Andrea Knaut

Sie haben den Nutzen der Technik noch nicht rational erkannt!

Biometrie verstehen und akzeptieren

„Du hast verdammt nochmal Gemüse zu essen, solange du deine Füße unter meinen Tisch stellst." – So manche Eltern erhoffen sich durch die Erklärung des funktionalen Sinns bestimmter Regeln, die Kinder auf etwas sanftere Weise zu erziehen als mit solchen Befehlen. Sie erhoffen sich allerdings seltener, dass ihr Kind dies als Neunmalklug zum Anlass nimmt, einen differenzierten Disput über den Sinn und Unsinn des Gemüseessens zu beginnen. Mit der Offenlegung aller Details und Hintergründe einer Regel wird nicht ihre Infragestellung bezweckt, sondern die Herbeiführung einer Einsicht in ihre Befolgung.

Die breite Einführung IT-gestützter Überwachungssysteme wird nicht selten in vergleichbarer Weise transparent gestaltet. Im Folgenden wird dies speziell am Beispiel biometrischer Systeme erläutert. Wir kennen sie inzwischen zur Genüge aus dem Alltag, seien es der TouchID-Sensor am iPhone, das Fingerabdrucklesegerät beim Meldeamt oder bei einer Grenzkontrolle, die biometrischen Passbilder für eine automatische Gesichtserkennung usf. Ein biometrisches System dient dem Mustervergleich digitalisierter individueller physiologischer Merkmale, um anhand dieser Menschen automatisch wiederzuerkennen. Manche werden diese Prozeduren nicht allzu sehr mögen und vielleicht soweit wie möglich auf sie verzichten.

Die Marketing-Strateg.innen der Unternehmen oder Politiker.innen, die biometrische Kontrollsysteme in Staaten mit halbwegs funktionierenden Grund- und Freiheitsrechten einführen wollen, sind im Idealfall stärker argumentativ in der Herbeiführung einer breiten gesellschaftlichen Einsicht in den Sinn der Technik gefordert. Eine gesellschaftliche Erziehungsaufgabe muss bewältigt werden.

> *„Fears about a global Big Brother will be* dismissed if end users are educated *about the workings and purpose of the biometric system."*[1]

Erziehungsziele sind, neben der Einsicht in Funktionsweise und Nutzen der Systeme, das Verhindern von Benutzungsproblemen und die Beruhigung der Ängste über einen ungenügenden Umgang mit persönlichen Daten. Statt Angst wird Akzeptanz benötigt. Diese lässt sich nicht nur durch begleitende Aufklärungskampagnen befördern, sondern auch durch ein entsprechendes Systemdesign. Akzeptanz ist hierbei nur ein Baustein eines komplizierten Puzzles. Kontextabhängig gilt es, diesen sinnvoll gegen die Kosten, die möglichen Angriffe auf ein solches System oder gar die Feinde einer biometrischen Anwendung abzuwägen.[2] Eine Leitfrage ist dann, ob es unter Berücksichtigung all dieser Kriterien überhaupt möglich ist, ein passendes System zu finden.

Obwohl biometrische Verifikation – wie die Anmeldung mit TouchID am iPhone –, insofern sie die Passworteingabe obsolet macht, als eine besonders gebrauchstaugliche Authentifizierungstechnologie (*usable security*) gilt, ist die Akzeptanzproblematik noch lange nicht vom Tisch. Selbst grundlegende Anforderungen nach herrschenden Maßstäben von IT-Sicherheit und Datenschutz sind bisher gar nicht oder nur teilweise in der freiwillig nutzbaren Alltagsbiometrie und der hoheitlichen erfüllt. Dazu gehören etwa rückrufbare und verschlüsselte Templates, die Einbettung des Gesamtsystems in eine PKI, eine möglichst lokale Speicherung und Verarbeitung oder die Verknüpfung mit Multi-Faktor-Authentifizierung.[3] Eine bequeme Benutzbarkeit wird bei Erfüllung dieser Anforderungen auch schon schwieriger realisierbar.

Neben der verbrieften Einhaltung von IT-Sicherheitsstandards lässt sich Akzeptanz zusätzlich mit geeigneter Visualisierung biometrischer Prozesse, ihrer Eingaben und Resultate herstellen.

