Stadttheater Bielefeld 2019 – Foto: Jens Reimerdes, CC BY-SA 4.0

Stefan Hügel

BigBrotherAwards 2019

Auch im letzten Jahr gab es wieder reichlich Ereignisse, die einen BigBrotherAward verdient hätten. Wie immer berichten wir von der Preisverleihung: Wer hat es in den erlesenen Kreis der PreisträgerInnen geschafft?

Wir fassen in diesem einleitenden Beitrag des Schwerpunkts zum BigBrotherAward 2019[1] zunächst die Laudationes für die PreisträgerInnen kurz zusammen. Danach drucken wir drei Laudationes im Wortlaut ab. Die Verleihung fand am 8. Juni 2019 im Stadttheater Bielefeld statt. Moderiert wurde sie von der Journalistin Golineh Atai.

Moderatorin Golineh Atai – Foto: Markus Benter, CC BY-SA 4.0

Kategorie *Behörden & Verwaltung*

Der BigBrotherAward in der Kategorie *Behörden & Verwaltung* ging an den **Innenminister des Landes Hessen, Peter Beuth (CDU)**,

1. *für die bundesweit erstmalige Anschaffung einer Analysesoftware der CIA-nahen Firma Palantir,*

2. *dafür, dass diese umstrittene US-Firma über Einsatz und Betrieb der Software Zugang zum Datennetz der hessischen Polizei erhält, und*

3. *dafür, dass mit dieser Analysesoftware Massendaten aus polizeieigenen und externen Quellen in Sekundenschnelle automatisiert verknüpft, analysiert und ausgewertet werden können – mit fatalen Auswirkungen auf Grundrechte, Datenschutz und Rechtsstaat.*

Laudator Rolf Gössner erinnert zunächst daran, dass die schwarz-grüne Hessische Landesregierung bereits im Vorjahr mit einem BigBrotherAward ausgezeichnet worden war, für die Verschärfung des Hessischen Verfassungsschutz- und Polizeigesetzes. Dieses ist inzwischen in Kraft, es gibt Verfassungsbeschwerden dagegen.

Auf Basis dieses Gesetzes wurde nun die US-amerikanische Firma *Palantir* beauftragt, ihre Analysesoftware *Gotham* bei der hessischen Polizei in Betrieb zu nehmen, mit spezifischen Anpassungen, unter der Bezeichnung *Hessen-Data*. Dies wird durch §25 des neuen Hessischen Polizeigesetzes ermöglicht, der Datenanalysen zur vorbeugenden Bekämpfung von über 40 Straftaten erlaubt.

Das US-amerikanische Unternehmen Palantir wurde 2004 gegründet, mit finanzieller Unterstützung der CIA. Diese Firma wurde nun damit beauftragt, die hessischen Polizeidatenbanken mit externen Datenbanken, z. B. Social-Media-Diensten zu verknüpfen und zu analysieren. Dabei ist nicht auszuschließen, dass auch vertrauliche Daten in die USA abfließen – dort unterliegt Palantir aber dem *Foreign Intelligence Surveillance Act* (FISA), nach dem Daten auf Anforderung an US-Geheimdienste übermittelt werden müssen.

Hessen-Data soll Datenanalysen liefern, durch die Bedrohungslagen leichter erkannt und terroristische „Gefährder" identifiziert werden können. Es geht also um Aufklärung im Vorfeld von Gefahren, wenn noch keine Straftat begangen wurde. Damit entwickelt sich Polizeiarbeit hin zu geheimdienstlicher Arbeit:

> *Hessen-Data ist ein Dammbruch für die polizeiliche IT-Arbeit: Bislang waren die Polizeidaten-Bestände der Strafverfolgung und Gefahrenabwehr nicht miteinander verknüpft, weil personenbezogene Daten aus datenschutzrechtlichen Gründen prinzipiell nur für den Zweck verwendet werden dürfen, für den sie erhoben wurden – also entweder für Strafverfolgung oderfür Gefahrenabwehr. Dieser Zweckbindungsgrundsatz wird mit Hessen-Data aufgehoben.*

Zusammenfassend schließt Rolf Gössner:

> *Die Analyseplattform Hessen-Data steht im Dauerkonflikt mit dem Recht auf informationelle Selbstbestimmung als Ausprägung des Allgemeinen Persönlichkeitsrechts (Artikel 2 Abs. 1 GG). Außerdem wird mit dem Einsatz der Palantir-Software eine wichtige Grundsäule des Datenschutzes buchstäblich niedergerissen: nämlich das Prinzip der Zweckbindung, wonach personenbezogene Daten grundsätzlich nur für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Und das Ganze auch noch weitgehend ohne wirksame Kontrolle und in einer unheiligen Allianz mit einem*

Hauptakteur des US-amerikanischen Militär- und Geheimdienstkomplexes.

