VISCHER

La nouvelle loi sur la protection des données.

C’est ainsi que fonctionne l’utilisation secondaire de données personnelles

David Rosenthal, Partner, VISCHER AG
mercredi 6 septembre 2023

Trois exemples

- Une banque évalue les créanciers de ses clients en ce qui concerne leur contenu, afin de piloter des mesures de marketing pour elle-même et pour des tiers
- Un établissement financier souhaite compléter les données de ses clients provenant d'un tiers dans son «Clean Room» avec des informations sur le comportement d’achat des mêmes clients sur des portails en ligne externes, afin d’identifier des modèles permettant un établissement de profils plus précis de ceux-ci
- Une banque veut enregistrer les conversations des clients et les faire transcrire par une IA afin de construire des modèles d’IA permettant d’automatiser les conversations des clients par une telle IA

Une telle utilisation secondaire est-elle autorisée?

- La réponse succincte pour la loi suisse sur la protection des données (LPD)
  - À des fins non personnelles, la plupart du temps oui
  - À des fins personnelles, habituellement seulement avec un préavis en temps opportun ou sinon avec consentement
- Objectif à caractère personnel?
  - Exemple d'évaluation des données client
  - Mieux comprendre les clients = objectif non personnel
  - Mieux interpeller les clients individuels = objectif personnel
- Utilisation secondaire autorisée? → vérification multiniveau requise

Étape 1: S'agit-il en fait de données personnelles?

- La loi sur la protection des données ne s'applique qu'aux données personnelles
  - Est-il possible pour une entreprise et son personnel de tirer des conclusions sur une personne physique?
  - Également pas indirectement sur la base d'autres sources (Internet, bases de données, etc.), dont un intérêt pourrait exister dans leur engagement?
  - Si ce n'est pas le cas: aucune donnée personnelle *pour cette entreprise*
  - Pour d'autres, ou peut-être déjà à l'avenir, les données doivent donc être gardées secrètes, protégées et, si nécessaire, effacées

} «approche relative»

- Anonymisation versus pseudonymisation
  - Les données ne sont anonymisées que si *personne* ne peut les réidentifier
  - Cependant, la possibilité purement théorique ne compte pas

Anonyme?

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]

Diverses techniques

- Masquage des données (par exemple par substitution, mélange, variation des nombres et des données, cryptage, mise au neutre ou suppression, caviardage)
- Généralisation (p. ex. tranches d'âge)
- Agrégation
- Ajout de «bruit»

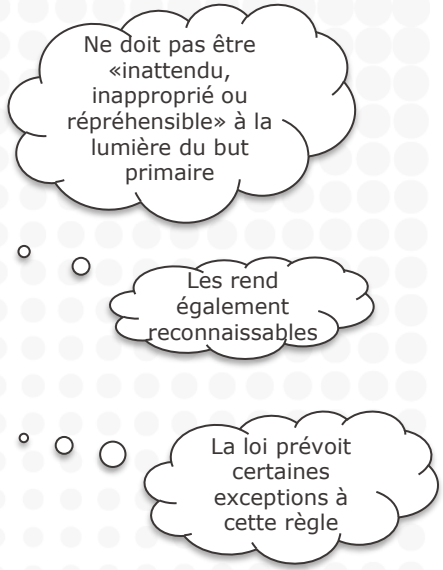
Mesures diverses

- l-Anonymat
- I-Diversité
- t-Closeness

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

Étape 2: Exigences LPD pour l'utilisation secondaire remplies?

- Les données doivent exister de manière admissible
- La finalité de l'utilisation secondaire doit être reconnaissable lors de la collecte ou compatible avec celle-ci *[= nouveau]*
- La finalité de l'utilisation secondaire doit être mentionnée dans la déclaration de confidentialité au moment de la collecte *[= nouveau]*
  - La collecte est le relevé planifié de données, qui peut également être effectuée rétrospectivement dans les états internes (= indirectement)
- Utilisation proportionnelle (c'est-à-dire seulement ce qui est nécessaire, judicieux et raisonnable → minimisation des données et limitation dans le temps)
- Aucune retransmission de données personnelles sensibles à un tiers et la personne concernée ne s'y est pas opposée (opt-out)



Étape 3: L'utilisation secondaire est-elle justifiée?

- Par consentement (par exemple dans le cadre d'un contrat)
  - Contrairement au RGPD, l'utilisation secondaire est également envisageable après une résiliation (contrat, intérêt prépondérant)
- Par un intérêt privé prépondérant (art. 31 nLPD)
  - par exemple, à des fins non personnelles, comme la recherche, la planification ou les statistiques, dans les conditions suivantes (al. 2, let. e):
    - Anonymisation dès que possible (sauf si impossible ou avec un effort disproportionné)
    - Données personnelles sensibles uniquement anonymement à des tiers; lorsque cela n'est pas possible, d'autres mesures de protection doivent y suffire
    - Aucune donnée personnelle dans les résultats publiés