Andrea Knaut

Vor acht, neun Jahren gingen Bilder des Prototyps eines ePass mit flexiblem AMOLED-Display durch die Presse.[4] Die Bundesdruckerei und Samsung hatten ihn in Kooperation produziert und tingelten damit über internationale Computermessen. Inzwischen hat Samsung die Forschung an transparenten OLED-Displays zunächst auf Eis gelegt, da es an Nachfrage mangele.[5] Als wichtiges Argument für den Einsatz von Displays in Passdokumenten nannte Manfred Paeschke, damals Leiter der Innovationsabteilung der Bundesdruckerei GmbH, dass die Transparenz der Technologie auch die gesellschaftliche Akzeptanz von elektronischen Dokumenten steigere. [6]

Gegenwärtig bewirbt die Bundesdruckerei den Mitarbeiterausweis *Go ID!* mit integriertem alphanumerischem Display so:

> *„Ein integriertes Display erleichtert die Nutzung. Dort werden Statusmeldungen und Hinweise angezeigt. So weiß der Inhaber immer, welcher Prozessschritt gerade erfolgt und was er als nächstes tun muss."*[7]

Ebenso bedeutsam aber ist die diskursiv begleitende Aufklärung über den allgemeinen Nutzen der Technik: Biometrie gilt als das Mittel zur Verhinderung der schwerwiegenden Bedrohung durch Identitätsbetrug. Ein historisches Anwendungsfeld ist die negative Identifikation, bei der festgestellt wird, ob ein

und dieselbe Person zum Beispiel unter verschiedenen Namen in einem System registriert ist. Schon der britische Kolonialbeamte William J. Herschel nutzte Fingerabdrücke nach diesem System. Er begann um 1860 herum in der Britischen Ostindien-Kompanie in Bengalen, die an die indischen Angestellten ausgezahlten Pensionen mit einem Fingerabdruck quittieren zu lassen, um doppelten Pensionsbezug zu verhindern.

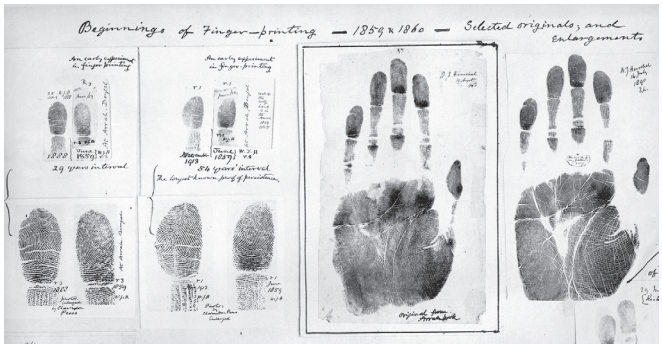

Abbildung 1: Die Anfänge der Daktyloskopie, Experimente mit Fingerabdrücken von William J. Herschel (1833–1917), die er in den Jahren 1859/1860 fertigte

Die koloniale Tradition setzt sich heute ironischerweise fort, wenn automatisierte Fingerabdruckidentifizierungssysteme europäischer Exportschlager für ehemalige Kolonialstaaten sind, wie zum Beispiel das Bank-Verifikations-Nummer-System in Nigeria. Es stammt von der deutschen Firma Dermalog, die auch in Deutschland der wichtigste Hersteller sämtlicher hoheitlicher Biometrie-Systeme ist. Im Auftrag der nigerianischen Regierung realisierte Dermalog das System im Rahmen der landesweiten „Kampagne gegen Korruption und Misswirtschaft [, die …] zur Streichung zahlreicher Stellen von Gehaltslisten des öffentlichen Dienstes [geführt hat]."[8]

