei und nicht nur Personen überwacht würden, von denen Gefahr ausgehe. Außerdem fehle die Zweckbindung der erhobenen Daten.[5]

Im Gegenzug brüstet sich das Projekt selbst gerne damit, eine eigene Ethikkommission zu besitzen. Die für EU-Projekte vorgesehene interne Ethikkommission widmet sich dem Datenschutz. Sie betrachtet das Thema allerdings nur bezüglich.der Projektdurchführung, also dem Schutz der bei dem Projekttestbetrieb angesammelten Daten, nicht aber in Bezug auf die gesamtgesellschaftliche

3 http://diepresse.com/home/politik/eu/523901/index.do
4 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2009-0068+0+DOC+XML+V0//DE
5 http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/die-moderne-verbrecherjagd/

Dimension, wenn das System einmal eingeführt ist. Eine Technikfolgenabschätzung ist also noch nicht einmal vorgesehen. Das ist wenig verwunderlich, wie auch Weichert feststellte, denn „das INDECT-Projekt selbst beschäftigt bislang keine einzige Institution, die sich mit Bürgerrechten auskennt.“[6] Den Vorsitz der Ethik-Kommission führt Assistant Chief Constable Drew Harris vom Police Service Northern Ireland. In dieser Funktion ist er u.a. zuständig für organisierte Kriminalität, das Hauptermittlungsteam, Geheimdienste und Sondereinsatzkommandos. Zusätzlich ist er Vorsitzender des Ressorts "Hate Crimes" in der britischen Association of Chief Police Officers (ACPO).
Die vorgesehene Kontrollinstanz sitzt praktischerweise gleich im selben Haus. Es handelt sich um Drews Assistentin Zulema Rosborough, die dort als Detective Chief Inspector beschäftigt ist.
Ein Großteil der ethischen Leitlinien besteht in der Zusage, geltende Datenschutz- und Menschenrechtsvorschriften der EU und der am Projekt beteiligten Länder einzuhalten. Diese Selbstverständlichkeit als Ziel zu nennen, grenzt an Frechheit. Bezeichnenderweise wird an dieser Stelle der Verbrechensbekämpfung höhere Priorität als den Persönlichkeitsrechten des einzelnen Bürgers eingeräumt.
Alle im Projekt erarbeiteten Dokumente müssen dieser so besetzten Ethikkommission vorgelegt werden, die dadurch zensierend wirken kann. So wird die Freiheit der Forschung insbesondere für die beteiligten Hochschulen stark eingeschränkt. Ein kritischer Diskurs von Methodik und Ergebnissen in der Öffentlichkeit wird behindert.

Kritikpunkte

Dem kritischen Informatiker sträuben sich die Nackenhaare bei der Vorstellung, dass ein Überwachungssystem automatisch erkennen soll, welche seiner sensoralen Wahrnehmungen auf eine Gewalt Bedrohung oder ein abnormes Verhalten schließen lässt. Für die Modellbildung wurden 199 polnische Polizisten befragt, was sie für verdächtig halten. Dabei wurde zum Beispiel das gleichzeitige Zuströmen von mehreren Personen auf einen Punkt, etwa bei einem Flashmob und ebenso die gegenteilige Bewegung als verdächtig eingestuft. Solche Bewegungen können durch Auswertung von RFID Chips analysiert werden, die zunehmend in Personaldokumenten mitgeführt werden oder sogar versteckt in Kleidungsstücken oder Verpackungen verborgen sind. Gleichzeitig sollen mit INDECT auch an strategisch interessanten Orten (Bahnhöfe, Flughäfen, Plätze, Veranstaltungsgebäude) RFID-Reader installiert werden. Weitere Bewegungsprofile können aus mobilen Telekommunikationsgeräten (GSM Mobiltelefon, Smartphones) und GPS Geräten gewonnen werden, die ebenfalls personenbeziehbar sind und üblicherweise ständig mitgeführt werden. Wenn zukünftige Überwachungssysteme eine Person entdecken, die so etwas nicht dabei hat, macht diese sich erst recht verdächtig.