Die vollständige Laudatio von Rolf Gössner ist ab Seite 39 nachzulesen.

Kategorie *Arbeitswelt*

In der Kategorie *Arbeitswelt* gibt es 2019 keinen BigBrother-Award. Peter Wedde erläuterte im Interview aber exemplarisch einige Möglichkeiten der Überwachung von MitarbeiterInnen durch ihre Arbeitgeber. Auch wenn viele Unternehmen den Datenschutz ernst nähmen – sei es aus Einsicht oder sei es wegen der zu erwartenden Strafen – gebe es häufig kleinere Fälle, die nicht an die Öffentlichkeit kommen, da das Interesse bei Journalisten an solch „unbedeutenden" Fällen gering ist. Er nannte einige Beispiele:

- Unzulässige Überprüfung der Daten von VertriebsmitarbeiterInnen mit Korrelation von Leistungsdaten mit der Gehaltsdatenbank und anschließender Kündigung „teurer" MitarbeiterInnen, wenn aus Sicht des Arbeitgebers die Leistung nicht ausreicht.

- Überwachung von externen Dienstleistern bei Banken, die mit kritischen Gelddaten zu tun haben, mit zwei Kameras (auf den Monitor und auf die Tastatur gerichtet). Bei MitarbeiterInnen der Bank kann der Betriebsrat durchsetzen, dass sie nicht mit Kameras überwacht werden; der Betriebsrat des externen Dienstleisters kann das nicht. Begründet wird die Überwachung mit Anforderungen der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), die jedoch auf Nachfrage dort nicht bestätigt werden – solche Überwachung sei schließlich nicht rechtens.

- Spracherkennungssoftware in Call Centern, die Anfragen z. B. darauf analysiert, ob eine AnruferIn lügt oder nicht, oder die die MitarbeiterInnen des Call Centers selbst aufgrund ihrer Stimme überwacht.

Peter Wedde weist auch auf die Bedeutung von Betriebsräten hin: Diese gebe es nur in etwa einem Drittel der Unternehmen. Wenn es Betriebsräte gibt, können sie regeln, was mit IT-Systemen passiert; sie können aber nicht verhindern, dass Arbeitgeber rechtswidrig handeln und haben dann nur schwache Eingriffsmöglichkeiten. Der Datenschutz unterliegt auch nicht der Mitbestimmung und Betriebsräte können Systeme letztlich nicht verhindern. Häufig verhielten sich betriebliche Datenschutzbeauftragte bei Datenschutzverstößen auch loyal zum Arbeitgeber und bieten wenig Unterstützung bei Beschwerden. Öffentliche Datenschutzbehörden sind unzureichend ausgestattet, um Eingaben zeitnah bearbeiten zu können.

Kategorie *Biotechnik*

Thilo Weichert hielt die Laudatio in der Kategorie *Biotechnik*. Dieser Preis ging an das Unternehmen **Ancestry.com**, weil es

das Interesse an Familienforschung dazu ausnutzt, Menschen zur Abgabe von Speichelproben zu veranlassen.

Früher wurde Familien- oder Ahnenforschung als Hobby betrieben, indem man beispielsweise Geburts-, Heirats- und Sterbeurkunden, Familienstammbäume oder Kirchenbücher auswertete. Heute bietet die DNA-Analyse die Möglichkeit, Verwandtschaftsbeziehungen nachvollziehen zu können. Man sendet eine Speichelprobe an ein Labor und erhält weitgehende Erkenntnisse über Verwandtschaft oder Herkunft. Vor allem in den USA gibt es mittlerweile viele Firmen, die solche Analysen anbieten.

Marktführer ist das Unternehmen *Ancestry.com*, gefolgt von der Google-Gründung *23andMe*. Ancestry.com ist inzwischen auch auf dem deutschen Markt präsent und hat eine Niederlassung in München eröffnet.