Innerhalb der einstmaligen Kolonialmacht Großbritannien genügte der Öffentlichkeit das schwerwiegende Argument der Verhinderung des betrügerischen Mehrfachbezugs staatlicher Leistungen allerdings nicht als Grund für die Einführung einer *National Identity Card*. Die schon in die 1990er zurückreichende Idee wurde unter Blair mit dem *National Identity Card Act 2006*, mit dem auch ein zentrales *National Identity Register* geschaffen werden sollte, gesetzlich verankert. In dem Register sollten unter anderem biometrisch verwertbare Finger- und Gesichtsdaten abgelegt werden, die auch auf der Karte gespeichert würden. Als es 2007 einen Regierungswechsel zu der von den Konservativen geführten Koalition mit den Liberaldemokraten unter Premierminister Cameron gab, wurde das Gesetz in großen Teilen wieder einkassiert. Obwohl es in der Umbruchphase 2009 noch Versuche gab, das Projekt zu retten, gilt es heute als gescheitert.[9] Geblieben ist die im *UK Borders Act 2007* vorgesehene *Biometric Residence Permit* für Immigrant.innen, die nicht aus dem Europäischen Wirtschaftsraum kommen.[10] Prinzipiell bleibt die Karte damit infrastrukturell verankert, betrifft aber nur die, die sich ihr wohl am wenigsten widersetzen dürften.

Die National Identity Card gilt nichtsdestotrotz als eines der wenigen Beispiele, bei denen massiver öffentlicher Druck für das Scheitern eines nationalen biometrischen Ausweisprojekts entscheidend war. Hat hier also eine überwachungspolitische Lobbyarbeit mit angemessener „Transparenzrhetorik" versagt? Aaron K. Martin kam in einer diskursanalytischen Untersuchung des Falls zu dem Schluss, dass es das Fehlen einer sogenannten *organizing vision* war, die das Projekt zum Kippen brachte.[11] „Organizing visions function to mobilize actors for the purposes of materializing an innovation."[12] In diesem Fall fehlte es an einem Leitbild, das die Firmen, die dem Home Office helfen sollten, das *National Identity Scheme* zu bauen, die Einrichtungen des öffentlichen Dienstes, die die Technologie dann breit nutzen sollten, sowie die Öffentlichkeit unter einen Hut brachte. Martin benennt verschiedene politstrategische Verfehlungen in der Entwicklung. Dazu gehört, dass der fast einzige diskursive Fokus der Regierung auf dem logistischen Problem des massenhaften Enrolments und dem Bedarf an öffentlichen Ressourcen lag: Wie könne man doppelte Enrolments verhindern? Wie würde wirklich die gesamte Bevölkerung abgedeckt? Es gab dagegen kaum Verlautbarungen darüber, wie Organisationen die neue Karte nutzen würden und welche Probleme sie genau lösen würde. Außerdem kam es nie zu einem Large-Scale-Deployment. Nur 14.670 Briten hatten sich bis 2009 freiwillig erfassen lassen. Davon erhielten 3.000 auf Flughäfen kostenlose Karten und viele weitere waren mobilisierte Mitarbeiter des öffentlichen Dienstes. Die Politik versagte darin, möglichst viele Organisationen zu involvieren. Es formierte sich ein wirkungsvoller medialer Diskurs einer Opposition gegen die Karte. Dieser gelang es, auch im Appell an die national verankerten Gedanken von *citizenship, freedom and identity*[13] ausreichend Ängste zu schüren, dass die Regierung unschuldige Bürger.innen verfolgen und ihre Privatsphäre bedrohen würde. Eine wichtige Rolle in der öffentlichen Debatte spielten zudem an die Öffentlichkeit durchgesickerte Home-Office-Dokumente.

Auch in Deutschland ist der biometrische Teil des elektronischen Personalausweises bekanntermaßen bisher wenig erfolgreich, obwohl „die eingebaute Sicherheitstechnik gar nicht mal so schlecht" sei, schreibt Merkert 2016 in der c't. Verschlüsselungs- und Zertifizierungsarchitektur sind technisch gut überlegt, stattdessen aber habe das Bundesamt für Sicherheit in der Informationstechnik (BSI) „wirtschaftliche und gesellschaftliche Aspekte ignoriert."[14] So seien die Lesegeräte und die Zertifikate nach wie vor zu teuer, und die Software litt lange unter schlechter Wartung.

