STANDPUNKTE 12 / 2015

WOLFIE CHRISTL

DURCHLEUCHTET, ANALYSIERT UND EINSORTIERT

ZUR FORTSCHREITENDEN DIGITALEN ERFASSUNG UNSERES ALLTAGS DURCH UNTERNEHMEN UND DEN DAMIT EINHERGEHENDEN GESELLSCHAFTLICHEN RISIKEN

In den letzten zehn Jahren hat sich eine Entwicklung zugespitzt, die auf die vollständige digitale Erfassung unseres Lebens hinausläuft. Unser Alltag wird heute von Tausenden Unternehmen überwacht, die uns ständig durchleuchten, einsortieren und bewerten – und unsere intimsten Details an den Handel, an Versicherungen sowie an die Finanz- und Personalwirtschaft verkaufen. Das digitale Geschäft mit unseren persönlichen Daten läuft auf Hochtouren. Um den damit verbundenen persönlichen und gesellschaftlichen Risiken etwas entgegenzusetzen, bedarf es dringend mehr Transparenz über die zunehmend aggressiven Unternehmenspraktiken, verbunden mit einer neuen europäischen Datenschutz- und Technologiepolitik[1].

Durch die rasante Weiterentwicklung der Informations- und Kommunikationstechnologien dringt die Erfassung persönlicher Daten immer mehr in den Alltag ein. Unsere Vorlieben und Abneigungen werden heute in einem Ausmaß digital gespeichert, verarbeitet und verwertet, das bis vor wenigen Jahren noch undenkbar war. Einzelne Personen werden über Geräte und Plattformen hinweg wiedererkannt, deren Verhalten und Bewegungen detailliert ausgewertet, Persönlichkeit und Interessen akribisch analysiert. Im sogenannten Internet der Dinge sind immer mehr Geräte und Objekte mit Sensoren ausgestattet und mit dem Internet verbunden, was umfassende Einblicke in das Leben ihrer NutzerInnen ermöglicht. Gleichzeitig lassen sich im Zeitalter von Big Data mit automatisierten Methoden schon aus rudimentären Metadaten über Kommunikations- und Online-Verhalten umfangreiche Persönlichkeitsprofile erstellen. Nicht nur Firmen in den Feldern soziale Netzwerke, Online-Werbung, mobile Apps oder Fitness arbeiten mit Hochdruck an Geschäftsmodellen, die auf der kommerziellen Verwertung der gesammelten Profile beruhen.

VOM SMARTPHONE ZUM INTERNET DER DINGE: DATENHUNGRIGE GERÄTE UND PLATTFORMEN

Facebook hatte zu Beginn des Jahres 2015 global um die 1,4 Milliarden zumindest einmal monatlich aktive NutzerInnen[2] und wertet in jeder Sekunde Millionen von Einzelinformationen über deren Kontakte, Interessen und Verhaltensweisen aus. Google gibt wenige Zahlen über registrierte NutzerInnen heraus, dürfte aber Zugriff auf vergleichbare, wenn nicht sogar noch größere Mengen täglicher Nutzungsinteraktionen haben. Allein schon die globale Dominanz als Suchmaschine und der hohe Marktanteil bei den meist mit einem Google-Account genutzten Smartphones auf Basis des Betriebssystems Android sprechen eine deutliche Sprache.

Smartphones und die darauf installierten Apps – also Zusatzprogramme von Drittanbietern – sind heute eines der größten Einfallstore für Unternehmen, die persönliche Daten über NutzerInnen sammeln. Diese Geräte weisen eine Vielzahl an Sensoren auf wie etwa Mikrofon, Kamera, GPS-Empfänger, Bewegungs-, Lage-, Licht-, Näherungs- und Magnetfeldsensoren. Smartphones ermöglichen durch die darauf gespeicherten Daten sehr weitgehende Einblicke in den Alltag ihrer BesitzerInnen. Dieser Markt wird von den beiden Plattformen Android (Google) und iOS (Apple) dominiert. Laut einer Untersuchung von Appthority übertragen 71 Prozent der kostenlosen Android-Apps und 32 Prozent der kostenlosen iOS-Apps persönliche Daten an Drittunternehmen.[3] Mehr als die Hälfte der Apps greift auf sensible Informationen wie Standortdaten zu. Nach einer anderen Untersuchung[4] greifen 31 Prozent von 1.200 populären Apps auf Daten zu, ohne dass dies für die eigentliche Funktion der App notwendig wäre. 59 Prozent der Apps informieren NutzerInnen nicht ausreichend darüber, welche Daten genutzt und weitergegeben werden.

