PROFILING, BIG DATA, ARTIFICIAL INTELLIGENCE UND SOCIAL MEDIA – GEFAHREN FÜR EINE GESELLSCHAFT OHNE EFFEKTIVEN DATENSCHUTZ

*Indra Spiecker genannt Döhmann**

Abstract: Der Beitrag behandelt drei zentrale Herausforderungen für den Datenschutz - Profiling, Big Data und Künstliche Intelligenz sowie die Datenverarbeitung in Sozialen Netzwerken und auf Plattformen. Er schildert die Problemlagen und zeigt auf, wo die DSGVO Regelungen trifft und wo Regelungslücken bestehen.

Inhaltsverzeichnis

* Die Autorin dankt Loïc Reissner für die kluge Unterstützung bei der Recherche/Fußnoten.

I. VORWORT

Erich Schweighofer hat in jeder Hinsicht Neuland betreten, er ist immer ein Grenzgänger gewesen. Seine Vita zeigt das eindrucksvoll: Es dürfte nicht viele Juristen geben, die mit Selbstverständlichkeit und größter Kompetenz mit Informatikern, Juristen und Ökonomen auf Augenhöhe diskutieren und forschen können – und sich dabei noch eigene Ansichten zutrauen, die auch noch aus einer reichhaltigen und breit gefächerten Erfahrung in der österreichischen und europäischen Verwaltungserfahrung schöpfen. Zudem hat er das Gebiet der Rechtsinformatik in der jüngeren Vergangenheit fast alleine im deutschsprachigen Raum besetzt. Seine Habilitation zur automatischen Textanalyse ist hierfür ein ganz wesentlicher Beleg. Ein wichtiges Bindeglied seiner vielfältigen Interessen ist die Regulierung von «Information» – weshalb sich auch das juristische Spektrum über eine Vielzahl von Rechtsgebieten erstreckt und durchaus auch in das Zivilrecht ausschreitet.

Die Autorin kennt und schätzt den Jubilar seit vielen Jahren, wenngleich erst aktuell eine gemeinsame Forschungstätigkeit im Projekt «SmartIdentification» gelungen ist – länderüberschreitendes Projekt zur datenschutzgerechten Überwachung von Grenzen. Auch hier geht dieser nicht die bekannten und einfachen Wege, sondern wagt sich an heikle Rechtsfragen und offene gesellschaftliche Problemstellungen heran.

Der folgende Beitrag, ein Übersichtsbeitrag über verschiedene hochproblematische Fallkonstellationen im Datenschutzrecht, aus dem Blickwinkel der DSGVO betrachtet, greift diese Zusammenarbeit in diesem Projekt auf, erweitert sie aber auf die grundlegenden Fragestellungen. *Erich Schweighofer* hat Datenschutz immer als ein Instrument begriffen, um Machtasymmetrien einzudämmen, die aus einem ungebremsten Informations- und Informationstechnologiezugang entstehen können. Dieses Problem ist bei Profiling, Scoring und Sozialen Netzwerken unverändert wirkmächtig. Es ist der

Gesellschaft und der Wissenschaft zu wünschen, dass wir auch weiterhin aus der Arbeitsgruppe Rechtsinformatik wesentliche Impulse erhalten!

II. EINLEITUNG UND HINTERGRUND

Seit Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DSGVO). Sie löste – nach zweijähriger Vorlaufzeit – die bisherige Europäische Datenschutz-Richtlinie von 1995 und die sie umsetzenden nationalen Datenschutzregelungen ab.

Inhaltlich hat sich durch die DSGVO wenig verändert. Sie behält die wesentlichen Grundsätze des Datenschutzes bei. So ist das Verbotsprinzip (Verbot, Daten zu verarbeiten, wenn nicht eine Einwilligung oder eine andere rechtliche Grundlage vorliegt) beibehalten (Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1), gilt weiterhin die Einwilligung als zentraler Ausdruck der Selbstbestimmung des Datensubjekts über die sie betreffenden Informationen (Art. 4 Nr. 11, Art. 7, Art. 6 Abs. 1 lit. a)[1], gibt es weiterhin eine unabhängige Datenschutzaufsicht (Art. 52), zusätzlich hat das Datensubjekt auch weiterhin ein Recht auf Auskunft, Löschung, Sperrung, Widerspruch und Information (Artt. 14ff.), gilt es bei der Datenverarbeitung zentrale Prinzipien wie Datenminimierung (Art. 5 Abs. 1 lit. c), Zweckbindung (Art. 5 Abs. 1 lit. b) oder Transparenz (Art. 5 Abs. 1 lit. a) zu wahren.