In bestimmten Anwendungsbereichen der Biometrie hat die Industrie weniger Überzeugungsarbeit nötig. Sind die von der biometrischen Erfassung betroffenen Personen sowieso schon weitestgehend rechtlos, wie es bei Asylbewerber.innen oder ohne gültige Papiere Aufgegriffenen der Fall ist, greift Biometrie am offensichtlichsten als autoritäres Instrument automatisierter Ressourcenverweigerung. Ein schon lange etabliertes Beispiel ist das automatische Fingerabdruckidentifizierungssystem Eurodac, das das Dubliner Übereinkommen umsetzen soll, nach dem der EU-Staat für einen Asylantrag zuständig ist, in den ein.e Asylbewerber.in zuerst einreist. In den verschiedenen Eurodac-Verordnungen wurden und werden zwar theoretisch im Rahmen der Datenschutzgesetzgebung der Europäischen Union Auskunftsrechte gewährt,[15] doch kaum eine.r nimmt sie in Anspruch. 2014 wurden bei 2,7 Mio. gespeicherten biometrischen Datensätzen lediglich 26 Abfragen im Sinne des Auskunftsrechts gestellt (2012: 111 bei 2,3 Mio. Datensätzen, 2013: 49 bei 2,4 Mio. Datensätzen).[16] Die Konsequenzen eines Eurodac-Treffers – Rückschiebung, menschenunwürdige Inhaftierung oder

Abschiebung – können lebensgefährlich sein. Doch greift der Schutz bürgerlicher Rechte nicht, ist die Akzeptanz der Technik nachrangig.

Als 2013 die neue Eurodac-Verordnung auch den Zugriff der Strafverfolgungsbehörden auf die Datenbank legalisierte, protestierten beispielsweise EU-Parlamentsabgeordnete der Grünen/Europäischen Freien Allianz gegen diesen schon frühzeitig von Kritiker.innen des Systems vorausgesagten Function Creep.[17]

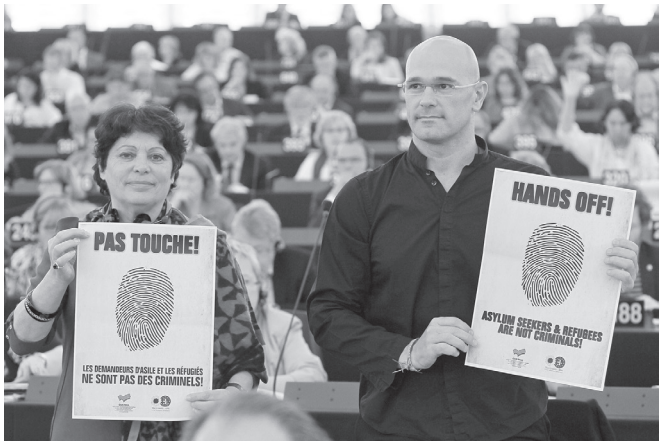

Abbildung 2: Finger weg! Asylbewerber.innen sind keine Kriminellen! – Proteste von EU-Parlamentsabgeordneten der Grünen/EFA gegen die Ausweitung der Zugriffs auf Eurodac für Strafverfolgungsbehörden, 12.6.2013

Die europäische Anti-Einwanderungspolitik bietet weiterhin das beste Testfeld für eine Überwachungsbiometrie, die kaum einer Rechtfertigung gegenüber ihren Usees bedarf und deren begleitende Auskunftsrechte nur noch in den Händen sehr standhafter Bürgerrechtler.innen zur Stärkung der Beweisfindung in einzelnen Rechtsverfahren von Nutzen sein dürften.

Bis hierher wurden beispielhaft verschiedene Strategien diskutiert, die Nutzer.innen Ängste vor einer vermeintlich falsch verstandenen Überwachungstechnik nehmen oder sie vor negativen Auswirkungen schützen sollen. Auf diese Weise können zwar durchaus transparentere Sicherheitssysteme entstehen, die allen Beteiligten mehr nutzen als schaden. Dies ist aber auch nur dann der Fall, wenn sie eben nicht allein als ein Instrument der Marktakzeptanz eines technischen Produkts dienen, sondern in Kauf genommen wird, dass es möglicherweise nie zu einer Markteinführung kommt. Denn ein sichtbar gemachtes Unrechtssystem bleibt ein Unrechtssystem. Informationelle Transparenz oder Sichtbarmachung erleichtert zwar erheblich die Wahrheitsfindung, ersetzt jedoch kein Urteil.

