https://police-it.org/millionen-von-facebook-nutzern-unfreiwillig-psychologisch-vermessen

Der Skandal ist nicht das 'Datenleck', sondern die Erstellung von Psychogrammen über Millionen von Nutzern

Millionen von Facebook-Nutzern unfreiwillig psychologisch vermessen

19. März 2018 | Von Abbe | Kategorie: AKTUELLES, DATENSCHUTZ UND POLIZEI

Eine dubiose Firma hat Millionen von Psychogrammen über Facebook-Nutzer erstellt und für politische Beeinflussungs-Kampagnen verwendet. Das ist der eigentliche Skandal hinter dem angeblichen Datenleck bei Facebook, das am Wochenende die Leitmedien bewegte. Die Nutzer hatten nie ihr Einverständnis gegeben, ja noch nicht einmal gewusst, dass ihre „Likes“ und Texteinträge genutzt werden, um sie psychografisch zu vermessen und mit Propaganda zu beliefern. Der Fall demonstriert, wie unkritisch und duldsam wir alle inzwischen hinnehmen, dass die Spuren, die unsere Internet-Nutzung hinterlässt, dazu genutzt werden, uns individualisierte Werbung und zielgerichtete Informationen auf den Bildschirm zu spielen. Google und Facebook sind damit zu den profitabelsten Unternehmen der Welt geworden. Und auch der Springer-Konzern macht schon 71% seines Umsatzes mit Werbung, großteils aus dem Internet.
Ist es da ein Wunder, dass auch die Polizei begehrlich auf den Datenschatz im Internet schielt. Im Entwurf zum neuen Bayerischen Polizeigesetz ist schon mal vorgesehen, dass Apple, Google, Facebook & Co den Zugriff auf Emails, Likes und Freundeslisten zulassen müssen. Gut möglich, dass dieses Gesetz zur Mustervorlage für alle anderen Bundesländer werden wird. | Lesedauer: Ca. 15 Minuten

---

Es mag daran liegen, dass echte Nachrichten an einem Wochenende selten sind. Umso lauter tönte der Observer/Guardian, dass *„50 Millionen Facebook Profile von (der Firma) Cambridge Analytica in einem der größten Dateneinbrüche ausgeschlachtet worden“* seien [1]. Die New York Times wusste, *„wie Berater von Trump die Facebook-Profile von Millionen abgeschöpft wurden“* [2]. Süddeutsche, Spiegel, Tagesschau, Neue Zürcher Zeitung und Welt (und viele weitere) zogen nach mit immer dem gleichen Tenor: *„Spätere Trump-Berater sollen 50 Millionen Facebook-Profile illegal ausgewertet haben“* [3].

Bemerkenswert an diesem medialen Sturm im Wasserglas ist: Nichts daran ist wirklich NEU:

- Nicht, dass Cambridge Analytica, die Firma im Zentrum dieser medialen Aufregung, ihre Anschubfinanzierung vom erzkonservativen Investor Robert Mercer erhalten hatte;
- nicht, dass Donald Trumps späterer Strategieberater, der Ultra-Rechte Steve Bannon, zu dieser Zeit Vice President von Cambridge Analytica war;
- nicht, dass das Gesch#ftsmodell von Cambridge Analytica (CA) darin besteht, Persönlichkeitsprofile von Nutzern sozialer Medien zu erstellen – die davon nichts wissen;

- und aufgrund der Auswertungsergebnisse politische Einstellung oder ein Abstimmungsverhalten zu beeinflussen. Das geschah bisher mindestens dreimal, nämlich
    - erst beim repulikanischen Präsidentschaftsbewerber Ted Cruz,
    - dann bei Donald Trump
    - und auch bei der Kampagne Leave.eu, die zur Entscheidung für den Brexit führte.
- Und es ist auch nicht neu, dass man für solche Auswertungen eine sehr breite Datenbasis braucht. Facebook wird seit Jahren immer wieder damit in Verbindung gebracht, dass die Daten zur Entwicklung der „Algorithmen“ für diese CA-Politkampagnen von Facebook-Nutzern stammten. Die dazu nie ihr Einverständnis gegeben hatten.