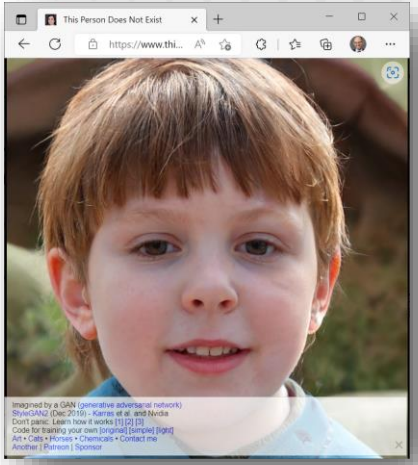
Pertinent uniquement si les spécifications précitées ne peuvent pas être respectées (sauf DSE)

Nouveau dans la LPD révisée

Exemple tiré de la pratique «Clean Room»

- Les sociétés A et B possèdent chacune des données sur les utilisateurs enregistrés
- Les deux chiffrent l'identifiant (par exemple, l'e-mail) de la même manière, de sorte que les enregistrements provenant des mêmes utilisateurs puissent être «mis en correspondance»
- A et B remettent leurs enregistrements au fournisseur de services C, qui met en correspondance les données, mais ne peut pas en déchiffrer l'identifiant
- Le fournisseur de services C analyse les données combinées et les utilise pour créer des modèles permettant de faire des prévisions; il transmet ceci, et seulement ceci à A et B.
- Essentiel: les modèles doivent être tels que ni A ni B ne puissent tirer de conclusions sur les données de l'autre

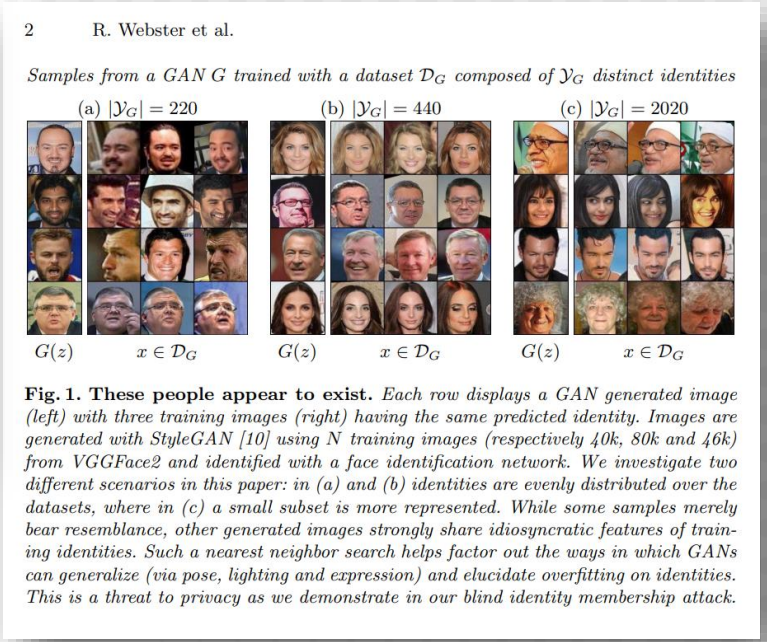
Modèles d'IA en tant que recueil de données personnelles?



this-person-does-not-exist.com

This person does ~~not~~ exist?

Vraiment pas de données personnelles?



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

Divers procédés d'extraction de données personnelles à partir de modèles d'IA censément anonymes, par exemple par des «Membership Inference Attacks»

Enseignement: les modèles d'IA ne sont pas anonymes en soi

Une solution: Differential Privacy

Exemple tiré de la pratique «Entretiens avec la clientèle»

- L'enregistrement de conversations nécessite le consentement d'une manière ou d'une autre (art. 179ter CP)
- Le but du traitement (c'est-à-dire la transcription et l'entraînement de l'IA) doit toujours être annoncé
- Aucune finalité personnelle, donc justifiable, mais limite l'utilisation des données (anonymisation)
- Implication correcte de tout prestataire de services, y compris en ce qui concerne le secret bancaire; envisager également la déclaration de confidentialité
- S'assurer que les données ne peuvent pas être extraites du modèle d'IA à partir de clients identifiables, même par des attaquants ayant des connaissances préalables de ces clients

Étape 4: D'autres limites?

Sources:
techcrunch.com,
cryptopolitan.com

- Réglementations contractuelles
  - NDA (Non Disclosure Agreement) interdisant l'utilisation détournée de sa destination première de (toutes) données
  - Le secret bancaire n'est généralement pas un obstacle
- Protection des données ressentie
  - Même une utilisation qui est autorisée par la loi sur la protection des données en soi ne peut pas être socialement acceptée et est «ressentie» comme une violation de la protection des données
    - par exemple, dans le cas de la commercialisation de données, la crainte pour la vie privée
  - L'opinion publique compte – le potentiel d'abus et de publicité négative a beaucoup de poids, mais l'accoutumance conduit à l'acceptation
  - Sanction de la violation: écho médiatique, déferlement de commentaires haineux, boycotts, enquête officielle, conséquences contractuelles

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.

Plus un prestataire est fort dans le public, plus la protection des données ressentie est importante

Sources: tagesanzeiger.ch, konsumentenschutz.ch

Les utilisations secondaires sont souvent permises, mais elles doivent être correctement intégrées et vendues.

VISCHER

Merci de votre attention!

Pour toute question: 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

Contact

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.