Angesichts der Erfahrungen mit der Rechtslage unter der der Datenschutz-Richtlinie verwundert dieses Vorgehen nicht: Es bestand weitgehend und recht schnell Einigkeit darüber, dass Datenschutz und Privatheit weiterhin in der EU erhebliche Geltung beanspruchen sollen – nicht zuletzt wegen der Vorgaben in Artt. 7 und 8 Europäische Grundrechtecharta und Art. 16 Abs. 1 AEUV. Zu einer grundsätzlichen Neukonzeption hatte die EU-Kommission keinen Anlass gesehen. Vielmehr sollte mit der DSGVO auf diverse Defizite und negative Erfahrungen reagiert werden. Dazu gehörte – neben der stark gewachsenen Bedeutung des Internets – das massive Vollzugsdefizit, das dazu geführt hatte, dass bestehendes Recht nicht um- und durchgesetzt wurde und stattdessen ein «Recht des Stärkeren» galt. Mit der DSGVO sollte also auch ein level-playing field

[1] Siehe HORNUNG/SPIECKER GENANNT DÖHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 212.

erreicht werden, das Datenschutzcompliance nicht länger zum Wettbewerbsnachteil werden lassen würde. Dazu gehörte auch die hohe Unterschiedlichkeit des angewandten Rechts in den verschiedenen Mitgliedstaaten einschließlich zum Teil widersprüchlicher Einschätzungen der Datenschutz-Aufsichtsbehörden.

Daher legt die DSGVO ihren Schwerpunkt auf eine Stärkung des Vollzugs.[2] Die Aufsichtsbehörden haben in der Konsequenz einen Aufgaben- und Befugniskatalog erhalten (Art. 57 und Art. 58), mit der Einrichtung des sog. «One-Stop-Shops» und einer führenden Aufsichtsbehörde (Art. 56) wird für grenzüberschreitend tätige Datenverarbeiter grundsätzlich ein Ansprechpartner in der gesamten EU zur Verfügung gestellt; parallel dazu sorgt das Kohärenzverfahren (Artt. 63ff.) für eine einheitliche Entscheidungspraxis aller Aufsichtsbehörden. Erhebliche Sanktionen fordern die Einhaltung der DSGVO ein.

Neu sind zudem einzelne Instrumente, z.B. die sog. Risikofolgenabschätzung (Art. 35) oder auch das Recht auf Datenportabilität (Art. 20). Damit haben – neben dem Persönlichkeitsschutzrecht und dem Technikrecht – nunmehr eindeutig auch verbraucher- und wettbewerbsrechtliche Instrumente Einzug gehalten; die Risikofolgenabschätzung kann zudem als ein Instrument eines risikobasierten Datenschutzrechts verstanden werden, das der DSGVO ansonsten nicht zu eigen ist.

Mit der DSGVO besteht nunmehr ein einheitlicher europäischer Rechtsrahmen. Mit seiner Hilfe können nun eine Vielzahl an Fragestellungen rund um die Digitalisierung im Zusammenhang mit personenbezogenen Daten bearbeitet werden. Drei Problembereiche, die technisch und gesellschaftlich von hoher Relevanz sind, sollen herausgegriffen werden, nämlich Profiling und Scoring (II.), die ganz erheblich auf die Techniken von Big Data und Künstlicher Intelligenz aufbauen (III.), sowie der Umgang mit Datenverarbeitung in Sozialen Medien (IV.). Für alle drei Bereiche gilt, dass einerseits die vielen Aussagen der am Gesetzgebungsverfahren Beteiligten den Schluss zulassen, dass sie von der DSGVO adressiert werden sollten, dass sie aber andererseits kaum konkrete Regelungen in der DSGVO gefunden

[2] Siehe HORNUNG/SPIECKER GENANNT DÖHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019,Einleitung Rn. 214.

haben und somit ihre Legitimität weitgehend durch Auslegung und systematische Interpretation ermittelt werden muss. Ein Fazit und Ausblick beschließen den Beitrag (V.).[3]

III. PROFILING UND SCORING: PERSONALISIERUNG DURCH DIGITALISIERUNG

1. Profiling und Scoring

Eine der vielen neuen Möglichkeiten durch die automatisierte Auswertung von Daten besteht darin, Profile von Personen zu erstellen. Das Scoring ist eine Unterform des Profilings,[4] bei dem die Zuschreibung von Eigenschaften oder einem zukünftigen Verhalten in einem mathematischen Wert abgebildet wird, also z.B. die Festlegung der Kreditwürdigkeit oder die Wahrscheinlichkeit des Eintritts bestimmter Versicherungs- oder Ausfallrisiken durch einen bestimmten Wert auf einer Skala.[5]

Das Verhältnis zwischen dem Datenverarbeiter, der diese Profile erstellt, und den Datensubjekten kann dabei sehr vielgestaltig sein, und ebenso können die Datenquellen sehr unterschiedlich ausgestaltet sein. Vorstellbar sind alle Kombinationen; längst gibt es einen Markt für den Ankauf sowohl von Rohdaten als auch von Profilen.

Es kann sich um Nutzer handeln, deren Daten aus dem konkreten Verhältnis zur Erbringung von Diensten ausgewertet werden, z.B. im Rahmen eines Online-Einkaufs oder eines Sozialen Netzwerks. Es kann sich um Fremde handeln, deren allgemein verfügbare Daten zusammengeführt werden, z.B. im Rahmen von Online-Marketing-Agenturen. Es kann sich um Dritte handeln, deren Daten gezielt zur Auswertung für bestimmte Zwecke übermittelt werden, z.B. bei einer Kreditvermittlungsagentur.

---

[3] Der Beitrag bezieht einige bereits früher publizierte Erkenntnisse ein, nämlich SPIECKER GENANNT DÖHMANN, K&R 2012, S. 717; CR 2016, S. 698; VVDStRL 2018, S. 9; GRUR 2019, S. 341.

[4] Siehe EHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Anhang 2 zu Art. 6 Rn. 19.