Das Angebot, so das Unternehmen, sei datenschutzkonform: „Sicherheit und Datenschutz genießen bei Ancestry oberste Priorität", so heißt es auf der Webseite. Jedoch, so Thilo Weichert:

Der Haken liegt – wie so oft – im Kleingedruckten und ist im Falle von Ancestry in einem dichten Gestrüpp von Bestimmungen verborgen: einer 16seitigen Datenschutzerklärung, elf Seiten Allgemeine Geschäftsbedingungen und siebeneinhalb Seiten Einwilligung in das Forschungsprojekt Ancestry Human Diversity Project.

Und weiter:

Mit dem Einsenden des Speichels erfolgt die Zustimmung zu den Datenschutzbestimmungen, wonach Ancestry selbst mit meinen Daten unbeschränkt über (Zitat) „Merkmale, persönliche Gesundheit und persönliches Wohlbefinden" Forschung durchführen kann. Wird dem Ancestry Human Diversity Project zugestimmt, so kommen „mitwirkende Partner" ins Spiel. Die Partner befinden sich (Zitat) „in den Vereinigten Staaten und anderen Ländern". Dabei kann es sich um „akademische Einrichtungen sowie Non-Profit-Organisationen, gewinnorientierte Unternehmen und Regierungsbehörden" handeln.

Doch damit nicht genug:

Menschen, die dort ihre DNA analysieren liessen, gerieten mitsamt ihren Familien ins Visier der Polizei, etwa weil sie mit dem so genannten „Golden State-Killer" auch nur entfernt verwandt sind. Um den Täter zu ermitteln, wurde die gesamte Verwandtschaft von den Ermittlern ausgeforscht. Kein Wort bei Ancestry.com über die potenzielle Strafverfolgung von biologischen Verwandten.

Als Fazit schließt Thilo Weichert:

Anbieter wie Ancestry missbrauchen das Interesse an Familienforschung, um einen Genom-Schatz für die kommerzielle Forschung anzuhäufen, denn das ist ihr eigentliches Geschäftsmodell. Die Datenschutzrechte der Probengeber und ihrer Verwandten müssen respektiert werden. Die deutschen Datenschutz- und Aufklärungspflichten werden aber von Ancestry aus Profitinteresse bewusst ignoriert. Wir sehen hier einen Trend: Nach der Ausbeutung von Internetdaten wird die Ausbeutung von Gendaten das nächste ganz große Ding. Ancestry ist der

Platzhirsch, der keine Datenschutz- oder Grundrechtsskrupel kennt.

Die vollständige Laudatio von Thilo Weichert ist ab Seite 41 nachzulesen.

Kategorie *Kommunikation*

Der BigBrotherAward in der Kategorie *Kommunikation* wurde an das Unternehmen **Precire Technologies GmbH** in Aachen verleihen. Es erhielt den Preis

für ihre wissenschaftlich zweifelhafte, wahrscheinlich rechtswidrige und gefährliche Sprachanalyse.

Laudatorin Rena Tangens erläuterte: Precire analysiert Sprechproben, um dadurch den Charakter eines Menschen herauszufinden, und damit auch z. B. seine oder ihre Eignung für eine ausgeschriebene Stelle. Dazu werde eine Probe von 15 Minuten benötigt, die nach Parametern wie Stimmhöhe, Lautstärke, Modulationsfähigkeit, Sprechtempo, Rhyhtmus analysiert wird. Das Ergebnis wird mit bereits vorhandenen Sprechproben verglichen und so auf den Charakter geschlossen. Der wissenschaftliche Wert dieser Analysen ist umstritten, doch ...

… Precire ... behauptet, ihr Verfahren sei wissenschaftlich abgesichert. Und winkt mit einer Buchveröffentlichung im wirtschaftswissenschaftlichen Springer Gabler Verlag. … Doch von seriöser Wissenschaft kann hier keine Rede sein, rügt Dr. Uwe Kanning, Professor für Wirtschaftspsychologie an der Hochschule Osnabrück in seiner Buchrezension. Er argumentiert, es existiere keine unabhängige Forschung zum Thema, der Algorithmus sei eine Blackbox und Geheimnis des Anbieters. Die vorhandenen Studien haben keine eigenen Zahlen erhoben, sondern sind Masterarbeiten, die sich auf die Daten stützen, die Precire ihnen zur Verfügung gestellt hat.