Ein weiteres Ergebnis der Befragung war, dass das Herumlungern in einem Park als normal, die gleiche Aktivität an einem Bahnhof oder vor einem Gebäude aber als verdächtig benannt wurde. Wie könnte die automatische Erkennung im zweiten Beispiel aussehen? Wenn ein mittels Mustererkennung als Person eingestuftes Objekt an einem Bahnhof von einer Überwachungskamera erfasst wird und seine Position für einen definierten Zeitraum nicht wesentlich verändert, wird es als verdächtig eingestuft. Die Kamera zoomt und fokussiert darauf, zeichnet in höherer Auflösung (HD-Qualität) auf und löst einen Alarm aus.

Die Modellbildung anhand der Interviews ist schon im Ansatz problematisch. Es wird erfragt, was verdächtig erscheint, nicht untersucht, was tatsächlich zu Straftaten führt(e). Damit basiert die Modellierung und die darauf aufbauende Implementierung automatischer Erkennung auf Vorurteilen. Die Interviews können zu einer im Entscheidungsmodell gründenden Diskriminierung führen. Bei der gewählten, sehr homogenen und nicht besonders großen Gruppe von Befragten

6 http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/die-moderne-verbrecherjagd/

können sich in den Aussagen sehr schnell Vorurteile manifestieren, etwa wenn ein bestimmtes Aussehen (männlich, jung, langhaarig, dunkelhäutig, …) in die Definitionen Eingang finden. Mindestens müssten die Modelle öffentlich hinterfragt und bei diskriminierenden Aussagen auch korrigiert werden können, wenn man sich überhaupt auf die Hybris einließe, so etwas schwammiges wie abnormes Verhalten oder Gewaltbedrohung halbwegs sinnvoll modellieren zu können. Eine solche notwendige Offenheit und Korrigierbarkeit der hinterlegten Modelle und Regeln widerspricht aber ihrem Einsatzzweck, weil sich potentielle Täter in ihrem Verhalten anpassen und so das System gezielt unterlaufen könnten. Diskriminierende Effekte verstärken sich als selbsterfüllende Prophezeiung, wenn bestimmte, von dem System wiederholt als verdächtig eingestufte Verhaltensweisen zu einer höheren Kontrolldichte für eine bestimmte Person oder Gruppe führen. Zum einen ist die Wahrscheinlichkeit der Entdeckung von Fehlverhalten bei einer oft kontrollierten Gruppe höher als bei einer weniger oft kontrollierten bei gleichem Anteil an Fehlverhalten in beiden Gruppen. Zum anderen kann die höhere Kontrolldichte und das Gefühl übermäßig drangsaliert oder belästigt zu werden, bei Betroffenen Gegenreaktionen auslösen, die wiederum zu “abnormen” Verhalten führen und so die modellierten Vorurteile bestätigen und bei dynamischer Anpassung der Regeln sogar verstärken. Je genauer eine Person ins Visier genommen wird, desto leichter fällt es zudem, irgendetwas zu finden, dass verdachtserhärtend, bestätigend oder verstärkend wirkt, – etwas bleibt hängen.
Diskriminierungseffekte durch automatisierte Entscheidung sind aus den Scoring Verfahren der SchuFa bekannt, wenn z.B. weiche Faktoren wie eine bestimmte Wohnlage dazu führen, dass es einem Wohnungssuchenden schwer gemacht wird, an Kredite oder Wohnungen in besseren Gegenden zu kommen, obwohl er selber noch nie mit Zahlungen im Rückstand war.

Hier zeigt sich einmal mehr das negative Menschenbild, dass dem ganzen präventiven Denkansatz zugrunde liegt, weil es die Menschen als potentielle Täter betrachtet und die Entscheidungen, die mindestens unangenehme Kontrollen auslösen können, in die Hand einer Maschine gibt. Die automatisierte Entscheidung mit den ausgelösten Folgeaktivitäten führt zu einer Vorverlegung des Zeitpunkts staatlichen Eingreifens in die Handlungen seiner Bürger. Ähnlich wie bei der Vorratsdatenspeicherung wird auch hier die Unschuldsvermutung pervertiert. Herumlungern ist kein Straftatbestand, nicht einmal eine Ordnungswidrigkeit. Auch die Teilnahme an einem Flashmob ist aufgrund des Versammlungsrechts in der Regel legal. Der Ansatz ist die konsequente Fortführung der von Kanzlerin Merkel proklamierten Null Tolleranz Politik gegenüber Fehlverhalten.[7]

So zu hören in einem Video aus dem Jahr 2006 in Berlin Kranoldplatz CDU Wahlkampf Redenerin Angela Merkel: „Die CDU hat seit Jahr und Tag dafür plädiert, dass an großen Plätzen genau solche Videoüberwachung eingesetzt wird. Wenn es die CDU nicht gegeben hätte, dann würden wir heute noch ´ne lange Diskussion mit SPD, Grünen und andern führen darüber, ob das nun notwendig ist oder nicht. Das sind aber Dinge, über die darf man nicht diskutieren, die muss man einfach machen.
[...]

