VISCHER

Das neue Datenschutzgesetz.
So klappt die Zweitverwertung von Personendaten

David Rosenthal, Partner, VISCHER AG
6. September 2023

Drei Beispiele

- Eine Bank wertet die Zahlungsempfänger ihrer Kunden inhaltlich aus, um gestützt darauf Marketingmassnahmen für sich und Dritte zu steuern
- Ein Finanzinstitut will Datensätze seiner Kunden von einem Dritten in dessen "Clean Room" mit Angaben über das Einkaufsverhalten derselben Kunden auf fremden Online-Portalen anreichern, um Muster zu identifizieren, die ein präziseres Profiling von Kunden ermöglichen
- Eine Bank will Kundengespräche aufzeichnen und von einer KI transkribieren lassen, um damit KI-Modelle aufzubauen, mit denen Kundengespräche automatisiert von einer KI geführt werden können

Ist eine solche Sekundärnutzung erlaubt?

- Die kurze Antwort für das Schweizer Datenschutzrecht (DSG)
  - Zu nicht personenbezogenen Zwecken meistens ja
  - Zu personenbezogenen Zwecken meistens nur mit rechtzeitiger Ankündigung oder sonst Einwilligung
- Personenbezogener Zweck?
  - Beispiel der Auswertung der Kundendaten
  - Kundschaft besser verstehen = nicht personenbezogener Zweck
  - Einzelne Kunden besser ansprechen = personenbezogener Zweck
- Sekundärnutzung erlaubt? → mehrstufige Prüfung erforderlich

Schritt 1: Liegen überhaupt Personendaten vor?

- Datenschutzrecht gilt nur für Personendaten
  - Ist für ein Unternehmen und seine Mitarbeiter ein Rückschluss auf eine natürliche Person möglich?
  - Auch nicht indirekt aufgrund von weiteren Quellen (Internet, Datenbanken etc.), an deren Einsatz ein Interesse bestehen könnte?
  - Falls nicht: Keine Personendaten *für dieses Unternehmen*
  - Für andere oder in Zukunft vielleicht schon, deshalb müssen die Daten geheim gehalten, geschützt und ggf. gelöscht werden

"relativer Ansatz"

- Anonymisierung vs. Pseudonymisierung
  - Anonymisiert sind Daten nur, wenn *keiner* re-identifizieren kann
  - Rein theoretische Möglichkeit zählt allerdings nicht

Anonym?

10-02-14 | FAST FEED

NYC Taxi Data Blunder Reveals Which Celebs Don't Tip–And Who Frequents Strip Clubs

By cross-referencing de-anonymized trip data with paparazzi photos, a privacy research could tell how much Bradley Cooper paid his driver.

[PHOTO: FLICKR USER PAULTOM2104]

Diverse Techniken

- Maskierung von Daten (z.B. durch Substitution, Mischen, Variationen von Zahlen und Daten, Verschlüsselung, Nullung oder Löschen, Schwärzen)
- Generalisierung (z.B. Altersbereiche)
- Aggregierung
- Hinzufügen von Rauschen

Diverse Messgrössen

- k-Anonymität
- l-Diversität
- t-Closeness

Quelle: www.fastcompany.com [https://bit.ly/3bssrB9] (2014)

Schritt 2: DSG-Vorgaben zur Zweitnutzung erfüllt?

- Daten müssen zulässigerweise vorliegen
- Zweck der Zweitnutzung muss bei der Beschaffung erkennbar oder damit vereinbar sein *[= neu]*
- Zweck der Zweitnutzung muss in der Datenschutzerklärung zum Zeitpunkt der Beschaffung aufgeführt sein *[= neu]*
  - Beschaffung ist die planmässige Erhebung der Daten, die auch nachträglich in internen Beständen (= indirekt) erfolgen kann
- Verhältnismässige Nutzung (d.h. nur, was nötig, sinnvoll und zumutbar ist → Datenminimierung und zeitliche Begrenzung)
- Keine Weitergabe besonders schützenswerter Personendaten an einen Dritten und die Person hat nicht widersprochen (Opt-out)

Darf angesichts des Primärzwecks nicht "unerwartet, unangebracht oder beanstandbar" sein

Macht sie auch erkennbar

Hierfür sieht das Gesetz gewisse Ausnahmen vor

Schritt 3: Ist die Zweitnutzung gerechtfertigt?