ROSA LUXEMBURG STIFTUNG

Auch tragbare Geräte zur Auswertung von Schritten, Puls, Schlaf und anderen Körperfunktionen – sogenannte Wearables – sind inzwischen ein Milliardengeschäft. Die von Fitnessarmbändern und Smartwatches gemessenen Daten über Körper und Gesundheit haben großes kommerzielles Potenzial. Während die NutzerInnen mit Spielmechaniken und Anreizen dazu motiviert werden, die Geräte möglichst oft zu nutzen, arbeiten die Unternehmen an Geschäftsmodellen zur kommerziellen Verwertung der erfassten Daten. Der Marktführer Fitbit wirbt etwa öffentlich mit Angeboten für Versicherungen und arbeitet bereits mit vielen Unternehmen im Rahmen betrieblicher Gesundheitsprogramme zusammen. Angestellte des Ölkonzerns BP wurden etwa dazu angehalten, mit Fitbit eine Million Schritte pro Jahr zu erreichen – ein Mitarbeiter ersparte sich dadurch 1.200 US-Dollar bei der Krankenversicherungsprämie.[5] Große US-Versicherer haben bereits Programme gestartet, die Wearables integrieren und bei Erreichen bestimmter Fitnessziele Belohnungen wie Einkaufsgutscheine oder Kinotickets versprechen. Generali hat für den deutschen Sprachraum ein ähnliches Programm angekündigt.[6] Es ist wahrscheinlich eine Frage der Zeit, bis KonsumentInnen direkte Rabatte auf Versicherungsprämien erhalten.

Im sogenannten Internet der Dinge werden zudem immer mehr Alltagsgegenstände mit kleinen vernetzten Computern und Sensoren ausgestattet. E-Book-Reader zeichnen detaillierte Informationen zum Leseverhalten auf, vernetzte TV-Geräte versenden Daten über das Fernsehverhalten. Vernetzte Autos, Stromzähler, Thermostaten und Brandmelder oder Kühlschränke liefern bald an vielen Stellen umfangreiche Daten über unser Alltagsverhalten. Dabei überwachen die NutzerInnen nicht nur sich selbst, sondern auch andere – etwa ihre Kinder oder ihre Angestellten, die entweder Geräte mit Sensoren mit sich tragen oder sich an Orten bewegen, die mit Sensoren ausgestattet sind. Das Angebot reicht von der elektronischen Fußfessel für Babys (Owlet Baby Care) bis zu Systemen wie Theatro, das die Ortung von Beschäftigten im Einzelhandel ermöglicht und Auswertungen über deren Verhalten, Produktivität und Bewegungsmuster bietet. Datenbrillen und Wearables zur digitalen Vermessung von Körper, Gesundheit, Verhalten und Umgebung werden immer unauffälliger und kommen heute etwa in Form von Pulssensoren in biometrischen Kopfhörern, Temperatur- und Feuchtigkeitssensoren in elektronischen Tattoos oder in Form von mit Sensoren ausgestatteten Ringen, Socken, T-Shirts, Büstenhalter, Zahnbürsten oder Gabeln daher. Viele ExpertInnen erwarten, dass Anreize zur Verhaltensänderung, beispielsweise zur Übernahme von gesünderen oder sichereren Lebensweisen oder von bestimmten Arbeitsweisen, zum zentralen Treiber für das Internet der Dinge werden.[7]

