www.jusletter.ch

Romy Daedelow

Wenn Algorithmen (unfair) über Menschen entscheiden...

Welchen Schutz bietet die Datenschutz-Grundverordnung?

La contribution examine les inégalités de traitement numérique par algorithmes et sa prise en compte par le Règlement général sur la protection des données (RGPD). Les technologies d'analyse intelligente utilisent des algorithmes pour déterminer les relations dans les données qui permettent des prévisions et des prédictions précises sur le comportement et les capacités humaines. Ces analyses peuvent être injustes, voire discriminatoires. L'utilisation de technologies intelligentes conformes à la protection des données exige une prise en compte de l'équité et de la justice en matière de données et le RGPD prévoit, à cette fin, certains instruments. (jp)

Catégories d'articles: Contributions
Domaines juridiques: Informatique et droit; Protection des données

Proposition de citation: Romy Daedelow, Wenn Algorithmen (unfair) über Menschen entscheiden..., in : Jusletter 26 novembre 2018

ISSN 1424-7410, https://jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsverzeichnis

I. Einführung: «Der massgeschneiderte Arbeitnehmer»

[Rz 1] Eine Welt, in der ausschliesslich Algorithmen mit ihrer kühlen mathematischen Logik über existentielle Fragen entscheiden, erscheint noch utopisch. Die Vorstellung, ein Computer analysiert mit Hilfe von Algorithmen und der enormen Fülle an Daten emotionslos und ohne subjektive Befindlichkeiten menschliche Verhaltensweisen und Leistungsfähigkeiten, übt dennoch eine gewisse Faszination aus.

[Rz 2] *Man stelle sich vor, ein Computer kann Eigenschaften und Fähigkeiten für eine konkrete Arbeitsstelle ermitteln. Bewerbungen werden mit diesen Eigenschaften abgeglichen und der Computer entscheidet über die Einladung zum Bewerbungsgespräch. Eine solche Vorstellung ist längst nicht mehr utopisch. Wegen der hohen Fluktuationsrate seiner Mitarbeitenden in einem Call Center hat ein U.S. Unternehmen eine Vielzahl von Arbeitnehmerdaten mit Hilfe eines eigens dafür entwickelten Algorithmus ausgewertet, um zu ermitteln, welche Eigenschaften es braucht, Arbeitnehmende längerfristig zu binden. Die Analyse brachte drei überraschende Kriterien zu Tage: entscheidend war die Aktivität in sozialen Netzwerken, die Entfernung zwischen Wohn- und Arbeitsort sowie die Persönlichkeit von Bewerbenden. Als geeignet gelten kreative Personen, deren Aktivität in sozialen Netzwerken eher gering und deren Wohnort nah am Arbeitsplatz war. Als nicht geeignet hingegen galten neugierige Personen, die in mehr als vier sozialen Netzwerken registriert waren und zum Arbeitsort pendeln mussten. Als Antwort auf dieses Ergebnis stellte das Unternehmen seine Einstellungspraxis um. Anstelle, wie bisher, die Berufserfahrung abzufragen, mussten Bewerbende in einem Online-Fragebogen auf Fragen antworten, die auf die computergenerierten Kriterien zugeschnitten waren. Entsprechend ihrer Angaben wurden Bewerbende in Kategorien «erwünscht» oder «unerwünscht» eingeteilt. Erstere erhielten eine automatische, maschinell erstellte Einladung zum Bewerbungsgespräch; letztere eine Ablehnung.*[1]

[Rz 3] Zwar vereinfacht dargestellt, zeigt dieser Fall dennoch, dass die Technik schon heute durchaus in der Lage ist, menschliche Auswahl- und Bewertungssysteme durch datengestütz-

[1] Fallbeispiel von Xerox Corp. in Anlehnung an den Artikel aus dem Wall Street Journal vom 20. September 2012 «Meet the New Boss: Big Data – Companies Trade in Hunch-Based Hiring For Computer Modeling» von Joseph Walker (Online-Version https://www.wsj.com/articles/SB10000872396390443890304578006252019616768, Website zuletzt besucht am 31. Juli 2018) und den Artikel aus der MIT Technology Review vom 27. Mai 2013 «The Machine-Readable Workforce» von Jessica Leber (https://www.technologyreview.com/s/514901/the-machine-readable-workforce/, Website zuletzt besucht am 31. Juli 2018).

te und von Algorithmen geprägte Analysen zu ersetzen. Bislang hauptsächlich in den Vereinigten Staaten angewendet, etablieren sich nun auch «vor unserer Haustür» bereits Unternehmen, die solche Analysetechnologien entwickeln. In der Schweiz, beispielsweise, verspricht die *People-Analytix Online Plattform*, individuelle Fähigkeiten von Mitarbeitenden aus Arbeitnehmerdaten mittels Algorithmen zu analysieren, Muster und Trends für künftig entscheidende Fähigkeiten von Mitarbeitenden zu ermitteln und daraus schliesslich Profile für gefragte Fähigkeiten zu erstellen[2]. *«Recognize the skill development needs of your workforce; Identify future-relevant skills and trends; Develop your employees in line with your strategy ...»*[3] so bewirbt die People Analytix AG ihr Produkt. Der Gehalt dieser Worte dürfte verdeutlichen, warum diese Technologien eine Faszination ausüben. Anwender, z.B. Arbeitgeber können mit solchen Technologien in Bewertungs- und Auswahlprozessen risikoärmer und effizienter entscheiden.

[Rz 4] Sind Menschen das Objekt dieser datengestützten Analysen, besteht die Gefahr von Grundrechtsverletzungen. In erster Linie ist das Grundrecht auf Datenschutz betroffen; ein Grundrecht, welches ausdrücklich in der Charta der Grundrechte der EU[4] verankert ist, aber auch in anderen Rechtsordnungen in Europa einen verfassungsrechtlichen Stellenwert einnimmt[5]. Auch bekannt unter der Bezeichnung «Recht auf informationelle Selbstbestimmung»[6] soll das Grundrecht auf Datenschutz sicherstellen, dass jede Person allein darüber bestimmen darf, ob und zu welchem Zweck ihre personenbezogenen Daten von wem verarbeitet werden.

[Rz 5] Doch neben der Gefährdung des Grundrechts auf Datenschutz weisen diese Analysetechniken ein weiteres Gefährdungspotential auf: Ein ihnen innewohnendes Diskriminierungsrisiko. Mittlerweile ist bekannt, dass Algorithmen Diskriminierungen und Ungleichbehandlungen verursachen können. Diese Problematik ist so brisant, dass sie auch im politischen Umfeld bereits «angekommen» ist[7]. In Deutschland wurde unlängst sogar über ein «Digitales Anti-Diskriminierungsgesetz» nachgedacht[8]. Das dürfte daran liegen, dass die allgemeinen Diskriminierungsschutzrechte, insbesondere das für die EU-Mitgliedsstaaten verbindliche Anti-Diskriminierungsrecht der Europäischen Union den gebotenen Schutz nicht vorsehen. Das hat mehrere Gründe: Einerseits sind die Funktionsweisen der Technologien und damit etwaige Diskriminierungshandlungen für Betroffene kaum nachweisbar. Andererseits verhindert ein starrer und nicht erweiterbarer Katalog an klassischen Diskriminierungsmerkmalen einen Schutz bei Benachteili-

---

2 Website der People-Analytix Online Plattform (https://www.people-analytix.com/, Website zuletzt besucht am 31. Juli 2018); siehe auch Online-Artikel aus Startupticker.ch vom 21. Februar 2018 «People Analytics mit People Analytix» von Sophie Küsterling (https://www.startupticker.ch/en/news/february-2018/people-analytics-mit-people-analytix, Website zuletzt besucht am 31. Juli 2018)

3 Vgl. die eingeblendeten Banner auf der Homepage der People-Analytix AG (https://people-analytix.com/, zuletzt besucht am 8. November 2018).