Wenn das alles nicht neu war, stellt sich die Frage: Was soll die Aufregung? Und warum gerade jetzt?

Wie die Facebook-Daten gewonnen wurden

2014, die Firma Cambridge Analytica war da noch keine zwei Jahre alt, gab es an der Universität von Cambridge in England einen russisch-amerikanischen Psychologen namens **Aleksandr Kogan**. Dessen Spezialgebiet ist die **Psychografie**, das ist ein relativ neuer Zweig der Psychologie. Sie „vermisst“ das Wesen bzw. Verhalten eines Menschen, indem sie das Individuum vergleicht mit einem Modell der Persönlichkeit, das aus verschiedenen Dimensionen besteht. Am bekanntesten in das Big Five-Modell, so benannt nach den fünf wesentlichen Dimensionen der Persönlichkeit, wie

- Offenheit für Erfahrungen (**O**penness)
- Gewissenhaftigkeit (**C**onscientiousness)
- Extrovertiertheit (**E**xtraversion)
- Verträglichkeit im Umgang mit anderen (**A**greeableness)
- emotionale Labilität und Verletzlichkeit (**N**euroticism).

Aus den Anfangsbuchstaben der fünf Dimensionen im Englischen leitet sich der Name OCEAN-Modell ab.

Kogan gründete eine Firma Global Science Research und begeisterte die Firma in der Nachbarschaft – eben Cambridge Analytica – von seiner Idee: Die Persönlichkeitsprofile von Nutzern im Internet zu messen und zu bestimmen. Und damit in der Lage zu sein, deren Verhalten besser einschätzen zu können. Oder, noch besser, um deren Verhalten durch Belieferung mit zielgerichteten Inhalten, die sich am Persönlichkeitsmuster des einzelnen ausrichten, beeinflussen zu können.

Die Interessenten am Test mussten sich mit ihrem Facebook-Login anmelden. Die Nutzer hatten eingewilligt, dass ihre Daten zu Forschungszwecken gespeichert werden.

Kurzfassung eines Persönlichkeitstests nach dem Big Five/OCEAN-Modell
Wenn Sie einen Persönlichkeitstest selbst ausprobieren möchten …

Die meisten waren sich nicht darüber im Klaren, dass die App von Mr. Kogan (‚wie übrigens viele andere Apps auch, achten Sie mal drauf!) u.a. auch die Facebook-Kontaktliste ihrer Freunde und Bekannten auslas. Diese neuen Facebook-Nutzernamen ermöglichten den Zugriff auf weitere

Nutzerprofile, quasi im Schnellballsystem. Insgesamt sollen davon 50 Millionen Facebook-Profile amerikanischer Nutzer betroffen sein. Von denen 30 Millionen „reichhaltig“ genug gewesen sein sollen, um auf deren Basis psychografische Profile der jeweiligen Nutzer anzulegen. Diese Daten soll Kogan weitergegeben haben an die Firma SCL/Cambridge Analytica [c]. So steht es in den länglichen Artikeln des Wochenendes bei Observer/Guardian und New York Times [1] [2].

Facebook wäscht seine Hände (noch) in Unschuld

In den vielen Artikeln dieses Wochenendes ist die Rede vom *„größten Datenleck aller Zeiten“*. Diesen Vorwurf bezeichnete Facebook in einer Stellungnahme vom Freitag, 16.3., als *„vollkommen falsch“* [4]. Denn die rund 270.000 Nutzer, die die App heruntergeladen haben, hätten ja freiwillig ihre Zustimmung gegeben, dass über die App z.B. auch der Ort aus ihrem Nutzer-Profil ausgelesen wird, oder die Inhalte, die sie *„geliked“* haben, sowie *„begrenzte“* Informationen über ihre Freunde – sofern deren Datenschutzeinstellungen dies zuließen.