[5] Vgl. auch ROßNAGEL, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 8.

2. Die Bedeutung des Profilings durch Personalisierung

Mit dem Profiling werden die Möglichkeiten der Digitalisierung dazu genutzt, den Einzelnen zunächst mittels Algorithmen aufgrund bestimmter Eigenschaften einer Gruppe zuzuweisen.[6] Dieser Gruppe sind – erneut durch mathematische Verfahren und zunehmend unter Einsatz von Big Data und Data Mining Techniken – ihrerseits eine Reihe von Eigenschaften zugewiesen. In Rekombination der Einzel- und Gruppendaten wird der Einzelne einsortiert und eingruppiert. Seine Neigungen, Präferenzen, Entscheidungen und Verhalten werden analysiert und darauf basierend für die Zukunft vorherbestimmt, um ihm individualisierte, benutzerspezifisch aufbereitete Angebote zu machen oder seine Entscheidungen zu beeinflussen. Der Möglichkeitsraum des Einzelnen wird dadurch einseitig und für ihn kaum auflösbar vorher- und fremdbestimmt.[7]

Solche Aussagen, die allein auf statistisch-mathematischen Analyseverfahren (Algorithmen) beruhen, können den Einzelnen unzutreffend beschreiben,[8] zumal der Einzelnen diese Aussagen über sich selbst oftmals nicht kontrollieren kann und nicht einmal selbst kennt[9]. Zudem kann die Katalogisierung und Gruppierung von Personen auch zu fehlerhaften, ungerechten und diskriminierenden Urteilen über eine Person führen.[10] Als davon Betroffener kann ein Einzelner zumeist die dem Profiling zugrundeliegenden Verarbeitungsprozesse weder nachvollziehen noch die Richtigkeit eines bestimmten Auswertungsergebnisses hinreichend kontrollieren.[11] Die Ergebnisse, die mittels Profiling erzielt werden, können also erhebliche Eingriffe in Rechte einer Person bedeuten; sie können ein Gefühl des Ausgeliefertseins und der

---

6 Zu den folgenden Ausführungen siehe bereits SPIECKER GENANNT DÖHMANN, VVDStRL 2018, S. 9, insb. 37ff.

7 Vgl. SPIECKER GENANNT DÖHMANN, VVDStRL 2018, S. 9, 37ff.

8 Vgl. BRITZ, Einzelfallgerechtigkeit versus Generalisierung, 2008.

9 Vgl. ROßNAGEL, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 9.

10 Siehe FRÖHLICH/SPIECKER GENANNT DÖHMANN, Verfassungsblog, 2018/12/26, https://doi.org/10.17176/20190211-224048-0.

11 Vgl. ROßNAGEL, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 9.

Fremdbeobachtung produzieren[12]. Ihren Ursprung finden diese auch in den zugrundeliegenden Datenverarbeitungen[13].

Die Gefahren für den Einzelnen und eine offene Gesellschaft, die seit den Anfängen des Datenschutzes gesehen wurden,[14] verwirklichen sich im Profiling. Die Fähigkeit des Datensubjekts, Einfluss auf die Umwelt zu nehmen, reduzieren sich dramatisch. Denn in Entscheidungen, die über ein Datensubjekt getroffen werden, sind die eingeflossenen Profile und Daten nicht mehr erkennbar; der Einzelne hat keine Möglichkeit, sich gegen einzelne Elemente eines Profils und des dahin führenden Verfahrens zu wehren, weil er noch nicht einmal erkennen kann, welche Daten unter welchen mathematischen Bedingungen zu welchem Zwischenergebnis geführt haben, um ihm dann eine Leistung bestimmter Art und Güte zu einem bestimmten Preis anzubieten oder auch zu verwehren.

Mit Hilfe von Profiling wird nämlich eine umfassende Personalisierung möglich. Diese ermöglicht flächendeckend die einseitige Entscheidungsbeeinflussung des Datensubjekts. Als Beispiel für diese, die Freiheitlichkeit einschränkenden Vorgehensweisen mögen die Verfahren der dynamisierten und personalisierten Preisfestsetzung[15] – z.B. Flugpreisanpassungen je nach Häufigkeit der Nachfrage – dienen. Der Nutzer hat keine Kenntnis der Beurteilungsgrundlagen und -maßstäbe, kann diese nicht kontrollieren und wird deshalb manipulierbar. Denn Auskunftsrechten über Personalisierung jeglicher Art wird – bisher erfolgreich – der Schutz der Betriebs- und Geschäftsgeheimnisse entgegengehalten[16].[17]

---

12 Vgl. Roßnagel, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 9.

13 Zum Problem der Datenqualität etwa Stevens, CR 2019, i.E.

14 Siehe Simitis/Hornung/Spiecker genannt Döhmann, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 10 und Rn. 22.

15 Siehe Ezrachi, Virtual Competition. The promise and perils of the Algorithm Driven Economy, 2016; Hong, Journal of Marketing Research 48 (2011), 48 ff.

16 Siehe nur für das deutsche Recht die sog. Schufa-Entscheidung des höchsten Zivilgerichts Bundesgerichtshof, BGHZ 200, 38.