ANALYSE PERSÖNLICHER DATEN UND VERHALTENSPROGNOSEN AUF BASIS VON BIG DATA

Schon heute werden statistische Methoden und andere Technologien der Analyse eingesetzt, um große Mengen digitaler persönlicher Daten zu analysieren und darin Muster und Zusammenhänge zu finden. Damit lassen sich Erkenntnisse über Einzelne gewinnen, die weit über die in den gesammelten Rohdaten enthaltenen Informationen hinausgehen oder sogar Prognosen über unser zukünftiges Verhalten zulassen. Eines der meistzitierten Beispiele des Einsatzes von statistischen Prognosen auf Basis persönlicher Daten, die auf den ersten Blick nicht sehr aussagekräftig zu sein scheinen, ist der Fall der US-Supermarktkette Target. Deren Leitung hatte versucht, schwangere Frauen und sogar deren Geburtstermine anhand der Analyse des Einkaufsverhaltens zu identifizieren. Recherchen des Journalisten Charles Duhigg zufolge war Target dabei nicht auf offensichtliche Informationen etwa zum Erwerb von Babykleidung oder Kinderwägen angewiesen, sondern zog Schlüsse aus der Menge bestimmter Hautlotionen, Seife, Watte, Waschlappen oder Nahrungsergänzungsmitteln, die in gewissen Zeitabständen gekauft wurden. Target weist allen KundInnen eine Nummer zu – egal ob sie mit Kreditkarte bezahlen, einen Gutschein verwenden, eine Umfrage ausfüllen, die Telefon-Hotline anrufen, eine E-Mail von Target öffnen oder die Website besuchen. Alle Einkäufe und Interaktionen werden protokolliert.

Niemand kann mit Bestimmtheit sagen, wie gut die Prognosetechnologien der Unternehmen wirklich funktionieren, deren Algorithmen sind völlig intransparent. Mehrere wissenschaftliche Studien haben aber gezeigt, dass sich schon auf der Grundlage rudimentärer Metadaten über das Online-Verhalten oder die Smartphone-Kommunikation weitreichende Einschätzungen treffen lassen: Allein auf der Basis von Facebook-Likes kann etwa mit hoher Zuverlässigkeit auf persönliche Eigenschaften wie Geschlecht, Alter, sexuelle Orientierung, ethnische Zugehörigkeit, politische Einstellung, Religion sowie Nikotin-, Alkohol- oder Drogenkonsum geschlossen werden.[8] Selbst wenn Internet-NutzerInnen bestimmte Websites anonym besuchen, lassen sich Aussagen zu deren Geschlecht, Alter, Beruf und Ausbildung treffen.[9] Strukturell ähnliche Daten über Internet-Suchanfragen, gekaufte Produkte oder musikalische Vorlieben bieten einen vergleichbaren Informationsgehalt.

Aus dem Telefonierverhalten wie etwa der Häufigkeit von Anrufen lassen sich mit Wahrscheinlichkeiten zwischen 70 und 76 Prozent der Charaktereigenschaften wie emotionale Stabilität, Extraversion, Offenheit für Neues, soziale Verträglichkeit oder Gewissenhaftigkeit ableiten, ohne auf die Kommunikationsinhalte selbst zuzugreifen.[10] Emotionen oder Zustände wie Zuversicht, Unschlüssigkeit, Nervosität, Entspannung, Trauer oder Müdigkeit lassen sich relativ zuverlässig mithilfe der Analyse von Rhythmus und Dynamik des Tippens erkennen – die Prognosezuverlässigkeit liegt dabei zwischen 77 und 88 Prozent.[11] Aus der Kenntnis vergangener GPS-Standorte lassen sich sogar zukünftige Aufenthaltsorte vorhersagen.[12] Wenn die Bewegungsprofile von Bekannten einbezogen werden, sind solche Prognosen besonders zuverlässig.

PRAKTISCHER EINSATZ IM WIRTSCHAFTSLEBEN

Persönliche Daten werden inzwischen in fast allen Wirtschaftsbereichen zur Vorhersage von Risiken, Ertragschancen oder der Loyalität von KundInnen ausgewertet. Das US-amerikanische Startup ZestFinance etwa kombiniert 70.000 Merkmale aus unterschiedlichsten Quellen, um daraus die Kreditwürdigkeit von Personen abzuleiten.[13] Das Hamburger Unternehmen Kreditech greift dafür unter anderem auf Standortinformationen und Daten aus sozialen Netzwerken zurück. Sogar das Surfverhalten auf der Website oder die Art, wie der Online-Kreditantrag ausgefüllt wird, oder wie häufig die Löschtaste benutzt wird, können als Information in die Analysen einfließen.