Das alles sei vollkommen legitim gewesen, sagt Facebook. Bis zu dem Zeitpunbkt, als Kogan die Daten weitergegeben habe an die Firma SCL/Cambridge Analytica [b] und an eine Firma Euonia Technologies. Deren Chef hieß 2014 Steve Bannon, der später strategischer Berater von Donald Trump im Wahlkampf wurde und nach der Wahl noch eine Zeitlang als ‚Chefstratege‘ im Weißen Haus wirkte. Ein gewisser Christopher Wylie arbeitete bei Euonia an der Entwicklung der „Algorithmen“, die dann von Cambridge Analytica eingesetzt wurden. Mit der Weitergabe der Daten an CA und Euonia/Wylie habe Kogan gegen die Facebook-Regeln verstoßen, sagt Facebook. Davon habe Facebook schon 2015 erfahren und von Kogan und den anderen Beteiligten die Erklärung verlangt – und auch erhalten – , dass die so erlangten Daten gelöscht wurden.

Ob es Facebook gelingt, sich mit dieser windelweichen, naiv-treuherzigen Stellungnahme aus der Affäre zu ziehen, bleibt abzuwarten. Jedenfalls hat die Staatsanwaltschaft in Massachusetts aufgrund der Artikel vom Wochenende eine offizielle Untersuchung der berichteten Sachverhalte angekündigt [in 3].

Influence Operations – Beeinflussungs-Kampagnen

Das strategische Konzept, das Cambridge Analytica anwendet, wurde nicht dort erfunden, sondern beim amerikanischen Militär. Es trägt dort den Namen Information Operations oder Influence Operations, also Informations- oder Beeinflussungs-Kampagne. Was das ist, erklärt die Rand Corporation, eine amerikanische Denkfabrik, die die US-Streitkräfte berät:

https://www.rand.org/topics/information-operations.html

Überträgt man die militärisch-martialische Sprache dieser Definition ins Zivile, so besteht die Beeinflussungs-Kampagne aus der Sammlung taktisch relevanter Informationen über ein Gegenüber (Wähler, Internet-Nutzer), sowie der Belieferung mit propagandistischen Inhalten, um

damit einen Vorteil (für den Auftraggeber der Kampagne) zu erzielen.

Das besonders Perfide an Cambridge Analytica

Genau das tut Cambridge Analytica, wenn es den einzelnen Nutzer

- zunächst psychografisch vermisst
- und dann gezielt mit individualisierter Propaganda versorgt.

Der Ansatz ist deshalb so perfide, weil der individuelle Nutzer zum Objekt einer „psychografischen“ Auswertung gemacht wird, ohne dass er davon weiß, geschweige denn zugestimmt hat. Und dass zur Grundlage dieser Auswertung Texte, Kontakte und Interessen des Nutzers gemacht werden, von denen der Nutzer nicht wusste, dass sie zur psychografischen Vermessung herangezogen werden.

Das Big Five-/OOCEAN-Modell ist weltweit ziemlich unumstritten in der Persönlichkeitspsychologie. Darauf basierende Tests eignen sich für die Auswertung von Internet-Daten deshalb so gut, weil sich dort jeder über Texte ausdrückt [c]. Bei der Entwicklung dieses Zweiges der Persönlichkeitspsychologie fand man nämlich heraus, dass die wesentlichen Persönlichkeitsmerkmale sich in der Sprache niederschlagen [5]. Aus der Verwendung bestimmter Begrifffe ist also eine Zuordnung zu bestimmten Persönlichkeitsmerkmalen möglich. Die Auswertung ist also eine leichte Aufgabe für den, der heimlich und ohne dass der Nutzer dies weiß, die Chats, Emails und sonstigen Textbeiträge des Nutzers mitliest und psychografisch auswertet.

Ich wundere mich sehr darüber, dass eine solche Vorgehensweise und die Beeinflussungs-Kampagne zu Wahlwerbungszwecken niemanden aufregt, sondern anscheinend als völlig legitim und normal hingenommen wird. Gemessen daran, wie nach erfolgter Persönlichkeitsauswertung jeder einzelne Nutzer ganz und dosiert angesprochen werden kann (das heißt Micro-Targeting, unten mehr dazu), liegt ein immense Gefahr in diesem Vorgehen. Wesentliche Kritik, geschweige denn Entscheidungen zum Verbot solcher Methoden, sind jedoch weit und breit nicht zu entdecken.