17 Spiecker genannt Döhmann, VVDStRL 2018, S. 9, 44.

Mit solchen Einschätzungen auf der Basis von massenhaften Datenauswertungen kann der Zugang zu Leistungen aller Art – sei es staatlichen, sei es privaten – davon abhängig gemacht werden, wie das Individuum typisiert und einsortiert wird. Personalisierte, auf Formeln basierende Aussagen über das zukünftige Verhalten bestimmen bei ungehindertem Einsatz den Freiheitsraum des Einzelnen, auch für sich selbst. Denn der personalisierte Zugang zu seiner Umwelt und die gezielte Manipulation führen in eine weiter gesteigerte Selbstbezüglichkeit.[18] Die Sortierung und konsequente Herausbildung von Parallelwelten wird zum Kernelement einer digitalisierten Gesellschaft; Dezentralisierung und Fragmentierung lösen sich aus dem kontinuierlichen Wechselspiel zur Einheit.

Wer meint, das sei allenfalls weit entfernte Zukunftsmusik: Längst haben Entscheider aller Art einschließlich des Staates diese Möglichkeiten der planvollen, einseitigen Separierung von Bürgern und Kunden erkannt. Ein staatlicher «Citizen Score» wie in China mag zwar derzeit in Europa unvorstellbar sein. Danach entscheidet ein Gesamtwert, in den Werte über soziales Verhalten einschließlich des persönlichen Umfelds einfließen, über Teilhabe und Zugang zu staatlichen und privaten Leistungen.[19] Ähnliche Ausprägungen der Gefahrenabwehr im «predictive policing»[20] werden allerdings

---

[18] Im Falle eines solchen perfektionierten personalisierten Lebens nähert sich der Nutzer dem kommunikativ isolierten Menschen an; er begegnet über den alles könnenden Apparat nur noch sich selbst. Diese totale Selbstbezüglichkeit würde den völligen Verlust der Teilhabe an einer – wie auch immer – vereinheitlichenden Öffentlichkeit bedeuten, Vgl. SCHULZE, Neue Mediengesellschaft: Droht das Kaspar-Hauser-Syndrom?, Tendenz 1995, 42 (43); BERGSDORF, Journalistische Ethik in der Informationsgesellschaft, in: GOURD/NOETZEL (Hrsg.) Zukunft der Demokratie in Deutschland, 2001, 392 f.; DERS. Herausforderungen der Wissensgesellschaft, 2006, 62 f. Diese narzisstische Komponente neuer Kommunikationsformen betont HAN, Im Schwarm, 2013, 65.

[19] Siehe dazu z.B. MEISSNER, MERCIS China Monitor: Chinas gesellschaftliches Bonitätssystem, abrufbar unter https://www.merics.org/fileadmin/user_upload/downloads/China-Monitor/merics_ChinaMonitor_39_deutsch_Web.pdf; http://www.faz.net/video/medien/punktrichter-citizen-score-ueberwachung-in-china-13848403.html; http://www.faz.net/video/medien/punktrichter-citizen-score-ueberwachung-in-china-13848403.html; http://www.deutschlandfunkkultur.de/chinas-sozialkredit-system-auf-dem-weg-in-die-it-diktatur.979.de.html?dram%3Aarticle_id=395126; siehe auch https://netzpolitik.org/2015/dystopia-wird-wirklichkeit-was-ist-dran-an-chinas-social-credit-system/.

[20] Man denke nur an Predictive Policing, das nicht nur auf (öffentliche) Räume, sondern auch auf Personen angewendet wird, auch wenn es derzeit noch sehr umstritten ist, vgl. RADEMACHER,

auch in den westlichen Demokratien trotz erheblicher rechtsstaatlicher Bedenken[21] bereits eingesetzt. Wenn nicht sehr genaue Rahmenbedingungen geschaffen werden, um solche Verfahren einzuhegen, besteht tatsächlich eine ernstzunehmende Möglichkeit, dass Digitalisierung genutzt wird, um die informationellen Vorsprünge gegenüber dem Einzelnen in eine nicht mehr zu überwindende und zu beherrschende Macht des Staates sowie einzelner Informationsintermediäre und -konzerne und derjenigen umzusetzen, die über die Auswertungstechnologie verfügen.

Denn beherrschend sind dann die Parallelwelten derjenigen, die über die Daten und die Algorithmen verfügen, nicht die Selbstbestimmtheit des Bürgers. Für das deutsche Recht bedeutete dies, dass fehlende Transparenz und fehlende Kontrolle den Bürger wider Art. 1 Abs. 1 GG zum Objekt machten, ihm den Wesensgehalt der Freiheitsgrundrechte nähmen und sein Recht auf (Un-)gleichbehandlung aus Art. 3 Abs. 1 GG[22] bedrohten – von einer freien und gleichen Wahl nach Art. 38 Abs. 1 GG als Voraussetzung von repräsentativer Demokratie[23] ganz zu schweigen.[24] Ganz ähnlich wäre dies auch für den gesamten Bereich der EU trotz unterschiedlicher individueller Verfassungen in den Mitgliedstaaten nicht zuletzt aufgrund der gemeinsamen europäischen Verfassungstradition und der Vorgaben der EU-Charta zu sehen.

Predictive Policing im deutschen Polizeirecht, AöR 2017, 366 ff.; EBERT, Entwicklungen und Tendenzen im Recht der Gefahrenabwehr, LKV 2017, 10 (12); LEGNARO/KRETSCHMANN, Das Polizieren der Zukunft, KrimJ 2015, 94 ff.; PERRY Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations, 2013.