Die Firma Evolv hilft Personalabteilungen bei der Bewertung von BewerberInnen und Angestellten. Dabei wird auf

die Daten von inzwischen drei Millionen Personen zurückgegriffen[14] – angefangen bei deren Beschäftigungshistorie und Arbeitsleistung bis hin zur Anzahl ihrer Social-Media-Accounts oder dem benutzten Browser bei der Online-Bewerbung. Auch das Startup ConnectedCube ist mit der Vorhersage der zukünftigen Leistung von Angestellten befasst. Der Versicherungskonzern Aviva versucht, Risiken für Krankheiten wie Diabetes, hohen Blutdruck oder Depression aus Daten über Konsumverhalten, Lebensstil oder Einkommen[15] abzuleiten. Am weitesten fortgeschritten sind derartige Auswertungstechnologien aber im reinen Online-Bereich. Das Werbeunternehmen MediaBrix analysiert die Emotionen von Online-SpielerInnen, spricht diese gezielt und individuell in ganz bestimmten Momenten, zwischen Begeisterung und Frustration, an. Damit konnte die Effektivität der Werbung im Web um 15 Prozent und bei mobilen Apps sogar um 30 Prozent gesteigert werden.

Große internationale Internet-Shops zeigen KonsumentInnen auf Basis von deren Online-Verhalten, Standortinformationen, benutzten Geräten oder Browsern unterschiedliche teure Produkte an oder gar gleiche Produkte mit Preisunterschieden von bis zu 166 Prozent.[16] Beim Reisebuchungsportal Orbitz wurde bei Nutzung eines Mac-Computers eine Auswahl von um bis zu 13 Prozent teurerer Hotels angeboten als bei der Nutzung eines PCs.[17] KonsumentInnen haben bei derartigen Praktiken keine Chance mehr, zu verstehen, wie Preise oder die Auswahl der ihnen angebotenen Produkte zustande kommen.

DATA BROKER UND WERBENETZWERKE: DAS GESCHÄFT MIT UNSEREN PERSÖNLICHEN DATEN

Internationale Player im Geschäft mit den persönlichen Daten – sogenannte Data Broker – verfügen über umfangreiche Daten und erwerben Daten über KonsumentInnen aus umfassenden Online- und Offline-Quellen[18] – angefangen von Informationen über das Zahlungsverhalten und Zeitschriftenabonnements über Aktivitäten in sozialen Medien bis hin zu Daten über religiöse Zugehörigkeiten und politische Präferenzen. Sie ziehen daraus Schlüsse über ethnische Herkunft, Einkommen oder Gesundheit und verkaufen diese Informationen an Versicherungen, Handelsunternehmen oder Personalabteilungen von Firmen und sogar an staatliche Stellen. Die Firma Acxiom etwa verfügt über umfangreiche Dossiers, in denen bis zu 3.000 Einzelinformationen unter anderem zu Ausbildung, zur Wohn- und Beschäftigungssituation, zur finanziellen Lage, zu Eigentumsverhältnissen, zum Wahlverhalten oder zu «Bedürfnissen» und «Interessen» im Bereich Gesundheit von über 700 Millionen Menschen festgehalten sind.[19] Das Unternehmen betreibt 15.000 Kundendatenbanken von globalen Top-Unternehmen und kooperiert mit Google, Facebook und Twitter.[20] Acxiom ist auch in Deutschland tätig und besitzt laut der Wochenzeitung *Die Zeit* Daten von über 44 Millionen Deutschen.[21] Das Unternehmen Datalogix verfügt über Transaktionsdaten von KonsumentInnen über ein Einkaufsvolumen von mehr als zwei Billionen US-Dollar[22] und erhebt im Rahmen einer Partnerschaft mit Facebook, wie oft NutzerInnen online Werbung für bestimmte Produkte sehen und daraufhin dann die entsprechenden Käufe in Geschäften tätigen.