Kaum weniger gefährlich: Micro-Targeting in der Werbung und hinter journalistischen Angeboten

Micro-Targeting nennt man das Verfahren, mit dem einem bestimmten Internet-Nutzer ganz gezielt bestimmte Inhalte oder Werbung auf den Schirm gespielt werden. Das geht inzwischen in Echtzeit. Es setzt natürlich voraus, dass der einzelne Nutzer auch als Individuum identifiziert werden kann.

Methoden zur Identifizierung des Individuums im Internet

Inzwischen sind die Methoden zur Identifizierung des einzelnen Individuums im Internet schon ganz schön ausgebufft:

- Cookies, also kleine Software-Plätzchen auf dem Endgerät sind da schon fast altbacken. Und vor allem keine Lösung, wenn ein- und derselbe Nutzer MEHRERE Endgeräte verwendet.
- Daneben gibt es die Möglichkeit, das einzelne Endgerät an seinem Hard- und Softwareprofil zu erkennen. Denn interessanter Weise unterscheiden sich die Geräte, trotz uniformer Betriebssysteme und Standardsoftware, doch ganz erheblich voneinander.
- Besonders ergiebig ist aber die Auswertung des Surf-Verhaltens des Individuums: Nehmen wir als fiktives Beispiel Herrn Mustermann, der montags bis freitags im Außendienst ist und

dort mal via Smartphone, ein andermal mit dem Tablet und ein drittes Mal im Internet-Café ins Internet geht. Morgens sieht er sich nicht nur die Ergebnisse der europäischen Fußball-Ligen an, sondern auch die der amerikanischen Baseball-League. Sein besonderes Interesse gilt dem Offroad-Fahren, daher besucht er am Wochenende vom heimischen Rechner aus entsprechende Foren. Und ist seit längerem auf der Suche nach einem möglichst jungen Landrover Defender, den er sich gerne in der Freizeit selbst wieder herrichten bzw. weiter ausstatten möchte. Das sind zwar keine Persönlichkeits-Merkmale. Aber doch aussagekräftige **Interessen-Merkmale**. Die vollkommen ausreichen, um Herrn Mustermann mit ziemlicher Sicherheit als Individuum im Internet ausfindig zu machen.

Micro-Targeting nach Art der freundlichen Helfer bei Google und Facebook

Die Firma Google und ihre tollen Produkte sind für die meisten Internet-Nutzer in der westlichen Welt unverzichtbar. Man denke nur an das Betriebssystem Android, den Email-Dienst GMail, Google Maps, an Google+, Google Photo, Youtube und natürlich die Google Suche. Wirklich ganz große Klasse, dieses Rundum-Sorglos-Paket. Das Ganze gibt es kostenlos.

Nur beim Installieren von Apps aus dem Google Play Store (sic?!) fragt sich inzwischen doch der eine oder andere Nutzer, warum er den Zugriff auf seine Smartphone-Kontaktliste erlauben soll, um den kostenlosen Routenplaner nutzen zu können. Aber da es ja so bequem ist, willigt man eben ein!

Ganz ähnlich sieht es übrigens bei Facebook aus. Dort heißen die Angebote am unteren Ende der Angel oder Whatsapp, Messenger und Instagram.

Daten als Ware: Mit kaum etwas anderem wird so viel Geld verdient

Mit dem **Geschäftsmodell – Daten als Ware** – wird so viel Geld verdient, wie in kaum einer anderen legalen Branche: Der Mutterkonzern Alphabet konnte im vergangenen Jahr mit seinen Google-Produkten rund 110 Miliarden Dollar Umsatz einfahren, 12 davon blieben als Reingewinn hängen. Facebook macht zwar wesentlich weniger Umsatz, „nur“ 40,6 Milliarden Dollar. Der Gewinn dort war allerdings mit 15,9 Milliarden Dollar noch wesentlich erfreulicher als bei Google.

