Luzerner Beiträge zur Rechtswissenschaft

Herausgegeben von Jörg Schmid

Olivier Heuberger

Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz

Band 144

Schulthess §

Luzerner Beiträge zur Rechtswissenschaft (LBR)

Herausgegeben von Jörg Schmid im Auftrag der
Rechtswissenschaftlichen Fakultät der Universität Luzern

Band 144

Olivier Heuberger

Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz

Schulthess § 2020

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7255-8137-5

www.schulthess.com

Inhaltsverzeichnis

Einleitung

«Der Einsatz der modernen Informations- und Kommunikationstechnologien in fast allen Lebensbereichen und die enorme Intensivierung der Datenverarbeitung und -verbreitung in Gesellschaft, Wirtschaft und Staat haben die Risiken von Persönlichkeitsverletzungen stark anwachsen lassen»[1], lautet der Einleitungssatz in der Botschaft zum Datenschutzgesetz aus dem Jahre 1988. Heute, rund dreissig Jahre später, heisst es in der Botschaft zum revidierten Datenschutzgesetz als Hauptziel der Revision ganz ähnlich: Es «sollen die Schwächen des Datenschutzgesetzes behoben werden, die aufgrund der rasanten technologischen Entwicklung entstanden sind»[2]. Seit dem Inkrafttreten des Datenschutzgesetzes[3] sind für den Datenschutz durch die technologischen und gesellschaftlichen Entwicklungen zudem neue Bedrohungen entstanden, die das Datenschutzgesetz teilweise nicht mehr handhaben kann, um einen genügenden Schutz für die betroffenen Personen zu gewährleisten.[4] Das Pendant auf europäischer Ebene, die seit Mai 2018 anwendbare europäische Datenschutz-Grundverordnung, führt vergleichbar aus, dass rasche technologische Entwicklungen den Datenschutz vor neue Herausforderungen stellen und das Ausmass der Erhebung und des Austauschs personenbezogener Daten eindrucksvoll zugenommen hat.[5] 1

Doch was hat sich in diesen rund drei Jahrzehnten technologisch dermassen verändert, dass es gerechtfertigt ist, Fragen zum Umgang mit Daten, im Spezifischen dem Profiling, aufzuwerfen? Im Zeitraum von 1988 bis heute entwickelten sich die Technologien zur Datenverarbeitung derart weiter, dass es damals den Fantasien von Science-Fiction-Literatur vorbehalten war, sich vorzustellen, dass selbstfahrende Fahrzeuge ein tatsächliches Fortbewegungsmittel sind, Landkarten in Echtzeit abgerufen werden können, im Internet gekaufte Waren gleichentags geliefert werden, Informationen in Echtzeit über 2

---

1 Botschaft DSG 1988, S. 414.

2 Botschaft DSG 2017, S. 6943.

3 Das im Entwurf vorliegende revidierte Datenschutzgesetz vom 15. September 2017 wird mit der Abkürzung ‚E-DSG' zitiert und dient in dieser Arbeit in Bezug auf die Bestimmungen zum Profiling und direkt damit zusammenhängende Bestimmungen als primäre Gesetzesangabe.

4 Botschaft DSG 2017, S. 6954; ähnlich bereits Bericht VE-DSG 2016, S. 17.

5 DSGVO, 6. Erwägungsgrund, S. 2.

Videoplattformen bezogen werden können und dass letztlich die ganze Welt des Internets in einem Smartphone Platz findet. Heute sind diese Vorstellungen keine Science-Fiction mehr.

3 Die Art, wie Menschen kommunizieren, ihre Freizeit verbringen oder Medien nutzen, hat sich durch das Internet in den letzten zwei Jahrzehnten in wesentlicher Weise verändert.[6] Dieser grundlegende gesellschaftliche Wandel hat sich in den letzten Jahren mit der Nutzung zahlreicher Geräte und Sensoren wie Smartphones, Tablets oder Fahrzeuge erweitert. Mit ihnen veränderte sich die Mobilität der Menschen, deren Einkaufsverhalten, die Art, Freunde zu treffen, und deren Arbeitswelt. *Daten und daraus ableitend Informationen*[7] verändern die Denkweise von Personen, beeinflussen deren politische und gesellschaftliche Ansichten, inspirieren zu neuen Ideen, wie Filme, Theater oder Musik umgesetzt werden können. Neue Technologien durchdringen das Leben in unzähligen Facetten in jedem Zuhause, in den Städten und auf dem Land. Dabei wissen Unternehmen wie Facebook, Twitter, Amazon, Samsung, Apple, Microsoft, IBM, Netflix oder Google weit mehr über ihre Kunden und zukünftigen Kunden als nur deren Identität und letzten Ferienort.[8] Dieses Wissen über eine Person in einem Profil zusammenzustellen, den Menschen in jeder Facette zu erfassen, zu kategorisieren und zu bewerten, wird als *Profiling*[9] bezeichnet. Das Recht versucht, das Profiling mit der nun erstmaligen gesetzlichen Verankerung in Art. 4 lit. f und Art. 5 Abs. 6 E-DSG datenschutzrechtlich einzufangen.