Die Firma Lexis Nexis gibt an, Daten über 500 Millionen KonsumentInnen[23] zu besitzen, und wirbt mit «Risikomanagement-Lösungen» für die Bereiche Versicherung, Handel oder den Gesundheitssektor. Angeboten werden unter anderem Daten über die Kreditwürdigkeit von Personen, Überprüfungen zum Hintergrund von ArbeitnehmerInnen[24] oder Informationen über sogenannte Problemmieter.[25] Darüber hinaus werden biometrische Services vom Fingerabdruck bis zur Stimmerkennung angeboten – oder Produkte zur Erkennung von «Risiken und Bedrohungen» in sozialen Medien.[26] Außerdem sind in den letzten Jahren Tausende Firmen entstanden, die sich auf Online-Tracking, Analyse und Werbung spezialisiert haben. Sie identifizieren NutzerInnen über Websites, Apps und Geräte hinweg und sammeln gewaltige Mengen an persönlichen Informationen. Beim Aufruf beinahe aller populären Websites wird jeder einzelne Klick an mehrere Drittunternehmen übertragen, ebenso bei vielen Smartphone-Apps. Das *Wall Street Journal* hat bei einer Untersuchung der 50 populärsten Websites 2010 festgestellt, dass bis auf Wikipedia alle auf derartige Weise die Daten ihrer NutzerInnen an Dritte weiterleiten. 37 der 50 populärsten Internetseiten übertrugen bei jedem Klick Informationen an über 30 Drittparteien, 22 davon sogar an über 60 Drittparteien. Die Analyse- und Werbeplattform Flurry ist global auf 1,4 Milliarden Smartphones und Tablets installiert und zeichnet die Nutzungsaktivitäten in 540.000 unterschiedlichen Apps auf.[27] Das Unternehmen wirbt damit, ein Drittel aller globalen App-Aktivitäten zu überwachen, und ermöglicht Werbetreibenden eine gezielte Ansprache nach Geschlecht, Alter und Interessen. Zudem werden die NutzerInnen Kategorien wie Hardcore-SpielerInnen oder frischgebackene Mütter zugeordnet oder nach ihrer sexuellen Orientierung klassifiziert.

GESELLSCHAFTLICHE IMPLIKATIONEN

Heute ist kaum mehr nachvollziehbar, welche Daten zur eigenen Person und zum persönlichen Verhalten von Unternehmen digital erfasst und gespeichert werden, wie diese Daten verarbeitet werden, an wen sie weitergegeben oder verkauft werden, welche Schlussfolgerungen daraus gezogen werden und welche Entscheidungen auf Basis dieser Schlüsse über sie gefällt werden. Viele Unternehmen ermöglichen den NutzerInnen nicht einmal mehr den Zugriff auf ihre eigenen Daten und betrachten ihre Algorithmen als Betriebs- und Geschäftsgeheimnis.

Die Verarbeitung und Weiterleitung von persönlichen Daten – jenseits des ursprünglichen Verwendungszwecks bei deren Erfassung – ist heute fast schon eine Selbstverständlichkeit. Überall dort, wo große Datenmengen gespeichert werden, drohen Datenmissbrauch und -verlust. Dadurch entstehen große Risiken für Einzelne – von Belästigung und Stalking bis hin zum «Identitätsdiebstahl» und Cyber-Kriminalität. Wenn Unternehmen Kriterien wie Geschlecht, Alter, ethnische oder religiöse Zugehörigkeit, die materielle Situation oder den Gesundheitszustand ihrer KundInnen zunehmend in ihre geschäftlichen Überlegungen mit einbeziehen, wächst die Gefahr von Diskriminierung und Ausschluss. Generell führt dieser Prozess zu einer potenziellen Einschränkung von individuellen Chancen und Wahlmöglichkeiten. Dies zeigen heute bereits Fälle von «Diskriminierungen» bei Angeboten und Preisen, wobei auch lebensentscheidende Fragen etwa in den Bereichen Finanzen, Gesundheit, Versicherung oder Arbeit betroffen sein können. Verschärfend kommt hinzu, dass «mögliche Diskriminierungseffekte» noch nicht einmal mehr nachzuvollziehen sind, wenn wir «keine Entscheidungsmacht» mehr über die «Wege unserer eigenen Daten» haben, wovor der EU-Parlamentarier Jan Phillip-Albrecht warnt.[28] Der

Datenexperte Michael Fertik behauptet gar, dass durch individuelle Preise und personalisierte Angebote die Reichen schon jetzt «ein anderes Internet sehen» würden als die Armen.[29]

Abgesehen von Fehlern bei der Erfassung der gesammelten Daten können Fehler in den Prognosemodellen und damit falsche Schlussfolgerungen äußerst negative Auswirkungen auf einzelne Personen haben. Big Data ist weit entfernt von wirklicher Objektivität oder davon, wirklich zuverlässige Vorhersagen zu liefern. Die Prognosen sind prinzipiell unscharf, da sie auf Korrelationen und Wahrscheinlichkeiten beruhen. Wer beispielsweise die «falschen Personen» kennt, im «falschen Bezirk» wohnt oder sich bei der Anwendung einer Smartphone-App «falsch verhält», muss damit rechnen, entsprechend klassifiziert zu werden, und negative Konsequenzen tragen, ohne sich dagegen wehren zu können. Wenn Versicherungsunternehmen die Risikoabschätzung zunehmend von Lebensgewohnheiten und Verhaltensweisen abhängig machen, werden dadurch außerdem Risiken immer mehr individualisiert. Auch eine Verweigerung der Teilnahme an der Datenerfassung kann Konsequenzen haben: Wenn keine oder zu wenige Daten über eine Person vorliegen, schätzt ein Unternehmen das Risiko für eine Kundenbeziehung unter Umständen prinzipiell als zu hoch ein.