4 Charta der Grundrechte der Europäischen Union, ABl. EU C 326/02, 26. Oktober 2012, S. 391–407.

5 So z.B. in der Schweiz, Art. 13 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

6 So z.B. in Deutschland, wo das Recht auf informationelle Selbstbestimmung auf verfassungsrechtlicher Ebene aus dem allgemeinen Persönlichkeitsrecht Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 des Grundgesetzes für die Bundesrepublik Deutschland (GG, BGBl. I S. 2347) seit dem sog. «Volkszählungsurteil» des Bundesverfassungsgerichts (BVerfGE 65, 1) abgeleitet wird.

7 So z.B. in den USA unter der Obama-Regierung «Big Data: A Report on Algorithmic Systems, Opportunity and Civil Rights», Mai 2016, (https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf, Website zuletzt besucht am 31. Juli 2018).

8 Siehe Artikel aus der Zeit-Online vom 03. Juli 2017 «*Maas schlägt digitales Antidiskriminierungsgesetz vor*» von Patrick Beuth (Website zuletzt besucht am 31. Juli 2018 https://www.zeit.de/digital/internet/2017-07/heiko-maas-algorithmen-regulierung-antidiskriminierungsgesetz)

gungen, denn Computer treffen Entscheidungen anhand von neuen, durch Daten und Algorithmen generierten Differenzierungsmerkmalen. Und schliesslich bringt das Diskriminierungsrecht Betroffenen bei Verstössen gegen das Diskriminierungsverbot nur einen Schadensersatzanspruch. Dringlicher wäre jedoch ein wirksamer präventiver Rechtsschutz, der Betroffenen Instrumente in die Hand gibt, Diskriminierungen durch Analysetechnologien effektiv nachzuweisen und einen rechtmässigen Einsatz zu erzwingen oder den Einsatz dieser Technologien sogar zu unterbinden.

[Rz 6] Einen wichtigen Beitrag hierfür könnte die seit dem 25. Mai 2018 in der EU geltende Datenschutz-Grundverordnung (DSGVO)[9] leisten. Mit der Einführung des Begriffs «Profiling» versucht die DSGVO, die neuen Analysetechnologien rechtlich zu definieren und automatisierten Entscheidungen, die auf Profilingresultaten beruhen, rechtliche Grenzen zu setzen. Gemäss dem Schutzziel der DSGVO müssen bei der Verarbeitung von personenbezogenen Daten die Grundrechte natürlicher Personen beachtet werden. Dazu gehören auch Diskriminierungsschutz und Gleichheitsgewährleistung. Ein ausdrückliches Diskriminierungsverbot enthält die DSGVO allerdings nicht. Die Verordnungsgeber dürften dennoch einen gewissen Diskriminierungsschutz beabsichtigt haben, da bestimmte Datenverarbeitungsprozesse mit Diskriminierungspotential verboten werden. Das zeigt sich insbesondere durch den Schutz besonders sensibler Daten in Art. 9 DSGVO mit Schutzkategorien, ähnlich denjenigen des Anti-Diskriminierungsrechts. Deren Verarbeitung ist grundsätzlich nicht zulässig. Art 9[10], auch «informationelles Diskriminierungsverbot» genannt, ist letztlich eine einfachgesetzliche Ausprägung des Diskriminierungsschutzes aus Art. 21 der EU-Grundrechtscharta[11]. Ein Rückgriff auf die DSGVO bei Diskriminierungsfällen ist also naheliegend.

[Rz 7] Der Beitrag soll einen Überblick darüber vermitteln, ob die DSGVO tatsächlich ein wirkungsvolles Gesetz gegen digitale Ungleichbehandlungen ist. Dazu ist es zunächst notwendig, der Frage nachzugehen, wie es überhaupt zu solchen Ungleichbehandlungen kommt.

II. Können Computer ungerecht sein?

[Rz 8] *Im oben genannten Beispielsfall wünscht sich Bewerberin A eine längerfristige Stelle und hat sich in ihrer letzten Stelle durch ihre sehr guten Beratungs- und Problemlösungsfähigkeiten ausgezeichnet. Ein Computer kategorisiert A jedoch als ungeeignet, da sie in mehr als vier sozialen Netzwerken registriert ist. A sieht sich als Opfer einer Fehlklassifizierung durch einen Computer und fühlt sich ungerecht behandelt. Bewerber B, ebenfalls auf der Suche nach einer längerfristigen Stelle, hat Berufserfahrungen in Call Centern, wird vom Computer als ungeeignet klassifiziert, weil der Wohnort von B zu weit entfernt vom Arbeitsplatz entfernt ist. Der Wohnort des B liegt in einem Stadtbezirk mit einem hohen Ausländeranteil, zu dem auch B gehört. B ist der Meinung, das Auswahlkriterium «Wohnort nah am Arbeitsplatz» diskriminiere indirekt Bewerber anderer Herkunft, weil ausländische Bewerber von diesem Ablehnungskriterium überproportional betroffen sind.*

---

9 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU vom 4. Mai 2016, Nr. L 119, S. 1–88 (zit. DSGVO).

10 Artikel ohne Gesetzesbezeichnung im fortlaufenden Text sind diejenigen der Datenschutz-Grundverordnung.

11 Thilo Weichert, in: Datenschutz-Grundverordnung/BSDG Kommentar, Hrsg. Jürgen Kühling und Benedikt Buchner, 2. Aufl., München 2018 (zit. Kühling/Buchner/Verfasser, DSGVO), Art. 9 N. 2.

[Rz 9] Hochkomplexe *Data Mining*-Analysetechnologien können auf neue Art und Weise Erkenntnisse über Menschen gewinnen, insbesondere künftiges menschliches Handeln oder Verhalten vorhersagen (*Predictive Analytics*). Ausgangspunkt derartiger Analysen ist die Sammlung von Daten, was durch konkretes Abfragen (z.B. Online-Fragebögen) oder durch die Nutzung von vorhandenen Daten ermöglicht wird. Datenbanken sind dank Big Data in der Lage, eine enorme Fülle an Daten aufzunehmen und zu speichern[12]. Nach der Datensammlung finden die eigentlichen Analyseprozesse des Data Minings statt[13]. *Pattern Mining* dient dem Auffinden von statistischen Zusammenhängen in vorhandenen historischen Daten. Das ermöglicht die Beschreibung oder Vorhersage bestimmter Parameter, z.B. welche Attribute ein Mensch in bestimmten Lebenssituationen entweder haben oder nicht haben sollte oder wie sich Menschen in bestimmten Situationen verhalten werden[14]. Kausalität spielt dabei keine Rolle; ein Algorithmus sucht nach Datenkorrelationen, d.h. Muster in den Daten, die sich hauptsächlich mathematisch-statistisch nachweisen lassen. Die Vorhersagen ermöglichen es, Risiken besser einzuschätzen und Entscheidungen nach einem individuellem Risikofaktor zu treffen. Das kann durch Algorithmen gesteuerte *Klassfikationsverfahren* geschehen. Die datengenerierten Attribute werden in Kategorien oder Profilen zusammengefasst und bilden ein Modell für einen Klassifizierungsprozess, der darauf abzielt, individuelle Daten den Kategorien automatisch zuzuordnen. Dazu muss ein entsprechender Algorithmus mit sog. Trainingsdateien «trainiert» werden und «lernt» aus diesen vorhandenen Datenmodellen künftige Regeln[15]. Ein Computer kann z.B. Bewerbende automatisch in die Profile «geeignet» oder «ungeeignet» einsortieren und dann automatische Entscheidungen treffen[16].