Man darf nicht sagen, ach, das ist doch nicht so schlimm. Hier ‘n bisschen was weggeschmissen und dort einen angerempelt, hier mal auf’m Bürgersteig gefahren und dort mal in der dritten Reihe geparkt, immer so hinter dem Motto “Is alles nicht so schlimm”. „Ist alles nicht nach dem Gesetz, und wer einmal Gesetzesübertretungen duldet, der kann anschließend nicht mehr begründen, warum’s irgendwann schlimm wird und irgendwann nicht so schlimm ist. Und deshalb: Null Toleranz bei Innerer Sicherheit, meine Damen und Herren.”[8]

Neben diesen eher unbeabsichtigten schädlichen Nebenwirkungen könnten die im INDECT Projekt

7 Siehe Kasten
8 “Auf Nummer sicher“, Fernsehspiel, das am 15. Mai 2007 im ZDF lief bzw. den Ausschnitt findet man auch unter http://www.youtube.com/watch?v=wcVRlzP6SQA

entwickelten Systeme aber auch aktiv missbraucht werden, etwa für Stalking oder Voyeurismus, ein Problem, das schon aus der normalen Videoüberwachung bekannt ist. Es würde durch ein Manipulieren der Regeln für die automatisierte Erkennung aber nochmals verstärkt werden. Wäre es nicht eine Versuchung, wenn „abnormal“[9] tief ausgeschnittene Dekolletés dem geneigten Betrachter kredenzt werden könnten?

Auch die geplante Weiterentwicklung der Watermarking-Technologie birgt erhebliches Potential, die Überwachung zu perfektionieren. Es ist denkbar, mit Wasserzeichen nicht nur die Integrität der übertragenen Daten zu sichern, sondern den Herkunftsnachweis auch gezielt zu nutzen, um nachzuverfolgen, mit welchem Gerät an welchen Orten z.B. bestimmte Bilder aufgenommen wurden. Dies wurde bereits bei Farblaserkopierern praktiziert, indem diese ein Wassserzeichen mit der registrierten Seriennummer des Kopierers in das Bild einfügten und diente damals hauptsächlich dazu, Kopien von Banknoten zurückverfolgen zu können. Eine Erinnerung an die in der DDR praktizierte Registrierung und Rückverfolgbarkeit von Schreibmaschinentexten durch die Stasi drängt sich hier geradezu auf. Die generierbaren Bewegungs- und Herkunftsdaten würden wohl auch umgehend Begehrlichkeiten der Medienverwertungsindustrie zum Aufspüren von Raubkopien wecken. Umgekehrt könnte das Watermarking Anonymität etwa bei Wistleblowing oder investigativer journalistischer Arbeit gefährden und ungewollt deren Quellen offenbaren.

Die Nutzung der im INDECT Projekt entwickelten Technologien erscheint schon unter den aktuellen gesellschaftlichen Rahmenbedingungen in der EU als problematisch. Leider kann nur mit großem Aufwand verhindert werden, dass sie auch in Gesellschaften gelangt, die in Bezug auf totalitäre Überwachung noch wesentlich weiter fortgeschritten sind. Selbst der Versuch, die Weiterverbreitung von Nuklearwaffen zu verhindern, ist in Teilen gescheitert. Die beteiligten Privatfirmen dürften kaum ein Interesse an strikten Exportbeschränkungen haben. Wie skupellos in der Vergangenheit Überwachungstechnologie in totalitäre Regime exportiert wurde, zeigt das Beispiel von Nokia/Siemens, die Abhörvorrichtungen für Telekommunikation u.a. in den Iran exportierten.[10] Es ist schon bemerkenswert, dass ausgerechnet in der demokratischen EU Projekte gefördert werden, deren Ergebnisse der Unterdrückung und Stabilisierung von Diktaturen dienen können.

