DIGITALE | GESELLSCHAFT

Totalrevision des Datenschutzgesetzes (November 2019)

Beispiele zum Profiling und zu Datenverlusten

Cambridge Analytica (Beeinflussung; potenziell 87 Millionen betroffene Personen)

Über eine Facebook-App haben im Jahr 2014 etwa 270'000 Menschen an einem Persönlichkeitstest mitgemacht und mit der Nutzung der App der Verwendung Ihrer Facebook-Daten zugestimmt.

Facebook hat den Betreibern dieser App aber nicht nur Zugang zu den Persönlichkeitsprofilen der Benutzer dieser App gegeben, sondern auch zu den persönlichen Daten ihrer Facebook-Freunde. Betroffen waren 87 Millionen Menschen, die davon nichts wussten und von denen die meisten sicher auch keine Einverständniserklärung gegeben hätten, wären sie explizit danach gefragt worden. «Zugestimmt» hatten sie allerdings im rechtlichen Sinne, einfach durch die mit der Nutzung von Facebook einhergehenden Akzeptanz der AGB.

Diese Persönlichkeitsprofile wurden an Cambridge Analytica verkauft, die nach eigenen Angaben daraus Attribute wie sexuelle Orientierung, Ethnizität, religiöse und politische Ansichten oder Drogensucht präzise voraussagen konnte. Diese «psychographischen Profile» benutze Cambridge Analytica, um mittels auf einzelne Individuen zugeschnittene politische Werbebotschaften den US-Präsidentschaftswahlkampf 2015/2016 für Donald Trump sowie die Brexit-Abstimmung im UK für die «Leave.EU» Kampagne zu beeinflussen. [1, 2]

Einige Lehren, die aus diesem Skandal gezogen werden müssen:

- Eine Einwilligung zur Nutzung von persönlichen Daten zum Profiling muss informiert, freiwillig und ausdrücklich erfolgen.
- Auch Daten aus einer einzelnen Quelle können ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen. Eine Unterscheidung des Risikos – bei einem risikobasierten Ansatz – ist nicht einfach vorzunehmen.
- Die geplante Übernahme des sogenannten Marktortprinzips ist die Voraussetzung, damit auch ausländische Unternehmen zur Rechenschaft gezogen werden können, wenn sich Sachverhalte in der Schweiz auswirken (Art. 2a Abs. 1; Beschluss Nationalrat).
- Die Prinzipien «Datenschutz durch Technik» und «datenschutzfreundliche Voreinstellungen» müssen ins Datenschutzgesetz (wie in Art. 6 vorgesehen) übernommen werden.

Equifax (Kreditauskunft; Verlust von 143 Millionen Personendaten)

Der Firma Equifax wurden 2017 die persönlichen Daten von 143 Millionen US-Einwohnerinnen und Einwohner gestohlen. Die Unternehmung war zu diesem Zeitpunkt die grösste Kreditauskunftsfirma in den USA und vielleicht sogar der Welt. Die gestohlenen Daten umfassten die Namen, Sozialversicherungsnummern, Geburtsdaten, Adressen und Führerscheindaten. Solche Daten können von Kriminellen verwendet werden, um Identitätsdiebstahl zu begehen, d.h. unter der (angenommenen) Identität der Betroffenen Transaktionen durchzuführen. [3]

Der Datendiebstahl wurde ermöglicht, weil es Equifax versäumte, eine Angriffsstelle (im Apache Struts Framework) zu schliessen, obwohl diese Behebung (Patch) bereits zwei Monate vor dem Diebstahl publiziert wurde. Die Firma zahlte in einer aussergerichtlichen Einigung bis zu 700'000 Dollar Bussgeld. [4]

Es gibt eine Reihe von Lehren aus diesem Vorfall. Die wichtigsten davon sind:

- Viele der riesigen Datensammlungen werden früher oder später gestohlen.
- Datensicherheit ist kostspielig und aufwändig – und wird daher oft vernachlässigt. Für fahrlässige Datenverluste und Datenschutzverstösse müssen daher empfindliche Strafen (für die Firmen, nicht für Mitarbeiter!) verhängt werden können.
- Daten, welche nicht gesammelt werden, können auch nicht gestohlen werden: Datenvermeidung und Datensparsamkeit sind daher wichtige Datenschutz-Prinzipien.

Swisscom (Verlust von 800'000 «nicht besonders schützenswerten» Personendaten)

Unbekannte haben sich im Herbst 2017 Zugang zu Daten über 800'000 Kundinnen und Kunden von Swisscom verschafft. Die Unternehmung spricht im Anschluss euphemistisch von verschärften Sicherheitsmassnahmen für Kundenangaben und betont, dass es sich nicht um «besonders schützenswerte Personendaten» handelte. Abhanden kamen Vor- und Nachname, Wohnadresse, Geburtsdatum und Telefonnummer der Betroffenen. [5]

Wie bei Equifax gilt:

- Der Stellenwert von Datenschutz und Datensicherheit muss auch in der Schweiz erhöht werden.

Schweizer Verlage erstellen Persönlichkeitsprofile ihre Leserinnen und Leser

Die Schweizer Verlage führen schrittweise einen Login-Pflicht ein. Damit wollen sie das Geschäftsmodell von Google, Facebook & Co. kopieren – und die Persönlichkeitseigenschaften ihrer Leserinnen und Leser zu Geld machen. Die Absicht ist, personalisierte Werbung sowie personalisierter Inhalt auszuspielen.

Dies bedeutet, dass jeder Leserin und jedem Leser unterschiedliche algorithmisch ausgewählte Inhalte präsentiert werden, welche auf die vermuteten Interessen zugeschnitten sind. Dies droht, bestehende Präferenzen und Neigungen einseitig zu verstärken, indem «genehme» Informationen tendenziell bevorzugt und konträre Sichtweisen und Argumente ausgeblendet werden. [6]

Forderungen, die sich daraus ergeben:

- Wie im geltenden Datenschutzgesetz muss beim Profiling die Anforderung, dass eine erforderliche Einwilligung ausdrücklich erfolgen muss, bestehen bleiben.
- Sollte die Schweiz einen risikobasierten Ansatz bei der Einwilligung zum Profiling wählen, muss ein Widerspruchsrecht vorgesehen werden. Dieses muss einfach und ohne Nachteile wahrgenommen werden können, indem z.B. für eine Dienstleistung mit Geld anstatt mit Daten bezahlt wird (Koppelungsverbot).