[Rz 10] Doch gerade diese Modellbildung und Einsortierung von Daten kann zu diskriminierenden Ergebnissen führen: Entweder dadurch, dass sich im Datenmodell die in der Gesellschaft bestehenden Vorurteile und entsprechendes Diskriminierungsverhalten widerspiegeln oder durch Fehlklassifizierungen. Ersteres kann auf verschiedene Weise entstehen: Allein schon die Sammlung der Daten für die Entwicklung eines Datenmodells kann vorurteilsbelasted sein. Sind z.B. Datenbanken unvollständig und wird dadurch eine Gruppe von Menschen unterrepräsentiert, dann spiegelt sich das auch im Ergebnis der Analyse wieder[17]. Klassisches Beispiel sind Frauen in Führungspositionen, über die es aufgrund der gesellschaftlichen Verhältnisse weniger historische Daten gibt als über Männer. Wird diese Tatsache in der Entwicklung von Datenmodellen, z.B. zur Auswahl von Bewerbenden, ignoriert, sind solche Datenmodelle nicht neutral. Daten-

12 Bart Custers, «Data Dilemmas in the Information Society: Introduction and Overview», in: Discrimination and Privacy in the Information Society, Hrsg. Bart Custers, Toon Calders, Bart Schermer, Tal Zarsky, Berlin, Heidelberg 2013, S. 7, 8.

13 Die bekanntesten Data Mining-Methoden sind Pattern Mining (oder Regressionsanalyse) zum Auffinden von Mustern in Daten, Clusteranalysen zur Identifikation von Gruppen in einem Datensatz und Klassifikationsverfahren zur Zuordnung z.B. von Personen in vorbestimmte Gruppen oder Klassen (z.B. durch einen sog. Entscheidungsbaum), siehe dazu insgesamt Toon Calders und Bart Custers, «What is Data Mining and How Does it Work?», in: Discrimination and Privacy in the Information Society (Fn. 12), S. 31–42 (Fn. 12).

14 Vgl. Toon Calders und Bart Custers (Fn. 13), S. 37; Ziel des Data Minings ist in der Regel Erkenntnisse zu gewinnen, die entweder Zustände beschreiben oder Zustände vorhersagen, siehe hierzu Usama Fayyad, Gregory Piatetsky-Shapiro, Padhraic Smyth, «From Data Mining to Knowledge Discovery in Databases», in: Advances in Knowledge Discovery and Data Mining, AI Magazine, AAAI Press (u.a.), Menlo Park, California 1996, S. 43.

15 Vgl. Toon Calders und Bart Custers (Fn. 13), S. 32, 33.

16 Im Beispielsfall kann die Regel dann lauten: «WENN Aktivität in mehr als vier sozialen Netzwerken DANN ungeeignet und WENN ungeeignet DANN keine Einladung zum Bewerbungsgespräch».

17 Toon Calders und Indrė Žliobaitė, «Unbiased Computational Processes», in: Discrimination and Privacy in the Information Society (Fn. 12), S. 46 u. 49; vgl. auch Solon Barocas and Andrew D. Selbst, Big Data's Disparate Impact, California Law Review, Vol. 104, 2016, S. 684-687.

modelle können weiterhin auf Attributen beruhen, die nach aussen hin neutral wirken, dennoch aber mit einem sensiblen Charakteristikum zusammenhängen und dadurch gewisse Gruppen von Menschen benachteiligen[18]. Das zeigt das Beispiel von Bewerber B im obigen Fall; das neutrale Attribut «Entfernung zum Arbeitsplatz» könnte mit der Herkunft einer Person korrelieren und daher Personen mit einem bestimmten ethnischen Hintergrund diskriminieren. In Klassifizierungsverfahren können sich Vorurteile schliesslich auch in der Definition von Zuordnungskriterien widerspiegeln[19]. Insbesondere kann ein Computer subjektiv geprägte Regeln vergangener Entscheidungen «erlernen», z.B. dass Frauen wegen einer möglichen Schwangerschaft eher ein Risiko darstellen und daher keine geeigneten Arbeitnehmerinnen sind[20].

[Rz 11] Fehlklassifizierungen, im Beispielsfall durch Bewerberin A dargestellt, resultieren aus der statistischen Natur der Analyseverfahren. Hier besteht die Gefahr eines sog. «Generalisierungsunrechts» oder statistischen Diskriminierungen[21]. Diese treten ein, wenn ein Mensch ein computergeneriertes Attribut eines Profils erfüllt und damit automatisch dem Profil zugeordnet wird. Negative Schlussfolgerungen aus dem Profil werden dann auf alle in das Profil zugeordneten Personen übertragen. Treffen diese auf eine Person im Einzelfall aber gar nicht zu, werden fehlerhafte Schlussfolgerungen über diese Person gezogen. Das führt zur Ungleichbehandlung, da die Person so behandelt wird, wie andere Personen, die jedoch die Profileigenschaft oder Vorhersage erfüllen.

[Rz 12] Können also Computer ungerecht sein? Sie können jedenfalls zu diskriminierenden, ungerecht(-fertigt)en Ergebnissen und dementsprechenden Entscheidungen führen. Computer haben dennoch keine bewusste Absicht, zu diskriminieren. Das Diskriminierungspotential ist vielmehr ein Ergebnis intelligenter Technologie, die in der Lage ist, nicht nur die gesellschaftlichen Verhältnisse zu spiegeln, sondern auch aus ihnen zu lernen. Noch hat der «Lehrer Mensch» die Handlungshoheit über derartige Analysetechnologien und es liegt in unseren Händen, diese rechtlich und ethisch vertretbar zu nutzen. Ob die DSGVO dazu einen Beitrag leisten kann, wird im dritten Teil dieses Beitrags überblicksmässig erläutert.