Was können wir tun?

Das INDECT Projekt findet bisher nur ein gemäßigtes Interesse in den breiten Medien und der Öffentlichkeit, obwohl hier Steuergelder für fragwürdige Entwicklung von problematischer Überwachungstechnologie ver(sch)wendet werden. Auf der FIfF Jahrestagung wurde ein Arbeitskreis ins Leben gerufen, der sich des Themas annimmt. Weitere Interessierte sind herzlich eingeladen. Unser Ziel ist es eine breitere Öffentlichkeit für das Thema zu sensibilisieren und die öffentliche Kritik zu verstärken. In einem ersten Schritt könnte ein Flyer mit komprimierten Informationen erarbeitet werden. Als Arbeitsplattform soll das neue FIfF-Mitglieder-WIKI dienen.[11] Wir können dort Informationsmaterial erarbeiten und von Dritten sammeln und verlinken. Wir wollen uns mit anderen Kritikern vernetzen. Bekannt sind uns bisher Aktivitäten vom AStA der Universität Wuppertal, von der Piraten-Partei, Stephen Booth und Personen aus dem Umfeld des CCC. Eine Stellungnahme des EU Datenschutzbeauftragten sollte ebenso eingeholt wie die Beschwerdemöglichkeiten bei der Ethikkommission der EU genutzt werden. Letztlich bleibt zu hoffen, dass sich die technisch sehr ambitionierten Ziele nicht in der geplanten Form realisieren lassen. INDECT wäre ja nicht das erste Mammutprojekt, das an allzu ehrgeizigen Wunschvorstellungen scheitert. Wir verurteilen aber schon den Versuch, diese

9 Vergleiche vorne bei den Projektzielen, wonach Abnormalität automatisch erfasst werden soll.
10 Vergl. Impressionen von 26C3, Vortrag von Andy Müller-Maguhn FIfF Kommunikation 1/2010
11 Wer Interesse hat, im AK mitzuarbeiten und Zugang zum WIKI benötigt, wendet sich bitte direkt an die Autoren.

Überwachungstechnologien zu verwirklichen und dafür Ressourcen zu verschwenden, die an anderer Stelle sinnvoller eingesetzt werden könnten zu verurteilen.

Die Technologien, die im INDECT Projekt entwickelt werden sollen, sind nicht grundsätzlich neu. Dadurch, dass sie bisher isoliert arbeitende Systeme vernetzen und zusammenführen wollen und bisher wegen des Aufwands nur vereinzelt mögliche Überwachungsmaßnahmen effizienter gestalten, entsteht eine neue Qualität von Überwachung, die uns dem Überwachungsstaat wieder einen erheblichen Schritt näher bringen kann. „Keiner hat vor einen Überwachungsstaat zu errichten“ sagte Bosbach 28.04.2007[12] in einer Gesprächsrunde auf Phoenix. Es ist heute Vorsitzender des Bundestags-Innenausschusses.

Links und weiterführende Infos

INDECT-Linkliste (noch unkommentiert)
http://www.indect-project.eu/
http://www.heise.de/tp/r4/artikel/31/31802/1.html
http://www.tob1as.de/lira/?p=640&cpage=1#quelle1
http://www.kt.agh.edu.pl/~romaniak/indect/Expectations%20of%20end%20users.pdf
http://www.src09.se/upload/Presentations/Day_1/Sessions-1100-1245/Session-1-Hall-B/Dziech.pdf
http://www.telegraph.co.uk/news/newstopics/politics/defence/6261756/MoD-how-to-stop-leaks-document-is-leaked.html
http://www.kt.agh.edu.pl/~romaniak/indect/Short%20introduction%20of%20partners%20.pdf
http://www.ppbw.pl/en/projekty_badawcze/p_dziech.html
http://futurezone.orf.at/stories/1631510/
http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/die-moderne-verbrecherjagd/
http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung?page=1
http://telemat.de/ndect-der-traum-der-eu-vom-polizeistaat-die-zeit/
http://www.heise.de/tp/r4/artikel/31/31802/1.html
http://www.heise.de/tp/r4/artikel/31/31425/1.html

12 http://www.youtube.com/watch?v=Smhe7ed-ftI