4 Profiling ist kein aus der rechtlichen Literatur entstandenes Konstrukt. Es ist zuallererst ein technologischer Vorgang und beschreibt den Prozess, mittels Algorithmen *Korrelationen*[10] zwischen Daten herzustellen, um das Verhalten und die Vorlieben einer Person oder einer Gruppe von Personen zu analysieren und vorauszusagen. Die Grundlagen für die Analyse und Bewertung der Persönlichkeit einer Person bilden Daten. Daten, die zwar seit längerem vorhanden, aber technologisch bis vor wenigen Jahren nicht oder nur unzureichend nutzbar waren und für Unternehmen damit keinen oder nur einen geringen

6 Vgl. UVEK, Bericht 2016, S. 3986 ff. m.w.H.

7 Zur Unterscheidung von Daten und Informationen, siehe hinten Rz. 71 ff.

8 «Google weiss noch mehr über uns, als wir meinen», SonntagsZeitung vom 10. Februar 2018, S. 19; dass sich die Identität nicht auf den Namen zu beschränken hat, eine Person dennoch bestimmbar ist, siehe hinten, Rz. 109 ff.

9 Siehe hierzu hinten, Rz. 54 ff.

10 Siehe hierzu hinten, Rz. 67 ff.

Mehrwert generierten. Die Entwicklung und Verbreitung von *KI-Technologien*[11] seit wenigen Jahren änderte dies grundlegend. Sie sind die Schlüsseltreiber für das Profiling. Es verbleibt jedoch ein diffuses Verständnis, was mit KI-Technologien gemeint ist und was die konkreten, rechtlichen Auswirkungen in Bezug auf das Profiling sein sollen. Die vorliegende Arbeit nimmt diese Problematik auf und stellt die Frage, wie es sich mit dem Persönlichkeits- und Datenschutzrecht verhält, wenn mithilfe von KI-Technologien ein Profil über eine Person oder eine Personengruppe angelegt wird.

Die Funktionsweise des Profilings ist für die meisten Personen weder ersichtlich noch verständlich, was zu einem Ungleichgewicht zwischen den Verantwortlichen, die die Daten bearbeiten, und denjenigen Personen, die die Daten bewusst oder unbewusst zur Verfügung stellen, führt.[12] Menschen werden jedoch unsicher, wenn sie nicht mehr überblicken, welche Unternehmen welche Daten über sie verarbeiten.[13] Beim Profiling besteht die Gefahr, dass Personen durch *Stereotypisierung*[14] beeinflusst, manipuliert oder diskriminiert werden.[15] Eine erste rechtliche Herausforderung beim Profiling besteht daher darin, Elemente von Persönlichkeitsmerkmalen zu beschreiben, die Stereotypisierungen erlauben. Profiling durch KI-Technologien erfolgt überdies häufig intransparent und gleicht einer *Blackbox*.[16] Der *erste Teil* dieser Arbeit bricht diese Blackbox auf, beschreibt die Begriffe KI-Technologien und Big Data sowie die dahinterliegenden Datenbearbeitungen, um nachvollziehen zu können, wie diese Technologien funktionieren. Sie führen sodann zum Zweck, zur Definition und Funktionsweise sowie zu den Arten des Profilings. 5

Die Möglichkeiten, mittels Datenkorrelationen einen Personenbezug herzustellen, haben sich mit den auf KI-Technologien basierenden *Algorithmen*[17] grundlegend verändert. Entscheidend ist, in welchem Zusammenhang Daten verwendet werden, der sich je nach Kontext der Datenbearbeitung verändert.[18] 6

---

11 Zur Definition von KI-Technologien siehe hinten, Rz. 13 ff.

12 Der Bericht VE-DSG 2016, S. 17 nennt als einen Hauptgrund der aktuellen Reform des DSG die zunehmende intransparente Datenbearbeitung, z.B. Profiling auf der Basis von Algorithmen.