III. Was kann die Datenschutz-Grundverordnung?

[Rz 13] Mit der neuen Regelung zum *Profiling* (Art. 4 Nr. 4) und einer überarbeiten Regelung zu automatisierten Entscheidungen im Einzelfall (Art. 22) versucht die DSGVO, den Datenschutz an die neuen technologischen Entwicklungen und an die neuen Möglichkeiten der Erhebung und des Austauschs von personenbezogenen Daten anzupassen[22]. Beide Regelungen erlangen Bedeutung, wenn es zum Einsatz datengestützter Analysetechnologien kommt. Ein Verbot von Diskriminierungen oder Ungleichbehandlungen ist diesen Regelungen dennoch, zumindest vom Wortlaut her, nicht zu entnehmen. Das heisst jedoch nicht, dass Diskriminierungs- und Gleichheitsaspekte ausser Acht gelassen werden dürfen. Im Gegenteil – über die Regelungen zum Pro-

18 Toon Calders und Indrė Žliobaitė (Fn. 17), S. 47 u. 49.

19 Toon Calders und Indrė Žliobaitė (Fn. 17), S. 46 u. 48.

20 Siehe hierzu auch Solon Barocas und Andrew D. Selbst (Fn. 17) S. 682.

21 Ausführlich dazu Gabriele Britz «Einzelfallgerechtigkeit vs. Generalisierung», Tübingen 2008 (Definition «Generalisierungsunrecht» S. 2 und statistische Diskriminierung S. 9).

22 Siehe Erwägungsgrund (EG) 6 DSGVO.

filing und zu den automatisierten Entscheidungen dürften diese Aspekte indirekten Eingang in das Datenschutzrecht finden.

1. Profiling und automatisierte Entscheidungen

[Rz 14] Während das Konzept der *automatisierten Entscheidung* bereits in der Datenschutzrichtlinie (DS-RiLi) von 1995[23] zu finden war, ist *Profiling* erstmalig im europäischen Datenschutzrecht geregelt. Art. 4 Nr. 4 DSGVO beschreibt das Profiling als «*jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, (...) persönliche Aspekte einer natürlichen Person zu bewerten, insbesondere Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel (...) zu analysieren oder vorherzusagen*». Kurz gesagt, ist Profiling ein automatisierter Datenverarbeitungsprozess zum Zwecke der Persönlichkeitsbewertung. Im eingangs erwähnten Fall dürfte wenig Zweifel daran bestehen, dass zumindest die Verarbeitung der individuell in den Online-Fragebogen eingegebenen Daten unter die datenschutzrechtliche Definition des Profilings fällt. Es handelt sich um ein datengestütztes automatisiertes Verfahren, mit dem Ziel, vorherzusagen, ob ein Bewerber oder eine Bewerberin für die Position im Call Center geeignet ist. Es soll also die Eignung des Bewerbers oder der Bewerberin vorhergesagt werden.

[Rz 15] Vom Profiling zu unterscheiden, sind automatisierte (Einzelfall-)Entscheidungen gemäss Art. 22. Danach hat eine betroffene Person das Recht, «*nicht einer ausschliesslich auf einer automatisierten Verarbeitung – einschliesslich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt*». Diese Formulierung ist etwas missverständlich, da auch hier das Profiling genannt wird. Profiling und automatisierte Entscheidungen im Einzelfall sind allerdings nicht dasselbe. Profiling ist ein Datenverarbeitungsprozess. Bei automatisierten Entscheidungen geht es, wie der Wortlaut vermuten lässt, um Entscheidungen und zwar um Entscheidungen, die auf der Grundlage von automatisierten Datenverarbeitungsprozessen getroffen werden. So kann das Ergebnis eines Profilings die Grundlage für eine automatisierte Entscheidung sein[24]. Art. 22 regelt also nicht die Zulässigkeit einer Datenverarbeitung als solcher, sondern die Nutzung der Ergebnisse einer bestimmten Datenverarbeitung[25]. Eine Entscheidung ist nur dann eine automatisierte Entscheidung, wenn sie ohne jegliches menschliches Zutun erfolgt. Obwohl viel diskutiert, dürfte dieses Kriterium so auszulegen sein, dass ein menschliches Zutun nur dann vorliegt, wenn ein Mensch inhaltlich die Entscheidung (mit-)bestimmt und damit (mit) zu verantworten hat[26]. Andernfalls gäbe es Umgehungsmöglichkeiten, um Art. 22 gar nicht zur Anwendung kommen zu lassen. Das nämlich dann, wenn der Computer die Entscheidung trifft, dennoch ein Mensch «nur für den Knopfdruck» pro forma dazwischengeschaltet wird.

---

23 Art. 15 der Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24 . Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EU vom 23. November 1995, Nr. L 281, S. 31-50 (zit. DS-RiLi).

24 Kühling/Buchner/Buchner, DSGVO (Fn. 11), Art. 4 Nr. 4 N.1.

25 Kühling/Buchner/Buchner, DSGVO (Fn. 11), Art. 22 N. 11.

26 Kühling/Buchner/Buchner, DSGVO (Fn. 11), Art. 22 N. 15 m. w. N.; siehe auch Artikel-29-Datenschutzgruppe (WP-29), «Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679» vom 3. Oktober 2017 in der aktuellen Version vom 6. Februar 2018, 17/EN, WP 251rev.01, S. 10 (zit. WP-29, N.251rev.01).

[Rz 16] Im obigen Fallbeispiel, in dem der Computer letztlich auf der Grundlage des Eignungsprofils der Bewerber über die Einladung zum Bewerbungsgespräch entschieden hat, darf man wohl von einer automatisierten Entscheidung ausgehen. Was nun, wenn die ermittelten Profilingergebnisse einzelner Bewerbender auf unzutreffenden, wenn nicht sogar diskriminierenden Kriterien beruhen und ein Computer diesen Personen daraufhin eine automatische Absage erteilt? Dann lohnt es sich, aus datenschutzrechtlicher Sicht einen Blick auf die Zulässigkeit des Profilings sowie der automatisierten Entscheidung zu werfen. Sie unterliegen strengen Rechtmässigkeitsvoraussetzungen:

a. Zulässigkeit von Profilingmassnahmen

[Rz 17] Eine spezielle Vorschrift zur Regelung der Rechtmäßigkeit des Profilings sieht die DSGVO nicht vor. Profiling ist grundsätzlich nicht verboten und unterliegt, wie jede andere Datenverarbeitung, den allgemeinen Verarbeitungsgrundsätzen, sofern personenbezogene Daten verarbeitet werden[27]. Bereits aus der DS-RiLi bekannt, müssen Datenverarbeitungen, somit auch das Profiling, den Grundsätzen der Rechtmäßigkeit und Transparenz, der Zweckbindung, der Datenminimierung, der Datenrichtigkeit sowie der Integrität und Vertraulichkeit entsprechen (Art. 5 Abs. 1 lit. a) – lit. f)). In der Praxis dürfte das auf Schwierigkeiten stossen. Denn die Funktionsweisen der datengestützten Analysetechnologien widersprechen in vielerlei Hinsicht den Prinzipien des Datenschutzrechts.