WAS TUN? HANDLUNGSEMPFEHLUNGEN FÜR POLITIK UND ÖFFENTLICHKEIT

Allgegenwärtige digitale Überwachung könnte künftig drastische Auswirkungen auf Gesellschaft, Demokratie und die Autonomie des Einzelnen haben. Man kann sich nur bedingt vor dieser Art der kommerziellen Überwachung schützen – denn selbst über Menschen, die keine datenerfassenden Angebote nutzen, werden digitale Profile angelegt. Technologieunternehmen aus dem Silicon Valley und anderen Regionen der Welt sind mit hohen Kapitalsummen ausgestattet, treiben die Entwicklung mit permanenten Innovationen voran und legen zunehmend die Regeln für die Informationsgesellschaft fest – während die Politik weitgehend passiv bleibt und viele BürgerInnen sich angesichts der geballten Konzernmacht und den immer größer werdenden Zugriffsmöglichkeiten auf ihre persönlichen Daten eher hilflos fühlen. Um die möglichen negativen Auswirkungen zu minimieren, sind aus Sicht des Autors folgende Schritte überfällig:

- Schaffung von mehr Transparenz über die Praktiken der Unternehmen – durch Forschung, Öffentlichkeit und staatliche Regulierung.
- Eine neue europäische Technologiepolitik: breite Unterstützung einer anderen Art von Innovation in Form von dezentralen Technologien, die mehr Kontrolle über persönliche Daten einräumen – auf allen Ebenen der Forschungs-, Förderungs- und Vergabepraxis.
- Stärkung einer kritischen Auseinandersetzung über Chancen, Risiken, Machtungleichgewichte und Lösungsmöglichkeiten.
- Stärkung der digitalen Zivilgesellschaft: Der Finanzierungsgrad von zivilgesellschaftlichen Organisationen mit Fokus auf Netzpolitik, digitale Technologien und deren gesellschaftliche Implikationen ist – etwa im Vergleich zur Umweltschutzbewegung – mehr als mangelhaft.
- Stärkung von digitaler Kompetenz und der Kenntnisse über Möglichkeiten, die eigenen persönlichen Daten zu schützen.
- Kluge und zügige Umsetzung der seit Jahren überfälligen gemeinsamen europäischen Datenschutzverordnung. Der Entwurf des EU-Parlaments ist zumindest ein guter Kompromiss, die aktuelle Version des EU-Rats wäre aus Sicht der Autors in der Praxis nahezu gleichbedeutend mit einer Abschaffung des Rechts auf informationelle Selbstbestimmung.[30]
- Darüber hinaus ist dringend darüber nachzudenken, wie rechtlich nicht nur Transparenz über die gesammelten Daten, sondern auch über die eingesetzten statistischen Verarbeitungsalgorithmen eingefordert werden könnte.

Wolfie Christl ist Publizist, Netzaktivist und Leiter von Cracked Labs, dem Institut für kritische digitale Kultur in Wien (http://wolfie.crackedlabs.org). Er beschäftigt sich mit den gesellschaftlichen Implikationen von Informationstechnologie – insbesondere mit ihren Auswirkungen auf die Privatsphäre, mit Überwachung und Verwertung persönlicher Daten im digitalen Zeitalter. Er ist Mitinitiator des vielfach ausgezeichneten kritisch-didaktischen Online-Spiels «Data Dealer».