21 Sehr kritisch zum Einsatz VG Koblenz DVBl. 2015, 453; dazu ALTER, Grenzziehung und Grenzüberschreitung: Zu lageabhängigen Personenkontrollen nach § 22 Ia BPolG, NVwZ 2015, 1567 (1568); GLUBA, Mehr offene Fragen als Antworten. Was für eine Bewertung des Nutzens von Predictive Policing noch zu klären ist, Die Polizei 107 (2016) 2, 53 ff.

22 Bezeichnend für die Konzentration auf das Gleichheitsgebot des Rechts aus Art. 3 GG, wenn auch unter Betonung der demokratischen Vereinheitlichungen, die daraus erwachsen, SCHORKOPF, Staat und Diversität. Agonaler Pluralismus für die liberale Demokratie, 2017, 18 ff.

23 Zur Entscheidungsfreiheit als Voraussetzung von Demokratie siehe GRZESZICK (Fn. 27), Art. 20 Rn. 17; zur staatsbürgerlichen Gleichheit z.B. BÖCKENFÖRDE (Fn. 29), Rn. 41; GRZESZICK (Fn. 27), Art. 20 Rn. 35 ff.

24 Siehe zum Vorstehenden schon SPIECKER GENANNT DÖHMANN, VVDStRL 2018, S. 9, 45.

3. DSGVO und Profiling

Angesichts dieser – längst bekannten – Auswirkungen von Profiling und darauf basierender Personalisierung sollte man meinen, dass sich die DSGVO intensiv mit deren rechtlicher Regulierung befasse und präzise Vorgaben mache.

a) Überblick

Tatsächlich findet sich in Art. 4 Nr. 4 DSGVO eine Legaldefinition. Danach ist Profiling «jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen». Die DSGVO sieht also einen sehr weiten Profiling-Begriff vor. Maßgeblich für das Profiling ist das mit der Verarbeitung verfolgte Ziel, nämlich die Bewertung bestimmter persönlicher Aspekte einer natürlichen Person,[25] ganz unabhängig von den konkreten Verarbeitungsschritten.

Auch in weiteren Vorschriften, z.B. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. f, Art. 15 Abs. 1 lit. h DSGVO, ist davon die Rede. Gezielt nimmt z.B. Art. 21 Abs. 1 Satz 1 DSGVO ein Widerspruchsrecht ausdrücklich auch für das Profiling an, ebenso für Abs. 2 für den Bereich profiling-basierten Direkt-Marketings. Art. 22 DSGVO schließlich verlangt – schon im Titel – enge Begrenzungen der Entscheidung aufgrund von Profiling. Dass der DSGVO-Gesetzgeber das Profiling als durchaus schwerwiegenden Eingriff in Datenschutz- und Privatheitsrechte einstuft, lässt sich zudem an Art. 35 Abs. 3 lit. a DSGVO erkennen, wonach eine Datenschutzfolgeabschätzung für Datenverarbeitungen mit hohem Risiko für die Rechte und Freiheiten natürlicher Personen jedenfalls beim Profiling durchzuführen ist, also Profiling per se als eine solche besonders gefährliche Datenverarbeitung gesehen wird. Weitere Regelungen ergänzen den Profiling-Rechtsrahmen der DSGVO.

---

25 BUCHNER, in: KÜHLING/BUCHNER (Hrsg.), DSGVO Kommentar, 2018, Art. 4 Nr. 4 Rn. 4.

Gleichwohl lässt sich nicht sagen, dass der DSGVO-Gesetzgeber tatsächlich das Profiling geregelt hätte – im Gegenteil. Anders als eine Vielzahl von Mitgliedstaaten, die im nationalen Recht auf der Basis der Datenschutz-Richtlinie eigenständige Vorschriften des Datenschutzes geregelt hatten, kennt die DSGVO keine Sondervorschriften für die Rechtmäßigkeit von Profiling[26]. Vielmehr sind nun, nach Wegfall der nationalen Regelungen, ganz allgemein die Vorgaben der DSGVO einzuhalten.[27]

b) Anwendbarkeit der DSGVO auf Vorgänge des Profilings

Die DSGVO kann für ein Profiling überhaupt nur als rechtlicher Rahmen herangezogen werden, wenn das Profiling auf der Verarbeitung personenbezogener Daten beruht, sich also auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO). Daher fällt die Auswertung anonymisierter Datenbestände nicht unter die Begriffsbestimmung.[28] Gerade wichtige Zwischenschritte im Profiling wie die Beurteilung von Gruppendaten und die Ermittlung der allgemeinen Aussagen durch algorithmische Verfahren werden daher von der DSGVO nicht erfasst.

c) Zweckbindung

Das Profiling unterliegt – wie jede Datenverarbeitung – dem Grundsatz der Zweckbindung, Art. 5 Abs. 1 lit. b DSGVO. Dieser Grundsatz ist deshalb für Profiling von besonderer Bedeutung, weil es nicht «das» Profiling als solches gibt, sondern vielmehr zwischen den verschiedenen Schritten unterschieden werden muss. Geht man – vereinfacht – von dem oben beschriebenen Dreischritt aus, dann sind mindestens die Schritte

---

[26] So kannte bspw. das BDSG a.F. in § 28b Sonderregelungen zum Scoring, ebenso wie zum Einsatz bestimmter Marketing-Techniken in § 30a BDSG a.F. Zu einer rechtsvergleichenden Übersicht siehe z.B. SPIECKER GENANNT DÖHMANN et. al., EDPL 2016, S. 535.