Erlösquelle ist bei beiden Firmen nicht die Software oder Nutzungsentgelte für die Plattform oder Suchmaschine. Vielmehr lockt das kostenlose Rundum-Sorglos-Komplettpaket Nutzer an, die anstelle einer Bezahlung Informationen über ihr Verhalten im Internet und ihre Interessen hinterlassen. Google bzw. Facebook erhalten ihr Geld von Werbetreibenden, die Google bzw. Facebook mit zielgerichteten Informationen über unsere Suchinteressen, unsere Photos und letzten Reisen, unsere Email-Kontakte und Video-Vorlieben versorgt. Und damit den Werbetreibenden die Möglichkeit einräumt, uns, je nach individuellem Verhaltens- und Interessenprofil, in Echtzeit versorgen zu lassen mit individualisierter Werbung.

Bei Facebook schwingt seit der Cambridge Analytica-Affäre zusätzlich die Befürchtung mit, dass die Nutzerprofile auch psychografisch ausgewertet und vermarktet werden.

Springer-Konzern: Micro-Targeting mit journalistischen Inhalten

Inzwischen ist auch der Springer-Konzern (und viele andere früheren Zeitungsverlage) auf den Zug aufgesprungen [A]. Den größten Teil am Umsatz im Konzern machen weder die Print- noch die Online-Ausgaben: Nein, mehr als 70% des Umsatzes von Springer stammen inzwischen ebenfalls aus Werbung. Die Aufgabe des Contents – des redaktionellen Inhalts – besteht nur noch darin, wie

es im jüngst vorgelegten Geschäftsbericht heißt, das *„sichere Markenumfeld“* für die Werbekunden zur Verfügung zu stellen. Das Kriterium *„sicher“* soll eine Abgrenzung zum Werbeumfeld bei Twitter, Facebook, Whatsapp & Co sein, denn durch die *„virale Verbreitung von Falschmeldungen“* (auf solchen Plattformen) würden *„Marken von Werbekunden einem rufschädigenden Umfeld ausgesetzt“*.

Einladung zu einem Gedankenspiel

Was wäre eigentlich geschehen, wenn Kogan bzw. Cambridge Analytica die Daten bei Facebook einfach GEKAUFT hätten?
Alle Artikel zum Aufreger dieses Wochenendes wären dann nicht geschrieben worden. Denn bisher hat man sich lediglich darüber aufgeregt, dass *„Facebook angezapft“* wurde, dass es ein angeblich *„riesengroßes Datenleck“* gegeben hätte usw.

Dass Millionen von Nutzern ohne ihr Wissen psychografiert werden, regt dagegen niemanden auf. Es regt auch niemanden auf, dass Facebok und Google (und andere) persönliche Mitteilungen aus Messenger-Diensten oder Emails ganz selbstverständlich mitlesen und auswerten. Dass viele Apps ganz selbstverständlich die Standortdaten nutzen wollen (wichtig für das Einkaufen in den Geschäften!), auf die Kontaktliste oder auf Fotos und Videos zugreifen wollen. Selbst eine scheinbar hamrlose App einer Sparkasse, die ich installieren musste für das Online-Banking, wollte diese und noch mehr Rechte haben. Wozu, bitteschön?!?!

Steckt hinter dieser Nonchalance und Duldsamkeit gegenüber permanent stattfindenden Eingriffen in die Privatsphäre ein im Kapitalismus generierter Fehlglaube, dass **wer dafür bezahlt auch ein Recht darauf hat**?!