1 Dieser Text basiert auf der Kurzfassung der vom Autor im November 2014 publizierten Studie «Kommerzielle digitale Überwachung im Alltag». **2** Vgl. http://allfacebook.de/zahlen_fakten/facebook-nutzerzahlen-2015. **3** Appthority: App Reputation Report, 4.8.2014, unter: www.nomasis.ch/fileadmin/user_upload/flyer/produkte/Appthority/App_reputation_report.pdf. **4** Office of the Privacy Commissioner of Canada: Global Privacy Enforcement Network Privacy Sweep, 10.4.2014, unter: www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp. **5** Ebd. **6** Gröger, Anne-Christin: Generali erfindet den elektronischen Patienten, in: Süddeutsche Zeitung, 21.11.2014. **7** Anderson, Janna/Lee, Rainie: The Internet of Things Will Thrive by 2025, Pew Research Center, Washington D.C. 2014, unter: www.pewinternet.org/2014/05/14/internet-of-things. **8** Kosinski, Michal/Stillwell, David/Graepelb, Thore: Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, 9.4.2013, unter: www.pnas.org/content/110/15/5802. **9** De Bock, Koen/Van den Poel, Dirk: Predicting website audience demographics for web advertising targeting using multi-website clickstream data, in: Fundamenta Informaticae 1/2010, S. 49–70. **10** Chittaranjan, Gokul/Blom, Jan/Gatica-Perez, Daniel: Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones, in: Proceedings of the 2011 Annual International Symposium on Wearable Computers, San Francisco 2011, S. 29–36, unter: http://infoscience.epfl.ch/record/192371/files/Chittaranjan_ISWC11_2011.pdf. **11** Epp, Clayton u.a.: Identifying Emotional States Using Keystroke Dynamics, in: Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems, Vancouver 2011, S. 715–724, unter: http://hci.usask.ca/uploads/203-p715-epp.pdf. **12** Talbot, David: A Phone that Knows Where You're Going, in: MIT Technology Review, 9.7.2012, unter: www.technologyreview.com/news/428441/a-phone-that-knows-where-youre-going/. **13** Crosman, Penny: ZestFinance Aims to Fix Underwriting for the Underbanked, 29.11.2013, unter: www.americanbanker.com/issues/177_223/zestfinance-aimsto-fix-underwriting-for-the-underbanked-1054464-1.html. **14** Javers, Eamon: Inside the wacky world of weird data: What's getting crunched, CNBC, 12.2.2014, unter: www.cnbc.com/id/101410448. **15** Scism, Leslie/Maremont, Mark: Insurers Test Data Profiles to Identify Risky Clients, in: The Wall Street Journal, 19.11.2010. **16** Mikians, Jakub u.a.: Detecting price and search discrimination on the internet, unter: http://conferences.sigcomm.org/hotnets/2012/papers/hotnets12-final94.pdf. **17** Mattioli, Dana: On Orbitz, Mac Users Steered to Pricier Hotels, in: Wall Street Journal, 23.8.2012. **18** Federal Trade Commission: Data Brokers. A Call for Transparency and Accountability, Bericht vom Mai 2014, unter: www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. **19** Acxiom: Annual Report 8, Bericht vom September 2013, unter: http://d3u9yejw7h244g.cloudfront.net/wpcontent/uploads/2013/09/2013-Annual-Report.pdf. **20** Dwoskin, Elizabeth: Data Broker Acxiom Moves to Tie Physical World to Online Data, in: Wall Street Journal, 14.5.2014. **21** Mclaughlin, Catriona: Acxiom. Die Besserwisser, in: Die Zeit, 5.7.2013. **22** Vgl. www.datalogix.com/audiences/online. **23** Vgl. www.lexisnexis.com/risk/about/data.aspx. **24** Vgl. www.lexisnexis.com/risk/downloads/literature/Business-Edition.pdf. **25** Vgl. www.lexisnexis.com/government/solutions/literature/screening.pdf. **26** Vgl. www.lexisnexis.com/risk/newsevents/press-release.aspx?id=1381851197735305. **27** Vgl. www.flurry.com/solutions/advertisers/brands. **28** Albrecht, Jan Philipp: Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden, München 2014. **29** Fertik, Michael: The Rich See a Different Internet Than the Poor. Ninety-nine percent of us live on the wrong side of a one-way mirror, in: Scientific American, 15.1.2013. **30** Vgl. http://lobbyplag.eu/governments/topics.

IMPRESSUM

STANDPUNKTE wird herausgegeben
von der Rosa-Luxemburg-Stiftung und erscheint unregelmäßig
V. i. S. d. P.: Henning Heine
Franz-Mehring-Platz 1 · 10243 Berlin · www.rosalux.de
ISSN 1867-3163 (Print), ISSN 1867-3171 (Internet)
Redaktionsschluss: April 2015
Lektorat: TEXT-ARBEIT, Berlin
Satz/Herstellung: MediaService GmbH Druck und Kommunikation
Gedruckt auf Circleoffset Premium White, 100 % Recycling