[Rz 18] Eines der wichtigsten Prinzipien im Datenschutzrecht ist der Grundsatz der Zweckbindung. Der Einsatz der Analysetechnologien vermag diesen Grundsatz nicht immer zu erfüllen. Eine gute Funktionsweise dieser Technologien erfordert eine gewisse Menge an Daten. Dabei dürfen die Anwender dieser Technologien nicht ohne Weiteres auf bereits bestehende Datenbestände zurückgreifen, die zu einem ganz anderen Zweck erhoben worden sind. Man denke z.B. an einen Arbeitgeber, der bestehende personenbezogene Arbeitnehmerdaten, die ursprünglich zu Zwecken der Begründung des Arbeitsverhältnisses erhoben worden sind, für Analysen nutzen möchte. Ohne erneute Einwilligung der Betroffenen für die Datenverarbeitung – ausdrücklich zum Zweck der Persönlichkeitsbewertung – oder einer zulässigen nachträglichen Zweckänderung (die nur unter den engen Voraussetzungen des Art. 6 Abs. 4 möglich ist), werden die Grundsätze der rechtmässigen Datenerhebung und der Zweckbindung verletzt. Werden darüber hinaus sogar falsche oder fehlerhafte Daten verwendet, kann das zudem den Grundsatz der Datenrichtigkeit verletzen.

[Rz 19] Analysetechnologien profitieren, dank Big Data, von der Vielzahl der täglich anfallenden Daten und deren Speicherung «auf Vorrat» ohne konkreten Verwendungszweck. Eigenmächtiges Sammeln von personenbezogenen Daten, insbesondere die täglich anfallenden Daten aus dem Gebrauch von digitalen Medien und Dienstleistungen ohne konkrete Einwilligung der Betroffenen ist genauso verboten, wie eine endlose Speicherung dieser Daten. Die Datenerhebung ist gemäss dem Grundsatz der Datenminimierung und Speicherbegrenzung auf das notwendige Mass zu beschränken. Die Daten müssen gelöscht werden, wenn der Zweck der Verarbeitung erfüllt ist.

27 Siehe EG 72 DSGVO.

[Rz 20] Der Grundsatz der rechtmässigen Datenverarbeitung (Art. 6) erfordert in der Regel eine Einwilligung. Liegt diese vor, sollte, gerade in Abhängigkeitsverhältnissen, deren Freiwilligkeit geprüft werden. Wie freiwillig ist z.B. eine Einwilligung für Bewerbende, wenn es keine Alternative zu einer Online-Bewerbung gibt, bei der ein Häkchen im «Einwilligungs-Feld» zwingende Voraussetzung für das Versenden der Bewerbung ist? Gegen die Freiwilligkeit spricht ein klares Ungleichgewicht in der Auswahl- und Entscheidungsfreiheit zugunsten der datenverarbeitenden Stelle und zulasten der betroffenen Person[28].

[Rz 21] Schwierig wird es dann, wenn das Analyseergebnis als Entscheidungsgrundlage für einen Vertragsschluss erforderlich ist. Dann darf auf eine Einwilligung verzichtet werden (Art. 6 Abs. 1 lit. b). Allerdings ist das Kriterium der *Erforderlichkeit* unbestimmt und eine Erklärung dazu könnte hier viele Seiten füllen. In Bezug auf Diskriminierungen und Ungleichbehandlungen sei nur gesagt, dass die Datenverarbeitung sich als objektiv sinnvoll für den jeweiligen Vertragszweck erweisen sollte[29]. Das dürfte bei einer Analyse, die auf einer fehlerhaften Datenerhebung oder auf vorurteilsbehafteten Algorithmen mit diskriminierenden Ergebnis beruht, nicht der Fall sein, ebenso wenig, wenn eine Fehlklassifizierung als Entscheidungsgrundlage für ein konkretes Rechtsgeschäft in Kauf genommen wird.

[Rz 22] Besonderes Augenmerk gilt sensiblen Daten, die in einem Analyseverfahren verarbeitet werden. Sensible Daten sind personenbezogene Daten, denen aufgrund ihrer Aussagekraft ein Diskriminierungsrisiko innewohnt und die daher einen weitergehenden Rechtsschutz erfordern. Eine Verarbeitung von sensiblen Daten ist grundsätzlich nicht zulässig (Art. 9 Abs. 1), es sei denn, eine der zahlreichen Ausnahmen (Art. 9 Abs. 2) kommt zum Tragen. Zu beachten ist aber, dass die Analyse selbst sensible Daten hervorbringen kann[30]. Eine eindeutige Regelung dafür existiert nicht. Dennoch dürfte eine weitere Datenverarbeitung, z.B. ein weiteres Profiling, wegen Art. 9 Abs. 1 nicht zulässig sein[31].

b. Zulässigkeit von automatisierten Entscheidungen

[Rz 23] Art. 22 Abs. 1 verbietet grundsätzlich automatisierte Entscheidungen, wenn sie einer Person gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen. Diskriminierungen oder Ungleichbehandlungen durch das Ergebnis von datengestützten Analysetechnologien äussern sich in der Regel durch Ausschluss einer Person aus einem Auswahl- oder Evaluationsverfahren und/oder in der Ablehnung eines Vertragsschlusses. Das Potential, Personen auszuschliessen oder zu diskriminieren wird als eine erhebliche Beeinträchtigung im Sinne der DSGVO angesehen[32].

---

28 Siehe EG 43 DSGVO.

29 Sebastian Schulz, in: Datenschutz-Grundverordnung VO (EU) 2016/679, Kommentar, Hrsg. Peter Gola, München 2017, Art. 6 N. 36.

30 Z.B. der Gesundheitszustand einer Person, der durch die Kombination zweier nicht sensibler Informationen wie Einkaufsverhalten bei Lebensmittel und Qualität der Lebensmittel, analysiert werden kann. Siehe WP-29, N.251rev.01 (Fn. 26), S.15.

31 Wenn Profiling sensible Daten hervorbringen kann, fordert die WP-29 von datenverarbeitenden Stellen, sicherzustellen, dass die Verarbeitung entsprechend dem ursprünglichen Zweck erfolgte, ein Verfahren zur rechtmässigen Verarbeitung dieser Daten identifiziert wird und die betroffene Person über die Verarbeitung informiert wird. Siehe WP-29, N.251rev.01 (Fn. 26), S. 15.

32 Siehe EG 71 DSGVO. Dort wird ausdrücklich eine automatische Ablehnung eines Online-Kreditantrags oder eines Online-Einstellungsverfahrens als erhebliche Beeinträchtigungen genannt. Siehe auch WP-29, N.251rev.01 (Fn. 26), S. 21.

[Rz 24] Automatisierte Ablehnungen und andere diskriminierende automatisierte Entscheidungen aufgrund von Profilanalysen sind allerdings nur im Grundsatz verboten. Es gibt drei Ausnahmen: Sie sind zulässig, (1) sofern die Entscheidung für einen Vertragsschluss oder die Vertragserfüllung erforderlich ist, (2) Gesetze in der EU oder in den EU-Mitgliedsstaaten die Entscheidung erlauben oder (3) eine ausdrückliche Einwilligung einer betroffenen Person vorliegt. Allerdings verlangt die DSGVO dann, angemessene Massnahmen zur Sicherstellung von Grundrechten und berechtigten Interessen der betroffenen Personen zu treffen (Art. 22 Abs. 3). Dazu muss insbesondere das vorgeschaltete Analyseverfahren fair und transparent, sowie fehler- und diskriminierungsfrei ablaufen[33]. Basiert eine automatisierte Entscheidung auf sensiblen Daten, ist sie grundsätzlich nach Art. 22 Abs. 4 untersagt. Hierbei ist daran zu denken, dass ein Profiling selbst auch neue personenbezogene Daten mit sensiblen Inhalten hervorbringen kann. Hier gilt dann ebenfalls Art. 22 Abs. 4.