Anmerkungen

1 *Hervorhebung durch Autorin. Gary Roethenbaugh: »Truths and Myths« about biometric technologies. In: Biometrics explained. International Computer Security Association (ICSA), 1998, https://web.archive.org/web/19980529094811/http://www.icsa.net/services/consortia/cbdc/explained.htm (22.2.2017). Auf dem Text basieren große Teile des Biometrics Tutorial der ISO/IEC SC37 von 2007.*

2 *Ruud M. Bolle et al.: Guide to Biometrics. Springer: New York, 2004, p. 10.*

3 *Stefan G. Weber: Alltagstaugliche Biometrie: Entwicklungen, Herausforderungen und Chancen. iit perspektive Nr. 21, 2014.*

4 *Jens Ihlenfeld: ePass mit AMOLED-Display zeigt Bewegtbilder. golem.de, 21.5.2008, http://www.golem.de/0805/59848.html (23.2.17) und Detlef Borchers: Bundesdruckerei und Samsung kooperieren bei „3D"-Ausweisen. heise online, 11.12.2008, https://heise.de/-188949 (23.2.17).*

5 *Kim Young-won: Samsung Display stops producing transparent OLED. 26.8.2016, http://www.koreaherald.com/view.php?ud=20160826000325 (23.2.17).*

6 *omnisecure: Bundesdruckerei-Mitarbeiter für Innovationspreis Berlin-Brandenburg nominiert. 29.10.2007, https://www.omnisecure.berlin/de/news-pcb/unternehmen-pcb/1101-bundesdruckerei-mitarbeiter-fuer-innovationspreis-berlin-brandenburg-nominiert (23.2.17).*

7 *Bundesdruckerei GmbH: CeBIT: Bundesdruckerei zeigt Mitarbeiterausweis der Zukunft. 13.3.2015 https://www.bundesdruckerei.de/de/3865-cebit-bundesdruckerei-zeigt-mitarbeiterausweis-der-zukunft (22.02.17).*

8 *Dermalog: Bekämpfung von Identitätsbetrug. 8.3.2016, http://www.dermalog.com/de/news/de_Nigeria_2016.php (23.2.17).*

9 *Mit dem Identity Documents Act 2010 wurde die Gültigkeit der National Identity Card als offizielles Identitätsdokument außer Kraft gesetzt.*

10 *UK Visas and Immigration: Biometric residence permits: general information for applicants, employers and sponsors. July 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/539328/In-Country_information_leaflet_.-_July_2016.pdf (23.02.17).*

11 *Aaron K. Martin: National Identity Infrastructures. Lessons from the United Kingdom. In: ICT Critical Infrastructures and Society. Springer: Berlin, Heidelberg, 2012, pp. 44–55.*

12 *ebd., S. 51*

13 *ebd., S. 53*

14 *Johannes Merkert: Kontaktlos – nutzlos. Warum der neue Personalausweis auch nach fast sechs Jahren nicht durchstartet. In: c't 18/2016.*

15 *EU-VO 2725/2000, Art. 18 und EU-VO 603/13, Art. 29.*

16 *eu-LISA: Annual reports in the activities of the Central Unit of Eurodac, 2013, 2014, 2015.*

17 *Ska Keller: Neues europäisches Asylsystem. Stigmatisierung von Flüchtlingen als Kriminelle. 12.6.2013, http://www.gruene-europa.de/neues-europaeisches-asylsystem-10041.html (23.2.2017). Zum Function Creep siehe auch: Elif Mendos Kuşkonmaz: The Eurodac Debate: Is It Blurring the Line Between Asylum and Fight Against Terrorism? In: Annales de la Faculté de Droit d'Istanbul. 2013. S. 79–102, http://dergipark.gov.tr/download/article-file/7072 (23.2.2017).*

CC BY

Andrea Knaut

Andrea Knaut ist Informatikerin und hat ihre Dissertation zum Thema *Fehler und Benutzungsprobleme von Fingerabdruckerkennungssystemen im gesellschaftlichen Kontext* geschrieben. Als wissenschaftliche Mitarbeiterin hat sie mehrere Jahre an der Humboldt-Universität zu Informatik und Gesellschaft und der Didaktik der Informatik geforscht und gelehrt. Sie ist aktiv in der Fachgruppe *Internet und Gesellschaft* der Gesellschaft für Informatik e. V. und Mitglied des FIfF e. V.