Fragen ergeben sich auch bei der Objektivität, sagt Rena Tangens. Ein Mitgründer von Precire erklärt: „Eine Maschine ist weniger fehleranfällig als ein Recruiter. Eine Maschine kann nur objektiv." Doch ...

… das ist eine äußerst naive Sicht der Dinge. Computer „verstehen" uns nicht. Das dürfen wir aber nicht mit Neutralität verwechseln. Computerprogramme sind auch voreingenommen, denn sie werden von Menschen programmiert. Menschen, die ihre eigenen Wertvorstellungen für selbstverständlich halten und in die Software mit einfließen lassen. Menschen mit bestimmten Fragestellungen, Zielen und Motiven. Und vor allem wird die Software mit einer ausgewählten Personengruppe als Referenz trainiert, die dann bestimmt, was als „normal", gut oder schlecht gilt.

Abschließend beschreibt Rena Tangens die Konsequenzen aus dieser Technologie:

Emotions- und Motivationserkennung per Sprachanalyse ist gefährlich, denn sie kann ohne unser Wissen irgendwo im Hintergrund passieren, wann immer wir sprechen. Diese Art der Sprachanalyse ist geradezu darauf angelegt, uns zu übervorteilen. So werden die einzelnen Menschen immer ohnmächtiger und unangreifbare Macht wandert immer mehr zu großen Konzernen, Versicherungen, Banken und staatlichen Stellen, die Zugriff auf unsere Daten und solche Technologie haben.

Die vollständige Laudatio von Rena Tangens ist ab Seite 43 nachzulesen.

Kategorie *Technik*

Laudator Frank Rosengart – Foto: Jens Reimerdes, CC BY-SA 4.0

Der BigBrotherAward in der Kategorie *Technik* wurde von Frank Rosengart angekündigt. Er geht an das **Technical Committee CYBER des Europäischen Instituts für Telekommunikationsnormen (ETSI)**,

für seine Bemühung, das Enterprise-Transport-Security-Protokoll (ETS) als Teil des neuen technischen Standards für die Verschlüsselung im Internet festzulegen und damit abgesicherte Verbindungen mit einer Sollbruchstelle auszustatten.

Internationale Gremien wie die Internet Engineering Task Force (IETF), gemeinsam mit Kryptographie-ExpertInnen, haben den Verschlüsselungsstandard Transport Layer Security (TLS) 1.3 entwickelt, die für die nächsten Jahre als sicher gelten soll. Doch …

… noch während der Beratungen über TLS 1.3 meldeten sich unter anderem Vertreter der Finanzindustrie zu Wort und wandten ein, dass sie strenge Compliance-Auflagen hätten, die es erforderlich machen, auch verschlüsselte Kommunikation, z. B. von Finanzberatern mit ihren Kunden, zu protokollieren – zum Beispiel um nachweisen zu können, dass sie gesetzestreu arbeiten. Sie behaupteten, sie bräuchten einen Nachschlüssel, um trotz Verschlüsselung für Dritte selbst alles lesen zu können. Dabei handelt es sich zwar um Daten, die sie auch auf ihren Servern im Klartext lesen könnten, aber für eine IT-Abteilung ist es einfacher, solche Daten an einem zentralen Punkt abzugreifen.

Das sehen offenbar auch Geheimdienste so, z. B. der GCHQ, der über Mitglieder des National Cyber Security Centre auch im

Technical Committee CYBER beim Europäischen Institut für Telekommunikationsnormen (ETSI) vertreten ist. ETSI entwickelte den Standard ETS (Enterprise-TLS) – mit Nachschlüssel, der beim Server-Betreiber hinterlegt ist:

> *Der Haken beim ETS-Standard ist aber, dass staatliche Stellen die Server-Betreiber verpflichten können, einen solchen festen Schlüssel einzustellen und diesen herauszurücken, um damit sämtliche Kommunikation mit Internetseiten im Nachhinein entschlüsseln zu können, zum Beispiel versendete Nachrichten.*

Und:

> *Eine besondere Gemeinheit ist außerdem, dass dieser „kaputte" Verschlüsselungsstandard für Browser und damit die NutzerInnen nicht vom „echten" zu unterscheiden ist. Es wird weiterhin das Schlüsselsymbol angezeigt; und der Browser hat technisch kaum eine Möglichkeit zu erkennen, ob ein fester Verbindungsschlüssel hinterlegt ist.*

Frank Rosengart schließt seine Laudatio:

> *Daher raten wir allen Entwicklern und technisch Verantwortlichen, einen großen Bogen um ETS zu machen und das deutlich sicherere TLS 1.3-Protokoll zu verwenden. Fatalerweise haben technisch nicht versierte Nutzerinnen und Nutzer kaum eine Möglichkeit, darauf Einfluss zu nehmen. Dieser zweite, unsichere ETS-Standard schafft eine verheerende Situation für die Online-Sicherheit.*

Kategorie *Verbraucherschutz*

Den letzten BigBrotherAward an diesem Abend, in der Kategorie *Verbraucherschutz*, kündigte padeluun an. Er ging an **Zeit Online …**

> *… dafür, dass sie*
>
> 1. *auf ihren Websites zeit.de und mycountrytalks.org zum Teil in großem Stil Werbetracker, wie auch das Facebook-Pixel einsetzen,*
>
> 2. *dafür, dass sie 2017 bei ihrem Projekt „Deutschland spricht" alle personenbeziehbaren Daten inklusiv der politischen Meinung auf den Rechnern von Google abgespeichert und verarbeitet haben und*
>
> 3. *dass sie sich für das Nachfolgeprojekt „My Country Talks" nicht nur von dem nimmersatten Werbeunternehmen mit Weltmachtsanspruch Google bei ihrem Projekt sponsern lassen, sondern dass sie zusätzlich Trackingtools eingebunden haben, mit denen Informationen an Dritte weiter gegeben werden können.*

Zeit Online hat im Jahr 2017 das Projekt *Deutschland spricht* durchgeführt, in dem Menschen unterschiedlicher Meinung ins Gespräch kommen sollten. Dieses Projekt wurde, so Laudator padeluun, zu Recht mit dem Grimme-Preis ausgezeichnet. Er kritisiert aber, dass die Daten der Teilnehmenden mitsamt ihren politischen Meinungen mit den Cloud-Tools der Google-Office-Suite verarbeitet und gespeichert wurden. Diese Tools würden auch sonst für große Teile der vernetzten Redaktionsarbeit genutzt. Den Informationen im Netz zufolge werden die Clouddienste anscheinend in Mountain View, Kalifornien von der Google LLC betrieben.

Der Verweis auf entsprechende Verträge und das EU-US-Privacy-Shield reiche dabei nicht aus, denn

> *Privacy Shield ist Augenwischerei. Das kann ich in 40 Treffern auf ZEIT ONLINE nachlesen. In 160 weiteren Treffen lese ich auf den Webseiten von ZEIT ONLINE, dass es da FISA gibt. Das heißt* Foreign Intelligence Surveillance Act *(auf deutsch: Gesetz zur Überwachung in der Auslandsaufklärung). Demnach dürfen die US-Geheimdienste bei allen US-Firmen ungehindert auf die Daten von Nicht-US-Bürgern zugreifen, wann immer sie wollen – egal, wo der Server steht. Und wie wir durch Edward Snowden gelernt haben, hatten die US-amerikanischen Behörden eine Standleitung zu Google.*

Außerdem …

> *… werden die Webseiten von Zeit Online über ein sogenanntes Content Delivery Network namens Fastly ausgeliefert. Die von mir getesteten IP-Nummern weisen nach Paris, aber Fastly ist eine US-amerikanische Firma, die in San Francisco, Kalifornien, angesiedelt ist. Und wie gesagt: FISA – der Foreign Intelligence Surveillance Act – gilt auch dann, wenn die Server US-amerikanischer Firmen in Europa stehen.*

Inzwischen gebe es eine neue Software, die mehreren Ländern genutzt wird. Diese ist nun nicht mehr bei Google gehostet, sondern in der Amazon Cloud.

„Das tun doch alle", sei häufig die Erklärung, so padeluun. Doch:

> *„Das tun doch alle", ist sicherlich kein guter Satz, um zu erklären, warum man Ethik und Moral außer acht lässt. Und wir kennen uns mit dieser Herausforderung durchaus aus: Auch wir Idealisten müssen Geld einnehmen, damit wir das ganze Jahr arbeiten und auch, um zum Beispiel die BigBrotherAwards finanzieren können.*

padeluun fährt fort:

> *Google ist aber einer der gierigsten Konzerne, der ein Datenmonopol anstrebt, und sich überall breit macht mit freundlichen bunten Lettern, Kicker in seine Firmenräume stellt, wo die Mitarbeiter der EU-Parlamentarier gern zum Feierabend auf 'ne Mate vorbeikommen und chillen, der kleine Wettbewerbe für Webdesigner ausschreibt, eine Konferenz hier und zwei Lehrstühle dort mitfinanziert, der (wie Facebook auch) Reisen ins „Valley" für Journalisten sponsert und Seminare und komplette Journalismus-Stipendien vergibt. Sprich: Google, Facebook und Co betreiben „Landschaftspflege" wie*

aus dem Lehrbuch der Lobbyarbeit. Was kann es da besseres geben, als mal der Zeit Online *eine Software für ein freundliches, verbindendes Projekt zu finanzieren?*

Abschließend fordert er:

Deshalb, ..., wünsche ich mir: Kehr um vom Weg, den Überwachungskapitalismus voranzutreiben und die Daten Eurer Leserinnen und Leser als Preis für Eure journalistische Arbeit zu verschachern. Gebt Google das Geld … wieder zurück. Sucht hartnäckig weiter nach Möglichkeiten, Journalismus ehrenvoll und in Würde zu betreiben und zu finanzieren. Verlange das auch von Deinen Herausgebern und Verlegern! Das wäre wahre Innovation.

Der Preis wurde exemplarisch an *Zeit Online* verliehen, da ein Großteil vergleichbarer Angebote vergleichbare Tracker enthalten.

Anders als die meisten PreisträgerInnen erschien Jochen Wagner, der Chefredakteur von *Zeit Online*, zur Preisverleihung. Er räumte ein, dass einige der Kritikpunkte auch aus seiner Sicht berechtigt sind, z. B. wird der Facebook-Pixel in die Seiten von *Zeit Online* eingebunden. Es seien aber nicht alle Punkte korrekt. Im Blog *Glashaus* bei Zeit Online nimmt er dazu auch schriftlich Stellung:

[D]as Projekt Deutschland spricht *wurde 2018 und wird 2019 über die genannte Plattform* My Country Talks *organisiert, so wie mittlerweile zahlreiche internationale Projekte. Die Plattform ist eine Eigenentwicklung mit einem aufwändigen Sicherheits- und Datenschutzkonzept. Google-Dienste werden dafür nicht genutzt, bis auf den vorgeschalteten Service reCaptcha, der Spam-Attacken und Bot-Angriffe blockiert. Insbesondere speichert die Plattform nicht „politische Ansichten von Menschen auf Servern in den USA". Alle Daten liegen in Deutschland.*

Aus Sicht von *Zeit Online* wurden die Webseite von *Zeit Online* selbst, die Marketing-Webseite *mycountrytalks.org* und die App von *My country talks* verwechselt. Ob bei der Nutzung immer trennscharf in den einzelnen Bereichen navigiert wird, ist nicht klar. Dass *Zeit Online* den Facebook-Pixel ausliefert, ist zu kritisieren; der Verweis darauf, dass „viele reichweitenstarke journalistische Angebote" dies tun, macht es nicht besser.

Weiter heißt es:

Der ZEIT-Verlag nutzt unternehmensweit die kostenpflichtige Variante G Suite für Unternehmen, bei der die Auftragsdatenverarbeitung und der Datenschutz geregelt sind. Eine Nutzung dieser Daten durch Google ist vertraglich ausgeschlossen,

Ob die üblicherweise sehr komplexen Vertragsbedingungen schlussendlich ausreichend sind, um tatsächlich einen angemessenen Schutz der Daten zu gewährleisten, wäre zu überprüfen.

Als Reaktion nahm padeluun auf der Webseite der BigBrotherAwards Stellung:

Jochen Wegner hat unter großem respektvollem Applaus den BigBrotherAward für Zeit Online persönlich entgegengenommen. Wir haben tatsächlich nur das öffentlich einsehbare Frontend von mycountrytalks.org untersucht (bei dem mittlerweile alle Tracker abgeschaltet sind). Zeit Online beteuert in ihrem Blog Glashaus, dass sie unsere früher schon geäußerte Kritik gehört hatten und die neu programmierte Anwendung, die als Snippets in den Websites der Partnermedien eingebunden wird, extrem datensparsam arbeitet. Seine Erläuterungen klingen plausibel. Wir werden das im weiteren Dialog mit Zeit Online weiter beobachten. Besonders die Einbindung der Snippets auf den trackingverseuchten Websites der Partnermedien dürfte eine Herausforderung sein. Am Wesenskern meiner Laudatio ändert sich nichts.