Was als Nächstes kommt: Der Zugriff von Polizei und Sicherheitsbehörden auf Daten von Google, Facebook & Co

Der nächste Schritt ist in Fachkreisen schon zu erkennen [B] [C]. Er macht sich (auch) fest an einem kongenialen Wettbewerber der Firma Cambridge Analytica. Der heißt **Palantir** und ist an der Westküste der Vereinigten Staaten ansässig. Hervorgegangen ist Palantir aus ebay und Pay Pal, zwei Internet-Unternehmen, an deren Gründung und Großwerdung der aus Deutschland stammende Peter Thiel maßgeblich beteiligt war. Beide Firmen hatten Probleme mit der Identitätsüberprüfung von Online-Kunden bzw. Zahlungsschuldnern. Palantir wurde daher mit der Aufgabenstellung gegründet und hat entsprechende Software entwickelt, um Daten aus ganz unterschiedlichen Quellen/Datenbanken/Plattformen zusammenzuführen und auswertbar zu machen.

Das war eine Problemstellung, wo sämtliche Sicherheitsbehörden – weltweit – in ganz besonderem Maße der Schuh drückt. In den Behörden gibt es diverse Datenbanken, auf regionaler, bundesländer-, nationaler und supranationaler Ebene. Daneben sind andere Datenquellen interessant, z.B. diverse öffentliche Register etc. Und bei den Polizeibehörden und Nachrichtendiensten träumt man natürlich auch davon, was – wie uns Edward Snowden berichtet hat – die Amerikaner mit **XKEYSTROKE**, PRISM & Co längst können. Profile anlegen über nahezu jeden Menschen – weltweit, solange er nur irgendwo im Telefonverkehr, Email oder beim Chatten, auf Blogs, Foren oder sonstigen Plattformen seine Spuren hinterlassen hat. Palantir sagt, sie hätten dafür eine Lösung. Und verkauft die seit einigen Jahren auch schon erfolgreich an

Sicherheitsbehörden innerhalb und außerhalb der Vereinigten Staaten.

Palantir und seine bisherigen Erfolge bei deutschen Sicherheitsbehörden

Schon 2015 berichtete die Zeit darüber [6], dass Palantir auch beim **Bundesnachrichtendienst** getestet wird. Vor wenigen Wochen erteilte das **Land Hessen** der deutschen Palantir-Tochter den Auftrag für *„Beschaffung und Betrieb einer Analyseplattform für die Polizei Hessen zur effektiven Bekämpfung des islamistischen Terrorismus und der schweren und Organisierten Kriminalität“*. Die eingeschränkte Zweckbestimmung halte ich für Vergabe-Lingo. Dahinter steckt wohl eher ein Pilotprojekt zur Erprobung der Eignung des Palantir-Systems für allgemeine (kriminal-)polizeiliche Zwecke.

So weit ist es schon mit dem Zugriff deutscher Polizeibehörden auf Google, Facebook & Co

Und nun kommen wieder Facebook, Google & Co ins Spiel. Denn den totalen Rundum-Blick auf Bürger, Gefährder und Straftäter erreicht Polizei doch erst dann, wenn sie auch umfassend die Daten *„aus dem Internet“* nutzen darf, also Nutzungsdaten von Google, Facebook & Co. Das halten Sie für weit hergeholt?! Nicht so weit, wie Sie denken: Denn im Entwurf zum neuen bayerischen Polizeiaufgabengesetz [7] ist vorgesehen, dass die Polizei von Telemedienanbietern (= Gesetztext-Lingo für Google, Facebook & Co) *„Auskunft über dort gespeicherte Nutzungsdaten verlangen kann und dass sich dieses Auskunftsverlangen auch auf künftige Nutzungsdaten erstrecken kann.“*

Der bayerische Landesvater, unter dessen Regentschaft dieses Polizeiaufgabengesetz im Bayerischen Landtag eingebracht wurde, wurde soeben Bundesinnen-, Bau- und Heimatminister. Schon im Sommer letzten Jahres haben sein Amtsvorgänger und die Innenminister der Bundesländer auf ihrer Frühjahrstagung beschlossen, eine Arbeitsgruppe einzurichten [D]: Die die Aufgabe hat, ein Musterpolizeigesetz zu erarbeiten, das einheitliche, gemeinsame, gesetzliche Standards in allen Bundesländern für die Arbeit der Polizeibehörden im Rahmen der Gefahrenabwehr definieren soll. Denn Versäumnisse, zuletzt im Fall des Attentäters vom Breitscheidplatz, lagen – so behaupteten es der bisherige Bundesinnenminister De Maizière und seine Gefolgsleute – vor allem daran, dass es in den Ländern unterschiedliche Polizeigesetze gibt. Dieses angebliche Manko soll mit dem neuen einheitlichen Polizeigesetz für alle Länder, für das nun ein Muster erarbeitet wird, überwunden werden.