[27] So auch ROßNAGEL, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 10; BUCHNER, in: KÜHLING/BUCHNER (Hrsg.), DSGVO Kommentar, 2018, Art. 4 Nr. 4 Rn. 2; Art. 22 Rn. 4, 11; RICHTER DuD 2016, S. 581, 585; KUGELMANN, DuD 2016, S. 566, 570.

[28] ROßNAGEL, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 3.

der Erhebung von Daten und die spätere Zuschreibung von Eigenschaften aus dem Profiling von der DSGVO erfasst, da sie personenbezogene Daten erfassen.

Der Grundsatz der Zweckbindung besagt, dass eine Datenverarbeitung nur dann zulässig ist, wenn die Datenverarbeitung zu demselben Zweck erfolgt wie der vorherige Schritt, also typischerweise der Erhebung.[29] Damit wird vorgebeugt, dass einmal vorhandene Daten vom Datenverarbeiter beliebig weiterverarbeitet werden können. Dies ist im Übrigen auch ein gewichtiges Argument gegen eigentumsrechtliche Vorstellungen zum Datenschutz wie das Dateneigentum oder die Datensouveränität, denn mit der Weitergabe von Daten an einen Datenverarbeiter oder einen Dritten verliert das Datensubjekt nicht etwa seine datenschutzrechtlichen Ansprüche, weil damit nicht der Verlust der eigenen Rechtsposition einhergeht.

Werden Daten also erhoben, geschieht dies typischerweise gerade nicht zum Zwecke des Profilings, sondern vielmehr im Rahmen eines Vertrags- oder Dienstleistungsverhältnisses, bspw. im Rahmen eines Online-Versandvertrages oder auch im Rahmen der Eröffnung eines Nutzeraccounts in einem Sozialen Netzwerk. Diese Datenerhebung ist dann typischerweise über Art. 6 Abs. 1 lit. a oder b gedeckt.

Die Verwendung der Daten für Zwecke des Profilings ist allerdings von diesem ursprünglichen Zweck nicht erfasst, es handelt sich um einen neuen bzw. einen anderen Zweck.

Unter der DSRL gab es nur den ursprünglichen und den neuen Zweck. Eine Datenverarbeitung, die zur Erfüllung eines neuen Zwecks erfolgte, musste neu gerechtfertigt werden. Die DSGVO ist hier weniger strikt; sie hat in Art. 5 Abs. 1 lit. b und Art. 6 Abs. 4 DSGVO die Möglichkeit eingeräumt, dass ein neuer Zweck als sogenannter «vereinbarer Zweck» eingeordnet werden kann. In der Folge ist die Datenverarbeitung zu einem solchen vereinbaren Zweck noch von der ursprünglichen Rechtsgrundlage, also z.B. der Einwilligung nach Art. 6 Abs. 1 lit. a), Art. 7, Art. 4 Nr. 11 DSGVO oder der Vertragsabwicklung nach Art. 6 Abs. 1 lit. b DSGVO erfasst.

[29] Siehe Hornung/Spiecker genannt Döhmann, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 237.

d) Rechtsgrundlage für die Verarbeitung: Einwilligung oder Interessenabwägung

Ist die DSGVO anwendbar – und dies wird insbesondere bei der Ermittlung von personenbezogenen Daten sowie der Anwendung von Profiling-Ergebnissen auf eine konkrete Person oder Personengruppe der Fall sein –, stellt sich zunächst die Frage nach der Rechtsgrundlage für die Durchführung eines Profilings. Denn nach Art. 5 Abs. 1 lit. a und Art. 6 Abs. 1 Satz 1 DSGVO gilt weiterhin das sog. Verbotsprinzip[30], wonach eine Datenverarbeitung entweder auf einer Einwilligung oder einer sonstigen Rechtsgrundlage beruhen muss. Das Profiling wird sich in den meisten Fällen entweder aus einer Einwilligung oder aber einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO ergeben müssen.

Bei der Einwilligung ist in besonderer Weise darauf zu achten, dass im Rahmen der Informiertheit auch das Profiling samt seiner Zwecke und der Empfänger und weiterer Datenverantwortlicher für das Datensubjekt erkennbar ist. Zudem kann die Freiwilligkeit problematisch sein, etwa dann, wenn von einem – guten – Score oder einem bestimmten Profil das Eingehen eines Vertrags oder die Gewährung von Zugang zu Leistungen abhängig gemacht wird.

Noch schwieriger ist es, eine rechtssichere Grundlage für Profiling auf der Basis von Art. 6 Abs. 1 lit. f zu schaffen. Nach dieser Vorschrift ist eine Datenverarbeitung zulässig, wenn das Interesse des Datensubjekts nicht überwiegt. Wiegen also das Interesse des Datenverarbeiters und des Datensubjekts gleich, darf die Datenverarbeitung durchgeführt werden. Die Kriterien für die Bestimmung der Intensität von Eingriffen lassen sich der DSGVO allerdings kaum entnehmen; allenfalls kann aus bestimmten Regelungen oder den Erwägungsgründen der DSGVO indirekt abgeleitet werden, was als schwerwiegend einzuordnen ist. Da mit der DSGVO nun eine verbindliche und umfängliche Europäisierung eingetreten ist, können hierfür Entscheidungen etwa der nationalen Verfassungsgerichte oder der nationalen höchsten Gerichte nur sehr eingeschränkt herangezogen werden, und auch die Entscheidungen des EuGH sind bisher noch zur alten

[30] Siehe HORNUNG/SPIECKER GENANNT DÖHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 212.