13 Botschaft DSG 2017, S. 6969; Bericht VE-DSG 2016, S. 17.

14 Siehe hierzu hinten, Rz. 61 ff.

15 MUNOZ/SMITH/PATIL, S. 5 und S. 58 f.; GUTWIRTH/HILDEBRANDT, S. 33 f.

16 Siehe hierzu hinten, Rz. 28 ff.

17 Siehe hierzu hinten, Rz. 17 ff.

18 Siehe hierzu hinten, Rz. 85 ff. und Rz. 409 ff.

Die Frage, inwieweit Datenkorrelationen Profiling ermöglichen, führt zur genaueren Betrachtung von Daten, ihrer Abgrenzung von Informationen und den Möglichkeiten, eine Person zu identifizieren. In der Theorie kann ein Personenbezug durch Anonymisierung oder Pseudonymisierung aufgehoben werden. Auf KI-Technologien basierende Algorithmen stellen jedoch genau diese Verbindung – je nach Kontext ohne unverhältnismässigen Aufwand – wieder her. Die bisherige datenschutzrechtliche Definition von Personendaten nach Art. 3 lit. a DSG[19] stösst somit möglicherweise an ihre Grenzen. Damit stellt sich die Frage nach dem rechtfertigenden Verbleib der Konzepte der Anonymisierung und Pseudonymisierung in der datenschutzrechtlichen Realität.

7 Liegt ein Personenbezug vor, gilt es zu klären, ob Daten, die eine Person zu einem bestimmten Zweck zur Verfügung gestellt hat, weiterverwendet werden dürfen und inwiefern diese Weiterverwendung von ihrer Einwilligung oder einem anderen Rechtfertigungsgrund getragen ist. Die Beantwortung verlangt eine trianguläre Betrachtung: Profiling steht in einem Spannungsverhältnis zum Grundsatz der *Zweckgebundenheit*, zur *Einwilligung* sowie zum *überwiegenden privaten Interesse*. Die Erstellung eines Profils ist nur dann zulässig, wenn Daten für Zwecke verarbeitet werden, die bei der Beschaffung angegeben wurden, aus den Umständen ersichtlich oder gesetzlich vorgesehen sind (Art. 4 Abs. 3 und Abs. 4 DSG). Sehen beispielsweise Allgemeine Geschäftsbedingungen die Verwendung von Daten für Werbezwecke vor, darf dann ein Verantwortlicher jegliche Daten einer Person analysieren, ein Profil erstellen und auf sie zugeschnittene Produkte oder Dienstleistungen anbieten bzw. sie von bestimmten Produkten ausschliessen? Solche Fragen der Zweckbindung sind eng verknüpft mit der Frage der Einwilligung. Die Einwilligung beim Profiling nach Art. 5 Abs. 6 E-DSG setzt voraus, dass diese informiert, freiwillig und eindeutig erfolgt. Zu klären ist, welche Voraussetzungen gegeben sein müssen, damit die Einwilligung nicht zu einem formellen Leerlauf verkommt. Ferner ist sie in Abgrenzung zum überwiegenden privaten Interesse zu setzen. Diese Themen werden im *zweiten Teil* dieser Arbeit analysiert und ausführlich erörtert.

[19] Vgl. den gleichlautenden Art. 4 lit. a E-DSG.

Wie die datenschutzrechtlichen Herausforderungen des Profilings angegangen werden können, wird im *dritten Teil* herausgestellt. Im Fokus steht, dass Verantwortliche Daten angemessen bearbeiten können und dass Personen gleichzeitig vor missbräuchlichen Datenbearbeitungen geschützt sind. Hierzu wird das Konzept der *datenschutzrechtlichen Adäquanz*[20] eingeführt. Als objektives Korrektiv des Verhältnismässigkeitsgrundsatzes ergänzt es die Datenschutzgrundsätze und die Rechtfertigungsgründe wie die Einwilligung und des überwiegenden privaten Interesses. Schliesslich rundet eine Schlussbetrachtung diese Arbeit ab und fasst die Ergebnisse der gewonnenen Erkenntnisse in zwölf Kernaussagen als Arbeitsinstrument für die Praxis zusammen. 8

Zusammenfassend liegt das Ziel der vorliegenden Studie darin, die Wechselwirkungen zwischen den technologischen und datenschutzrechtlichen Aspekten beim Profiling zu untersuchen. Die sich dabei stellenden Fragen sind: Was ist und wie funktioniert Profiling? Was sind die zugrunde liegenden Technologien, die Profiling ermöglichen, und wie funktionieren diese? Welche Daten dürfen beim Profiling wie bearbeitet werden? Wie ist Profiling mit dem datenschutzrechtlichen Grundsatz der Zweckgebundenheit vereinbar? Kann eine betroffene Person in eine solchermassen vorgenommene Datenbearbeitung einwilligen oder gibt es hierzu andere Rechtfertigungsgründe? 9

20 Siehe hierzu hinten, Rz. 406 ff.