„*Vielleicht entsteht daraus eine größere Debatte über den Einfluss, den ein so großer Konzern wie Google auf den deutschen Journalismus haben kann*", kommentierte die Moderatorin Golineh Atai abschließend bei der Preisverleihung.

Lob und Tadel

Im Abschnitt *Lob und Tadel* werden Organisationen und Menschen genannt, denen die Jury keinen Preis verliehen hat, die sie aber dennoch für erwähnenswert hält. Tadel gab es für:

- Mood Tracker, die helfen, die eigene Stimmung zu reflektieren und einzuordnen, ob man möglicherweise unter einer Depression leidet. Dazu verarbeiten sie sensibelste Daten über die psychische Gesundheit der NutzerIn. Ein solcher Mood Tracker ist Moodpath, ein anderer Selfapy. Eine Analyse von Moodpath hat aufgedeckt, dass er IP-Adresse, Google-Werbe-ID, den Paketnamen der App und ihre Versionsnummer, die Android-Version, das Gerät, die Displayauflösung und evt. weitere Daten an Facebook übermittelt.

- Berliner Verkehrsbetriebe (BVG) für die fortgesetzte Videoüberwachung ohne Transparenz über die Weiterverarbeitung. Inzwischen wurde bekannt, dass die Kameras auch in der Lage sind, Tonaufnahmen zu erstellen und zu versenden. Dies ist laut BVG deaktiviert – das kann aber nicht überprüft werden.

- „Smart Card" – Edeka in Porta Westfalica, der den EASY-Shopper betreibt, der den Komfort beim Einkaufen erhöhen soll: durch Scannen des Preises, Erstellen einer Einkaufsliste und GPS-gesteuertes Navigieren zum gewünschten Artikel im Einkaufsmarkt. Doch dazu braucht man eine App oder eine Rabattkarte, die mit der Einkaufsliste die Vorlieben beim Einkauf erhebt und speichert.

Lob gab es für die freie Ärzteschaft und Jens Ernst, der in der Telematik-Infrastruktur für den Austausch von Gesundheitsdaten auf eine Fehlkonfiguration aufmerksam gemacht hat, die dazu führte, dass Antivirenprogramme und Firewalls deaktiviert werden und damit Daten von Patientinnen und Patienten ungeschützt im Netz liegen. Dies sei ein fahrlässiger Umgang mit sensiblen Gesundheitsdaten, der erst dadurch öffentlich wurde.

Publikumspreis

Die Publikumswahl wurde erstmals sowohl mit Wahlzetteln im Saal als auch durch eine Online-Abstimmung durchgeführt. Beide Gruppen wählten mit jeweils ca. der Hälfte der abgegebenen Stimmen den Preisträger in der Kategorie *Behörden & Verwaltung*, den **hessischen Innenminister Peter Beuth** zum Gewinner des Publikumspreises.

Anmerkung

1 *Weitere Informationen und Nachweise finden sich auf der Webseite der BigBrotherAwards, http://www.bigbrotherawards.de. Von dort stammen auch alle Zitate aus den Laudationes.*

Rolf Gössner

Kategorie Behörden & Verwaltung – Laudatio

Der BigBrotherAward 2019 in der Kategorie „Behörden & Verwaltung" geht an den hessischen *Innenminister Peter Beuth* (CDU).

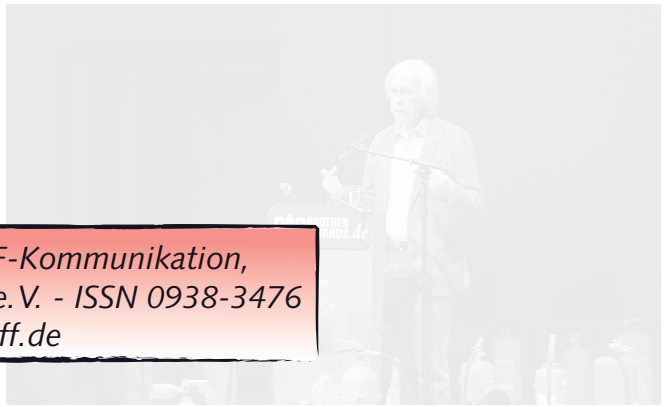
Er erhält den Negativpreis

1. für die bundesweit erstmalige Anschaffung einer Analysesoftware der CIA-nahen Firma Palantir,