Datenschutz-Richtlinie ergangen. Gleichwohl lassen sich hier insgesamt doch einige Anhaltspunkte finden.

Ein erster und besonders gewichtiger Anhaltspunkt besteht darin, dass in Art. 35 Abs. 3 lit. a DSGVO das Profiling als ein besonders eingriffsintensives, nämlich risikobehaftetes Vorgehen der Datenverarbeitung eingeschätzt wird. Denn hier hat der europäische Gesetzgeber zwingend eine Datenschutzfolgeabschätzung angeordnet.

Zum zweiten lässt sich den Entscheidungen des EuGH zur Vorratsdatenspeicherung[31] entnehmen, dass das Gericht eine anlasslose und breit angelegte Auswertung von Daten für nicht mehr zulässig hält. Nun ist Profiling keine Vorratsdatenspeicherung, aber gleichwohl handelt es sich hierbei auch um eine Auswertung auf der Basis von einer Vielzahl von Daten, die oftmals ohne konkreten Anlass zusammengeführt worden sind.

Zudem enthalten die Art. 13 und Ar. 14 DSGVO gesteigerte Informationspflichten für Profiling, aus denen sich einerseits folgern lässt, dass Profiling nicht generell unzulässig sein soll, dass es aber als besonders schwerer Eingriff auch besonderen Informationspflichten ausgesetzt ist.

Nicht zuletzt ist die Anwendbarkeit der DSGVO nach Art. 2 Abs. 2 lit. b DSGVO bereits dann gegeben, wenn das Verhalten von Personen in der EU beobachtet wird. Aus dem Merkmal des «Beobachtens» lässt sich schließen, dass es sich um eine zielgerichtete Erfassung handeln muss.[32] Just dies ist aber eine Maßnahme, die üblicherweise zum Profiling beiträgt oder aber von diesem wesentlich genutzt wird, auch wenn dies für die Erstreckung der DSGVO auf Verarbeitungen außerhalb Europas noch nicht einmal Bedingung ist.[33] Auch das macht sichtbar, dass der Gesetzgeber einem solchen Umgang mit den Datensubjekten als grundsätzlich problematisch ansieht.

---

31 EuGH C-293/12 und C-594/12 – Digital Rights Ireland; EuGH C-203/15 und C-698/15 – Tele2 Sverige.

32 Hornung, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 2 Rn. 57.

33 Vgl. Hornung, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 2 Rn. 59.

Schließlich ist zu berücksichtigen, dass Datenverarbeitungen, die dem Zweck des Profilings dienen, wie jede Big Data Anwendung und Auswertung auch, nicht zwingend dazu genutzt werden, über das Datensubjekt selbst in der Folge Aussagen treffen und diesem z.B. Empfehlungen unterbreiten zu können. Vielmehr geht es oftmals darum, überhaupt Aussagen über Personen entwickeln zu können. Daher ergeben sich erhebliche externe Effekte für unbeteiligte Dritte daraus, dass Daten für die Zwecke des Profilings gesammelt und dann für ein solches genutzt werden. Das widerstrebt dem Datenschutz.

Jenseits der besonderen Eingriffsintensität des Profilings selbst kann diese noch gesteigert sein, wenn z.B. besondere Daten nach Art. 9 DSGVO verarbeitet werden.[34] Zudem sind Quantität und Qualität des Profilings, insbesondere wenn ein «mehr oder weniger detailliertes Profil einer Person» erstellt werden kann[35], von weiterer Bedeutung, ebenso wie die Profilbildung bei Minderjährigen, die potentiellen Nachteile und Konsequenzen wie Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste oder Rufschädigung.[36] Letztlich ist gerade die Alltagstauglichkeit vieler IT-basierter Geräte, deren Nutzung zu einer Informationsflut und damit neuen Möglichkeiten des Profiling führt, ein wichtiger Aspekt, der die Verarbeitung dieser Daten zum Zwecke des Profilings beschränkt.[37]

Daher wird man folgern können, dass ein Profiling nur dann gerechtfertigt werden kann, wenn der Datenverarbeiter ein besonderes Interesse seinerseits hat, das in einem engen Zusammenhang mit Interessen des Datensubjekts steht. Der Vorstellung in Erwägungsgrund 47, dass berechtigte Erwartungen des Datensubjekts einzubeziehen sind, entspricht diesem Schluss. Somit wird nun die Beziehung der betroffenen Person

---

[34] SCHANTZ, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 6 Abs. 1 Rn. 105.

[35] EuGH C-131/12, NJW 2014, 2257 Rn. 80 – Google Spain.

[36] SCHANTZ, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 6 Abs. 1 Rn. 105ff.