Die vorgesehene Regelung zu Google, Facebook & Co lässt erkennen, dass mit dem neuen Gesetz noch ganz andere „Mankos“ aus polizeilicher Sicht, weitgehend unbemerkt von Medien und Öffentlichkeit, jedoch zur vollen Zufriedenheit der Polizei behoben werden sollen. George Orwell grüßt aus dem Grab …

In diesem Sinne: Wäre nicht bei jedem von uns im ureigenen persönlichen Interesse ein wenig mehr Zurückhaltung angebracht bei der Nutzung von Google, Facebok & Co?!
Das fragt die Autorin, die zumindest am eigenen Beispiel demonstrieren kann, dass man tatsächlich überleben kann ohne Facebook, Whatsapp, Snapchat, Instagram und zahlreiche Apps auf dem Smartphone.

Fußnoten

[a] Hinter diesem Link erreichen Sie einen Kurztest nach dem OCEAN-Modell in Deutsch

[b] "SCL"/Cambridge Analytica : Das „SCL" ist die Abkürzung für Strategic Communication Laboratories Group und bezeichnet das Mutterunternehmen von Cambridge Analytica. Mehr in diesem Wikipedia-Beitrag

[c] Andere Testverfahren beobachten das Verhalten des Probanden, die Interpretation von Farbklecksen (Rohrschach-Test) u.v.m.. Mehr dazu in diesem Wikipedia-Beitrag

Verwandte Beiträge

[A] Daten als Ware! Voll im Fokus des Springer-Konzerns, 09.03.2018, CIVES
http://cives.de/daten-als-ware-voll-im-fokus-des-springer-konzerns-7339

[B] Der Megatrend in der TECHNIK der Inneren Sicherheit, 13.02.2018, POLICE-IT
https://police-it.org/der-megatrend-in-der-technik-der-inneren-sicherheit

[C] Die Megatrends in der POLITIK der Inneren Sicherheit, 09.02.2018, POLICE-IT
https://police-it.org/die-megatrends-in-der-politik-der-inneren-sicherheit-2018ff

[D] Seehofer's Homeland und die Security, 16..03.2018, POLICE-IT
https://police-it.org/seehofers-homeland-und-die-security

Quellen

[1] Revealed: 50 Million Facebook profiles harvested for Cambridge Analytica in major data breach, 17.03.2018, Observer/Guardian
https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[2] How Trump Consultants Exploited Facebook Data of Millions, 17.03.2018, New York Times
https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

[3] Spätere Trump-Berater sollen 50 Millionen Facebook-Profile illegal ausgewertet haben, 17.03.2018, Spiegel Online
http://www.spiegel.de/netzwelt/web/donald-trump-berater-sollen-millionen-facebook-profile-ausgewertet-haben-a-1198654.html

[4] Suspending Cambridge Analytica and SCL Group from Facebook, 16.03.2018, Facebook
https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/

[5] ‚Big Five (Psychologie)' in Wikipedia, heruntergeladen am 17.03.2018
https://de.wikipedia.org/wiki/Big_Five_(Psychologie)

[6] BND beauftragt CIA-Firmen, 24.06.2015, Zeit Online
http://www.zeit.de/politik/deutschland/2015-06/sap-bnd-bundeswehr-hana

[7] Gesetzentwurf der Staatsregierung für ein Gesetz zur Neuordnung des bayerischen Polizeirechts (PAG-Neuordnungsgesetz), Drs.-Nr. 17/20425, 30.01.2018, Bayerischer Landtag
http://www1.bayern.landtag.de/www/ElanTextAblage_WP17/Drucksachen/Basisdrucksachen/0000013000/0000013038.pdf