- Durch Einwilligung (z.B. im Rahmen eines Vertrags)
  - Anders als unter der DSGVO ist die Weiternutzung auch nach einem Rückzug denkbar (Vertrag, überwiegendes Interesse)
- Durch überwiegendes privates Interesse (Art. 31 revDSG)
  - z.B. für nicht personenbezogene Zwecke wie Forschung, Planung, oder Statistik, unter folgenden Bedingungen (Abs. 2 Bst. e):
    - Anonymisierung so bald wie möglich (ausser wo unmöglich oder mit einem unverhältnismässigen Aufwand verbunden)
    - Besonders schützenswerte Personendaten nur anonym an Dritte; wo nicht möglich, reichen andere Schutzmassnahmen
    - Keine Personendaten in den publizierten Ergebnissen

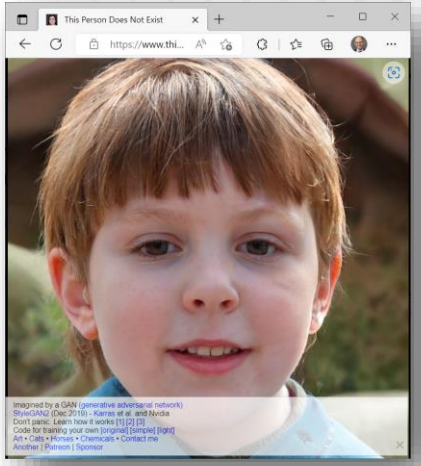
Nur relevant, falls die vorstehenden Vorgaben nicht eingehalten werden können (exkl. DSE)

Neu im revidierten DSG

Praxisbeispiel "Clean Room"

- Unternehmen A und B haben jeweils Daten über registrierte Benutzer
- Beide verschlüsseln den Identifier (z.B. E-Mail) auf dieselbe Art und Weise, so dass Datensätze, welche von denselben Benutzern stammen, "gematcht" werden können
- A und B geben ihre Datensätze dem Dienstleister C, der die Daten matcht, die Identifier aber nicht entschlüsseln kann
- Der Dienstleister C analysiert die kombinierten Daten und erstellt daraus Modelle, mit denen Prognosen möglich sind; diese und nur diese gibt er A und B
- Wesentlich: Die Modelle müssen so sein, dass weder A noch B Rückschlüsse auf Daten des jeweils Anderen ziehen kann

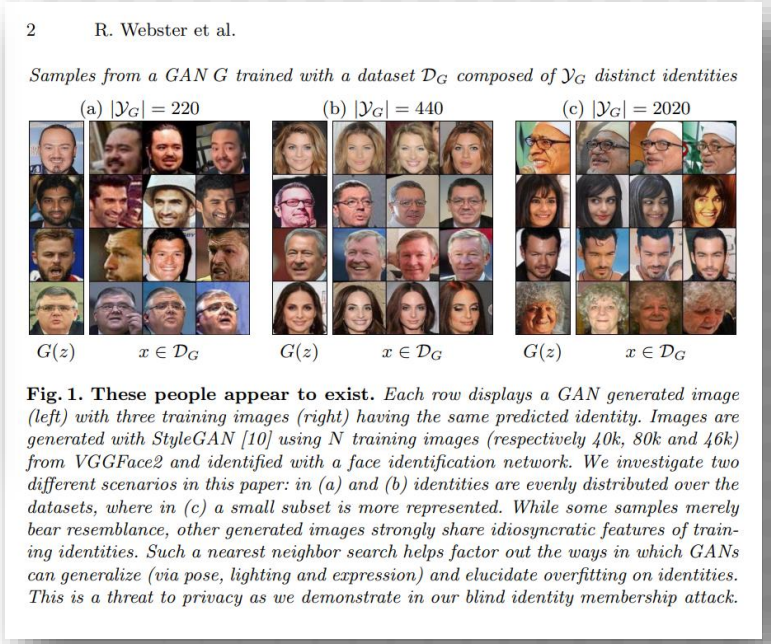
KI-Modelle als Sammlung von Personendaten?



this-person-does-not-exist.com

This person does ~~not~~ exist?

Wirklich keine Personendaten?