[Rz 25] Vor diesem Hintergrund können diskriminierende und durch Ungleichbehandlungen geprägte Entscheidungen unzulässig sein. Es mag schon zweifelhaft sein, ob die Ausnahmen aus Art. 22 Abs. 2 in einem Einzelfall zutreffen. Bei einer vorliegenden ausdrücklichen Einwilligung ist z.B. fraglich, ob diese auch eine automatisierte Entscheidung über ein fehlerhaft zustande gekommenes oder diskriminierendes Resultat umfasst. Und eine Entscheidung, die auf einem vorurteilsbelasteten und fehlerhaften Analyseverfahren basiert, dürfte für keinen Vertrag erforderlich sein. Im obigen Fallbeispiel könnte das diskutiert werden, da die automatisierte Auswahlentscheidung für ein Bewerbungsgespräch nicht einem konkreten Vertragsschluss, sondern nur vorvertraglichen Auswahlentscheidungen dient[34]. Jedenfalls sind aber die angemessenen Massnahmen nicht getroffen worden, weil die Entscheidung auf einem Verfahren beruht, welches Fehlklassifizierungen und Diskriminierungen zulässt und damit Rechte von Betroffenen verletzt. Das macht zwar die Entscheidung nicht unzulässig, löst aber Sanktionen aus[35].

[Rz 26] In jedem Fall muss betroffenen Personen eine ausdrückliche Möglichkeit eingeräumt werden, die automatisierte Entscheidung wieder zu einer «menschlichen» Entscheidung zu machen (Art. 22 Abs. 3). Dazu kann eine betroffene Person erwirken, dass eine mit entsprechender inhaltlicher und organisatorischer Verantwortung ausgestattete Person in die Entscheidung miteinbezogen wird. Eine betroffene Person hat zudem das Recht, ihren eigenen Standpunkt darzulegen und die automatisierte Entscheidung anzufechten und prüfen zu lassen.

[Rz 27] Diese kurze Darstellung der (Un-)Vereinbarkeit der Datenschutzregeln mit den Analysetechnologien sollte eine gewisse Vorstellung davon vermitteln, dass es die DSGVO den Nutzniessern von Profiling und automatisierten Entscheidungen in der Praxis nicht einfach macht, diese einzusetzen. Diskriminierungs- und Fairnessaspekte müssen also von datenverarbeitenden Stellen beachtet werden. Ein konkretes Diskriminierungsverbot gibt es allerdings nicht. Frag-

33 Kühling/Buchner/Buchner, DSGVO (Fn. 11), Art. 22 N. 36.

34 Die Ausnahmen sind auch dann einschlägig, wenn eine automatisierte Entscheidung für ein vorvertragliches Verhältnis erforderlich ist, siehe hierzu Fallbeispiel aus WP-29, N.251rev.01 (Fn. 26), S.23. Hingegen dürften Leistungsprofile von Arbeitnehmenden und Entscheidungen darüber (z.B. Beförderungen oder Degradierungen) nicht für einen Vertragsschluss erforderlich sein, da der Arbeitsvertrag als Rechtsgeschäft schon besteht. Zwar könnte der Standpunkt vertreten werden, dass ein solches Profil für die Erfüllung eines Arbeitsvertrags erforderlich ist. Hier knüpft die WP-29 aber zu Recht an das Erfordernis einer weniger einschneidenden Massnahme an (siehe WP-29, N.251rev.01 (Fn. 26), S.23). Wenn sich Arbeitgeber mehr auf einen Algorithmus verlassen, als z.B. ein persönliches Gespräch mit Mitarbeitenden zu suchen, realisiert sich genau das Risiko, welches Art. 22 verhindern soll, dass ein Mensch zum blossen Objekt eines computergestützten Verfahrens wird.

35 Kühling/Buchner/Buchner, DSGVO (Fn. 11), Art. 22 N. 31; mehr zu den Sanktionen unter III.2.b).

lich ist daher, wie ein Schutz vor Diskriminierungen und Ungleichbehandlungen aus der DSGVO erwirkt werden kann. Dazu nun der letzte Abschnitt:

2. Kann aus der DSGVO ein Schutz vor Diskriminierung und Ungleichbehandlung abgeleitet werden?

[Rz 28] Die DSGVO enthält bestimmte Rechte für betroffene Personen und Pflichten für die datenverarbeitenden Stellen. Damit gibt sie den Betroffenen gewisse Instrumente in die Hand, die auch in Diskriminierungsfällen zur Anwendung kommen können. Instrumente, die aber auch die datenverarbeitenden Stellen dazu bringen oder sogar zwingen können, den Einsatz und die Auswirkungen von Analysetechnologien sorgfältig auf Diskriminierungsrisiken zu prüfen und mögliche Risiken zu minimieren. Aus den Vorschriften der DSGVO lassen sich dafür drei Kategorien bilden: (1) Auskunfts- und Informationsrechte, die den Zugang zu Informationen zu den Datenverarbeitungs- und Entscheidungsprozessen und den Nachweis von möglichen Diskriminierungen erleichtern, (2) Sanktionen und Schadensersatz, die Verstösse gegen datenschutzrechtliche Vorschriften drastisch ahnden können und damit einen Anreiz für datenschutzkonforme Verfahren bieten und (3) Massnahmen zur Risikominimierung sowie Compliance-Massnahmen, mit denen Diskriminierungsrisiken gemindert und ausgeschlossen werden können.

a. Auskunfts- und Informationsrechte

[Rz 29] Faire, diskriminierungsfreie Datenverarbeitungsprozesse erfordern Transparenz; ein Erfordernis, mit dem Analysetechnologien nicht immer im Einklang stehen. Für Profiling und automatisierte Entscheidungen dürften daher die Auskunfts- und Informationsrechte an Bedeutung gewinnen. Art. 13 und 14 enthalten Informationsrechte für Betroffene. Noch bevor das Profiling durchgeführt wird, muss die datenverarbeitende Stelle aktiv und ohne Aufforderung verständlich erklären, wie ein Profilingprozess abläuft. Das heisst insbesondere, eine Person darüber zu informieren, dass sie Objekt eines Profilings wird und welche Auswirkung diese Massnahme für die betroffene Person hat[36]. Hierzu gehört auch die Information, ob eine Entscheidung über das Profilingergebnis getroffen wird, unabhängig davon, ob die Entscheidung eine «menschliche» oder eine automatisierte ist[37]. Bei einer automatisierten Entscheidung muss insbesondere auch deren Ablauf erläutert sowie über die Rechte aufgeklärt werden, die sich für Betroffene aus Art. 22 Abs. 3 ergeben.

[Rz 30] Art. 15 gewährt Betroffenen ein Auskunftsrecht auf weitergehende Informationen. Während die datenverarbeitende Stelle nach Art. 13 und 14 nur darüber informieren muss, welche Kategorien an personenbezogenen Daten verarbeitet werden, kann eine betroffenen Person nach Art. 15 insbesondere in Erfahrung bringen, welche ihrer personenbezogenen Daten für das Profiling und automatisierte Entscheidungen konkret verwendet worden sind[38].