2. dafür, dass diese umstrittene US-Firma über Einsatz und Betrieb der Software Zugang zum Datennetz der hessischen Polizei erhält, und

3. dafür, dass mit dieser Analyse[illegible] lizeieigenen und externen Q[illegible] tomatisiert verknüpft, analysiert und ausgewertet werden können – mit fatalen Auswirkungen auf Grundrechte, Datenschutz und Rechtsstaat.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de



Laudator Dr. Rolf Gössner – Foto: Jens Reimedes, CC BY-SA 4.0

Ja, wir haben die schwarz-grünen Regierungsfraktionen in Hessen schon letztes Jahr mit einem BigBrotherAward ausgezeichnet, und zwar für ihre damals geplante Verschärfung des Verfassungsschutz- und Polizeigesetzes[1]. Trotz aller Proteste sind diese Gesetze im Juli 2018 verabschiedet worden und seitdem in Kraft. Damit darf die hessische Polizei inzwischen neue Überwachungsmaßnahmen weit im Vorfeld eines Verdachts oder einer möglichen Gefahr ergreifen – etwa Staatstrojaner installieren oder Menschen in elektronische Fußfesseln legen, von denen sie nur annimmt, dass sie künftig Straftaten begehen könnten.

Damit aber nicht genug: Um diese neuen präventiven Aufgaben zu erfüllen und die dabei anfallende Datenflut zu bewältigen, holte sich die Polizei auch noch die umstrittene CIA-nahe Firma Palantir ins Haus. Deshalb kommen wir erstmals in der Geschichte der deutschen BigBrotherAwards nicht darum herum, einen zweiten Straf-Preis in Folge an einen Datenfrevler derselben Regierungskoalition desselben Bundeslandes verleihen zu müssen.

Der hessische Innenminister Peter Beuth ist dafür verantwortlich, dass die US-Firma Palantir beauftragt worden ist, ihre Analysesoftware *Gotham* im IT-System der hessischen Polizei zu installieren und in Betrieb zu setzen. Benannt ist diese Software nach jener fiktiven, von Kriminalität und Korruption verseuchten Stadt, in der Batman Verbrecher jagt und für Recht und Ordnung sorgt. Nachdem die *Gotham*-Software an hessische Polizei-Bedürfnisse angepasst worden ist, heißt sie *Hessen-Data*. Zur Nutzung ermächtigt wird die Polizei mit § 25a des verschärften Hessischen Polizeigesetzes (HSOG), weshalb dieser Paragraf auch spöttisch „Palantir-Ermächtigung"[2] genannt wird. Danach dürfen umfangreiche Datenanalysen durchgeführt werden zur vorbeugenden Bekämpfung von über vierzig Straftaten, die in § 100a Abs. 2 StPO (Telekommunikationsüberwachung) aufgelistet sind, sowie zur Abwehr bestimmter Gefahren.

Was aber ist nun so problematisch und grundrechtsschädigend an dieser Verknüpfungs- und Analysesoftware der US-Firma *Palantir*?

Palantir, benannt nach den *sehenden Steinen* aus *Herr der Ringe*, ist „eine der umstrittensten Firmen des Silicon Valley", so die *Süddeutsche Zeitung*. Sie gilt nach Einschätzung der US-Bürgerrechtsvereinigung ACLU als „Schlüsselfirma in der Überwachungsindustrie"[3]. Der US-„Star-Investor" und Milliardär Peter Thiel, der bereits den Online-Bezahldienst Paypal mitgegründet hatte, gründete die Firma im Jahr 2004 mit finanzieller Unterstützung des US-Geheimdienstes CIA. Die Kundenliste der Firma liest sich wie das Who-is-who der US-Militär- und Sicherheitsbürokratie: CIA, FBI, NSA, Pentagon, Marines und Airforce[4]. Oder anders ausgedrückt: Als Hauslieferant dieser Behörden ist die Firma tief in den militärisch-digitalen Komplex der USA verstrickt und ihr Geschäftsmodell heißt: BigData for BigBrother[5]. Peter Thiel sitzt zudem im Aufsichtsrat von Facebook und hat Donald Trumps Wahlkampf mit über einer Million US-Dollar unterstützt[6].

Die hessische Polizei beauftragte also diese hoch umstrittene Überwachungsfirma damit, ihre Polizeidatenbanken mit Social