2 R. Webster et al.

Samples from a GAN G trained with a dataset $\mathcal{D}_G$ composed of $\mathcal{Y}_G$ distinct identities

(a) $|\mathcal{Y}_G| = 220$ (b) $|\mathcal{Y}_G| = 440$ (c) $|\mathcal{Y}_G| = 2020$

$G(z)$ $x \in \mathcal{D}_G$ $G(z)$ $x \in \mathcal{D}_G$ $G(z)$ $x \in \mathcal{D}_G$

Fig. 1. These people appear to exist. *Each row displays a GAN generated image (left) with three training images (right) having the same predicted identity. Images are generated with StyleGAN [10] using N training images (respectively 40k, 80k and 46k) from VGGFace2 and identified with a face identification network. We investigate two different scenarios in this paper: in (a) and (b) identities are evenly distributed over the datasets, where in (c) a small subset is more represented. While some samples merely bear resemblance, other generated images strongly share idiosyncratic features of training identities. Such a nearest neighbor search helps factor out the ways in which GANs can generalize (via pose, lighting and expression) and elucidate overfitting on identities. This is a threat to privacy as we demonstrate in our blind identity membership attack.*

https://arxiv.org/pdf/2107.06018.pdf

Diverse Methoden zur Extraktion von Personendaten aus angeblich anonymen KI-Modellen z.B. durch "Membership Inference Attacks"

Erkenntnis: KI-Modelle sind nicht per se anonym

Eine Lösung: Differential Privacy

Praxisbeispiel "Kundengespräche"

- Aufzeichnung von Gesprächen erfordert so oder so Einwilligung (Art. 179ter StGB)
- Nutzungszweck der Bearbeitung (d.h. der Transkription und des Trainings der KI) muss grundsätzlich angekündigt werden
- Kein personenbezogener Zweck, daher Rechtfertigung denkbar, schränkt die Verwendung der Daten aber ein (Anonymisierung)
- Korrekter Einbezug etwaiger Dienstleister, auch im Hinblick auf das Bankgeheimnis; auch an Datenschutzerklärung denken
- Sicherstellen, dass aus dem KI-Modell keine Daten von identifizierbaren Kunden extrahiert werden können, auch nicht durch Angreifer mit Vorwissen über diese Kunden

Schritt 4: Andere Grenzen?

Quellen: techcrunch.com, cryptopolitan.com

- Vertragliche Regelungen
  - NDAs, welche die zweckentfremdete Nutzung von (allen) Daten verbieten
  - Bankgeheimnis i.d.R. kein Hindernis
- Gefühlter Datenschutz
  - Selbst eine datenschutzrechtlich an sich zulässige, Nutzung kann sozial nicht akzeptiert und "gefühlt" den Datenschutz verletzen
    - z.B. bei Versilberung von Daten, Angst um Privatsphäre
  - Öffentliche Meinung zählt – Missbrauchspotenzial und negative Publicity hat viel Gewicht, aber Gewöhnung führt zur Akzeptanz
  - Sanktionierung der Verletzung: Medienecho, Shitstorm, Boykotte, behördliche Untersuchung, Vertragsfolgen

Abo

Postfinance droht Online-Kunden mit dem Rauswurf

Die Post-Tochter will ein neues Schnäppchenportal aufbauen. Doch zuerst müs

Von Matthias Pfa
Aktualisiert:

Mittwoch, 3. Juni 2015

Zahlungsverkehrsdaten: Postfinance krebst zurück

Letzten Herbst kündigte die Postfinance an, die Zahlungsverkehrsdaten aller Kunden auszuwerten und ihnen entsprechende Angebote von Drittfirmen anbieten. Sie änderte hierfür ihre Teilnahmebedingungen und wollte die Nutzer des Onlinebanking-Portals E-Finance zwingen, diesen zuzustimmen, indem sie die Weiterführung der Onlinebanking-Vertrags von der Zustimmung abhängig machte.

Die Stiftung für Konsumentenschutz schritt engergisch ein und stellte den Postfinance-Kunden einen Musterbriefe zur Verfügung, um sich die Auswertung ihrer persönlichen Zahlungsverkehrsdaten zu wehren.

Nach Verhandlungen mit der Datenschutzbehörde (EDÖB) muss die Postfinance nun zurückkrebsen: **Sie darf die Zustimmung zur Auswertung der Zahlungsverkehrsdaten nicht von der Zustimmung zu den Teilnahmebedingungen abhängig machen.** Alle Kundinnen und Kunden, die den neuen Teilnahmebedingungen fürs E-Finance im Herbst bereits zugestimmt haben, werden ausdrücklich angefragt, ob sie in Zukunft Angebot von Dritten erhalten möchten oder nicht.

Je stärker ein Anbieter in der Öffentlichkeit steht, desto wichtiger ist der gefühlte Datenschutz

Quellen: tagesanzeiger.ch, konsumentenschutz.ch

Zweitnutzungen sind oft zulässig, aber sie müssen richtig verpackt und verkauft werden.

VISCHER

Danke für Ihre Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com

Kontakt

David Rosenthal
Partner, Head Data & Privacy,
VISCHER AG

drosenthal@vischer.com

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, “SIX”) for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.