36 Vgl. WP-29, N.251rev.01 (Fn. 26), S. 16.

37 Vgl. Kühling/Buchner/Bäcker, DSGVO (Fn. 11), Art. 13 N. 53.

38 Vgl. WP-29, N.251rev.01 (Fn. 26), S. 17.

[Rz 31] Für den Nachweis von Diskriminierungen durch Analysetechnologien dürften «aussagekräftige Information über die involvierte Logik» immer mehr an Bedeutung gewinnen[39]. Nur ein gewisses Verständnis darüber, wie es zum Profilingergebnis oder wie der Computer zu seiner Entscheidung kommt, verhilft einer betroffenen Person, Diskriminierungen überhaupt aufzudecken und auch nachzuweisen. An dieser Stelle werden seitens der Privatwirtschaft grosse Bedenken geltend gemacht, dass diese Forderung zur Offenlegung von Algorithmen führt und damit der Schutz von Geschäftsgeheimnissen verletzt wird. Dass ein Algorithmus offengelegt werden muss, ist jedoch nicht zwingend notwendig. Der betroffenen Person sollte in einfachen Worten eine Begründung geliefert werden, wie der Verarbeitungs- oder Entscheidungsprozess abläuft, insbesondere welche Kriterien für das Ergebnis ausschlaggebend sind. Am Beispiel eines Scorings im Rahmen einer Kreditvergabe sollte z.B. eine Bank darüber informieren, welche die Hauptkriterien sind, die zum Scoringergebnis geführt haben, inklusive einer Information über die das Hauptkriterium bestimmende Daten, deren Herkunft und ihre Relevanz[40].

[Rz 32] Auch Widerspruchs- und Anfechtungsrechte können Transparenz und Fairness erzwingen. Gegen ein Profiling kann Widerspruch eingelegt werden, um damit entweder ein noch nicht begonnenes Profiling zu verhindern oder ein bereits begonnenes Profiling zu unterbinden[41]. Eine automatisierte Entscheidung kann, wie bereits dargelegt, angefochten werden[42]. Aktuell gibt es Überlegungen, aus Art. 22 ein gesondertes Recht auf eine individuelle Erläuterung der Entscheidung abzuleiten, welches auch noch nach einer Entscheidung ausgeübt werden kann und welches durch Anwendung einer bestimmten mathematischen Methode die Entscheidung für die Betroffenen nachvollziehbar macht, ohne in Konflikt mit Geschäftsgeheimnissen zu kommen[43].

b. Sanktionen und Schadensersatz

[Rz 33] Verstösse gegen die Vorschriften der DSGVO können ernsthafte Sanktionen in Form von drastisch hohen Geldbussen[44] und Schadensersatzansprüche von Betroffenen nach sich ziehen. Die hohen Geldbussen bieten Betroffenen zwar keinen direkten Rechtsschutz gegen diskriminierende Massnahmen. Diskriminierung durch Analysetechnologien bieten allerdings eine Angriffsfläche für Verstösse gegen die DSGVO. Hintergrund sind die (str-)engen Rechtmässigkeitsvoraussetzungen, denen Profiling und automatisierte Entscheidungen unterliegen. Die Fehleranfälligkeit eines Profilingprozesses im Zusammenhang mit Diskriminierungen und Ungleichbehandlungen, insbesondere durch Verstösse gegen die Datenschutzgrundsätze, wurde bereits

39 Art. 13 Abs. 2 lit. f), Art. 14 Abs. 2 lit. g) und Art. 15 Abs. 1 lit. h) DSGVO.

40 «The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision.» WP-29, N.251rev.01 (Fn. 26), S.25. Siehe dazu auch das Fallbeispiel WP-29, N.251rev.01 (Fn. 26), S.24, 25.

41 Art. 21 DSGVO – Widerspruch gegen Verarbeitungen aufgrund von Art. 6 Abs. 1 lit. e) oder f) DSGVO.

42 Siehe unter III.1.b).

43 Es gibt Stimmen, die die Informations- und Auskunftsrechte als nicht ausreichend ansehen, da sie nicht im Nachhinein, also nach einem Profiling oder einer automatischen Entscheidung geltend gemacht werden können. Siehe Sandra Wachter, Brent Mittelstadt und Luciano Floridi, «Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation», Dezember 2016, International Data Privacy Law 2017 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469, Website zuletzt besucht am 31. Juli 2018); Zu Vorschlag, wie ein Recht auf Erklärung ausgestaltet sein könnte, siehe Sandra Wachter, Brent Mittelstadt und Chris Russel, «Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, Oktober, 2017, Harvard Journal of Law & Technology, 31 (2), 2018 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289, Website zuletzt besucht am 31. Juli 2018).

44 Bis zu 20 Mio. Euro oder 4% des weltweit erzielten Jahresumsatzes, Art. 83 Abs. 6 DSGVO

an anderer Stelle erläutert[45]. Erscheint eine automatisierte Entscheidung diskriminierend, ist deren Zulässigkeit zweifelhaft und es sollte unbedingt geprüft werden, ob die Ausnahmen aus Art. 22 Abs. 2 vorliegen, sensible Daten für die Entscheidungsfindung genutzt worden (auch aus dem Profiling neu hervorgebrachte sensible Daten) und ob die Massnahmen nach Art. 22 Abs. 3 vorgenommen worden sind[46].

[Rz 34] Erleiden Betroffene aus der Diskriminierung einen Schaden oder Nachteil kann unter Umständen Schadensersatz von der datenverarbeitenden Stelle gefordert werden. Dazu muss ein Verstoss gegen die DSGVO geltend gemacht werden[47]. Ein solcher wird bereits als gegeben angesehen, wenn eine Analyse auf falschen Informationen beruht und z.B. zu einer Nichteinstellung oder einem Vertragsabschluss mit schlechteren Konditionen führt[48].

[Rz 35] Es ist also nicht unwahrscheinlich, im Fall einer Diskriminierung oder Ungleichbehandlung auf Verstösse gegen die DSGVO zu stossen. Es «lohnt» sich also für Betroffene, diskriminierendes oder unfair erscheinendes Profiling und automatisierte Entscheidungen auf ihre datenschutzrechtliche Zulässigkeit zu prüfen. Die hohen Geldbussen und Schadensersatzmöglichkeiten bei Verstössen sollten für datenverarbeitende Stellen Anlass genug sein, Datenverarbeitungsprozesse sorgfältig auszuführen, möglicherweise von Massnahmen sogar abzusehen, wenn sich ein Diskriminierungsrisiko nicht verhindern lässt. Mit der Einführung eines Verbandsklage- und -beschwerderechts ist zudem zu vermuten, dass es für betroffenen Personen zunehmend einfacher wird, ihre Rechte bei Verstössen gegen die DSGVO geltend zu machen[49].

c. Massnahmen zur Risikominimierung und Compliance-Massnahmen

[Rz 36] Datenverarbeitenden Stellen sollte der sog. risikobasierte Ansatz der DSGVO bekannt sein[50]; die nachweispflichtige Verantwortlichkeit darüber, Risiken bei der Verarbeitung von personenbezogenen Daten zu evaluieren und je nach Risiko geeignete technische und organisatorische Massnahmen zur Risikoabwendung zu ergreifen. Zu diesen Risiken gehören auch Diskriminierungsrisiken bei Profilingmassnahmen und automatisierten Entscheidungen[51], die also in jedem Fall evaluiert und abgewendet werden müssen. Ein wesentliches Instrument hierfür ist die Datenschutz-Folgenabschätzung (DPIA)[52], ein gesetzlich beschriebenes Verfahren zur Risikoevaluierung und zur Ausarbeitung von Abhilfemassnahmen und Sicherheitsvorkehrungen. Diese ist zwingende Voraussetzung für ein Profiling mit personenbezogenen Daten[53]. Da das Thema Fairness und Gerechtigkeit bei Datenverarbeitungen zunehmend an Bedeutung gewinnt, ist zu

45 Siehe «Zulässigkeit von Profilingmassnahmen» unter III.1.a).

46 Siehe «Zulässigkeit von automatisierten Entscheidungen» unter III.1.b).

47 Art. 82 DSGVO.

48 Vgl. Kühling/Buchner/Bergt, DSGVO (Fn. 11), Art. 82 N.19.

49 Verbandsklage- und -beschwerderecht, Art. 80 DSGVO. Eine sich dem Datenschutz verschriebene NGO hat sich bereits unter dem Datenschutzverfechter und «Facebook-Widersacher» Max Schrems gebildet (siehe https://noyb.eu/team?lang=de, Website zuletzt besucht am 31. Juli 2018).

50 Art. 24 DSGVO.

51 Siehe ausführlicher EG 75 DSGVO.

52 Data Protection Impact Assessment, Art. 35 DSGVO.

53 Art. 35 Abs. 3 lit. a) DSGVO schreibt eine Datenschutz-Folgenabschätzung für die Durchführung eines Profilings vor.

vermuten, dass in einer DPIA mittlerweile auch die Evaluierung von Diskriminierungsrisiken und entsprechende Abhilfe gefordert wird.

IV. Zusammenfassung und Fazit

[Rz 37] Intelligente Analysetechnologien treffen mit Hilfe von Daten Aus- oder Vorhersagen zu menschlichen Verhaltensweisen, Leistungsfähigkeiten und anderen Charakteristika. Aus der Fülle der uns vorliegenden und täglich neu generierten Daten können Algorithmen statistische Zusammenhänge ermitteln. Daraus lassen sich bestimmte Merkmale ableiten, die zu Profilen von «erwünschten» oder «unerwünschten» Menschen zusammengefasst werden können. Diese Profile sind somit gewissermassen ein «Spiegel der Gesellschaft». Insbesondere die für die Profilbildung erforderlichen Daten spiegeln die in der Gesellschaft bestehenden Vorurteile und entsprechendes Diskriminierungsverhalten wieder und bieten damit Algorithmen die Vorlage, ebenso zu agieren. So werden vorurteilsbelastete und auf Stereotypen gestützte oder gänzlich neue Kategorien gebildet, in die Menschen eingeordnet werden können. Das kann zu fehlerhaften Schlussfolgerungen über eine Person und damit zu ungerechten und diskriminierenden Ergebnissen und digitalen Ungleichheiten führen.

[Rz 38] Digitale Ungleichbehandlungen überschreiten in der Regel die Grenzen des klassischen Anti-Diskriminierungsrechts. Neue digital erstelle Diskriminierungsmerkmale sind gesetzlich nicht geschützt; die Technologien sind für Laien kaum nachweisbar. Datenschutzrechtlich unterliegen Datenanalysen über Menschen dem Konzept des Profilings, einer in der DSGVO geregelten speziellen Datenverarbeitungsmethode. Entscheidungen, gestützt auf ein Profilingergebnis allein durch einen Computer, ohne menschliches Zutun, sind Gegenstand des Art. 22 DSGVO. Vor diesem datenschutzrechtlichen Hintergrund spielen auch Diskriminierungsrisiken eine Rolle. Ein direktes Verbot von Diskriminierungen gibt es in der DSGVO zwar nicht. Auch ist die DSGVO kein «Allheilmittel» gegen Diskriminierungen und Ungleichbehandlungen. Diskriminierungs- und Fairnessaspekte müssen dennoch im datenschutzrechtlichen Kontext Berücksichtigung finden. Insbesondere bietet eine digitale Diskriminierung eine Angriffsfläche für datenschutzrechtliche Verstösse, die mit drastisch hohen Geldbussen sanktioniert werden können. Datenverarbeitende Stellen sollten deshalb das Thema Diskriminierung durch Analysetechnologien hinreichend ernst nehmen. Die DSGVO bietet Instrumente an, Diskriminierungsrisiken zu erkennen, zu vermindern oder sogar auszuschliessen. Dazu gehört in erster Linie ein sorgfältiger Umgang mit den Vorschriften der DSGVO. Allein die Einhaltung der datenschutzrechtlichen Prinzipien aus Art. 5 DSGVO dürfte einen wesentlichen Teil des Risikos bereits minimieren.

[Rz 39] Das sollte auch in der Schweiz berücksichtigt werden. Zwar gilt die DSGVO, im Gegensatz zu den EU-Mitgliedsstaaten, in der Schweiz nicht direkt und unmittelbar. Die Verordnungsgeber haben jedoch den Geltungsbereich der DSGVO auch auf Gebiete ausserhalb der EU ausgedehnt. Gerade im Hinblick auf Profiling sollte Art. 3 Abs. 2 lit. b) beachtet werden, der den Anwendungsbereich auch auf Nicht-EU-Staaten ausdehnt. Unabhängig davon, ob eine Niederlassung im EU-Raum besteht, ist die DSGVO für Schweizer Unternehmen oder Institutionen anwendbar, wenn Verhaltensprofile aufgrund von Internetaktivitäten von Personen im EU-Raum durchgeführt werden[54]. Aber auch dann, wenn kein EU-Sachverhalt vorliegt, darf vermutet werden, dass

54 Siehe hierzu EG 24 DSGVO.

die Schweiz sich im Rahmen der Datenschutzrevision den EU-Datenschutzstandards anpasst und digitale Diskriminierungssachverhalte ähnlich beurteilen wird.

Romy Daedelow, Ass. iur, Doktorandin am Lehrstuhl für Soziales Privatrecht von Prof. Dr. Kurt Pärli, Universität Basel, Schweiz

Der Beitrag ist anlässlich der Law & Robots Tagung 2018 an der Universität Basel mit dem Thema «Predictive Analytics bei Versicherungen und in der Arbeitswelt: Diskriminierung durch Algorithmen» entstanden. Auf dieser Tagung ist das Thema Diskriminierung durch Algorithmen durch mehrere Vorträge aus verschiedenen Perspektiven und Fachrichtungen näher beleuchtet worden. Einen diesbezüglichen Vortrag hielt neben der Autorin dieses Beitrags auch eine der Herausgeberinnen dieser Jusletter-Sonderausgabe «Algorithmen und Recht», Prof. Dr. Isabelle Wildhaber. Die Autorin dankt den Herausgeberinnen, Frau Prof. Dr. Wildhaber und Frau Prof. Dr. Lohmann für die Ermöglichung der Veröffentlichung ihres Beitrags.