[37] Vgl. SCHANTZ, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 6 Abs. 1 Rn. 121.

zum Verarbeiter zu einem entscheidenden Kriterium für die Zulässigkeit einer Verarbeitung wegen berechtigter Interessen.[38] Im Umkehrschluss lässt sich folgern, dass eine Maßnahme des Profilings, die nicht durch den ursprünglichen Verarbeiter und nicht in einem engen Zusammenhang mit dem Verhältnis zwischen dem ursprünglichen Verarbeiter und dem Datensubjekt steht, es schwer haben wird, den Test der Interessenabwägung zu bestehen. Rein wirtschaftliche Gründe werden jedenfalls typischerweise nicht genügen,[39] wenn nicht ein enges Verhältnis zwischen Datensubjekt und Verarbeiter und eng begrenzte Umfänge und Auswirkungen des Profilings ausnahmsweise anderes vorsehen.

Einige Mitgliedstaaten haben in ihrem mitgliedstaatlichen Recht eigenständige und speziellere Vorschriften für Scoring vorgesehen.[40] Mangels einer Öffnungsklausel[41] in der DSGVO sind diese Vorschriften europarechtswidrig,[42] auch wenn es angesichts der Bedeutung des Profilings, insbesondere im Zusammenhang mit Big Data Anwendungen, empfehlenswert wäre, hier klare(re) Vorgaben zu machen.

e) Anforderungen an die Durchführung des Profilings

Jenseits der eigentlichen Problematik einer belastbaren Rechtsgrundlage für die Durchführung und Anwendung der Ergebnisse von Profiling sieht die DSGVO weitere Anforderungen vor. Diese erfassen eher das Verfahrensrecht als das materielle Recht. So soll nach Erwägungsgrund 71 UAbs. 2 Satz 1 DSGVO der Verantwortliche nur geeignete mathematische oder statistische Verfahren für das Profiling verwenden sowie technische und organisatorische Maßnahmen treffen, mit denen insbes. sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten fuhren, korrigiert werden, das

---

38 ALBRECHT, in: Simitis/Hornung/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 6 Einleitung Rn. 10.

39 SCHANTZ, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 6 Abs. 1 Rn. 121.

40 Z.B. § 31 Bundesdatenschutzgesetz Deutschland.

41 Dazu z.B. WAGNER/BENECKE EDPL 2017, S. 528; BENECKE/WAGNER DVBl 2016, S. 600.

42 Siehe EHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Anhang 2 zu Art. 6 Rn. 20.

Risiko von Fehlern minimiert wird und diskriminierende Wirkungen ausgeschlossen werden.

Aus diesen Anforderungen wird man die Verpflichtung ableiten müssen, von vornherein nur solche Datenarten für das Profiling zu verwenden, die für die Bewertung eines bestimmten Persönlichkeitsaspekts nach der angewandten Methode erheblich, d.h. auch inhaltlich zutreffend sind. Zudem sollte das Profiling einer regelmäßigen und kontinuierlichen Beobachtung und Überprüfung durch den Verantwortlichen unterzogen werden, um dessen Qualität zu sichern. Dies ist besonders dann erforderlich, wenn selbstlernende Algorithmen verwendet werden, die sich selbst weiterentwickeln.[43]

Insgesamt müssen wegen der besonderen Gefährdungslage durch Profiling die Transparenz-, Integritäts- und Rechtmäßigkeitsanforderungen besonders hoch angesetzt werden;[44] eine Kontrolle von In- und Output ist unerlässlich. So sehen Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g DSGVO weitreichende Informationspflichten des Verantwortlichen vor, die sich auch auf die involvierte Logik und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffenen Personen erstrecken. Korrespondierend dazu verpflichtet Art. 15 Abs. 1 lit. h DSGVO zu einer entsprechenden Auskunft gegenüber den betroffenen Personen. Art. 21 Abs. 1 DSGVO sieht zudem ein Widerspruchsrecht gegen das Profiling vor, welches das Datensubjekt jederzeit geltend machen kann. Ein weitergehendes Widerspruchsrecht sieht Art. 21 Abs. 2 für den Fall vor, dass das Profiling mit Direktwerbung in Verbindung steht.[45] Nach Art. 35 Abs. 3 lit. a ist im Falle des Profilings zudem eine Datenschutz-Folgenabschätzung durchzuführen.

Und auch das European Data Protection Board ist gemäß Art. 70 Abs. 1 lit. f DSGVO gefordert, Leitlinien, Empfehlungen und bewährte Verfahren zur näheren Bestimmung der Kriterien und Bedingungen für die auf Profiling beruhenden Entscheidungen bereitzustellen. Dies unterstreicht noch einmal die Bedeutung des Profiling.

---

43 Scholz, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 11.

44 Vgl. Scholz, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 9.

45 Scholz, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 4 Rn. 12.

f) Art. 22 als mögliche Grenze für Profiling

Die Bedeutung von Art. 22 DSGVO kann nicht überschätzt werden, ist die Vorschrift doch eine der wenigen Vorschriften, die sich mit den Folgen von datenschutzrelevanten Vorgängen befasst. Sie verlangt vom Datenverarbeiter und Entscheider, eine Entscheidung nicht ausschließlich auf der Basis einer automatisierten Verarbeitung zu treffen, wenn dieser eine Person unterworfen ist.

Die Vorschrift adressiert eine zentrale Frage der Informationsgesellschaft: Sollen Entscheidungen über die Möglichkeiten zur Ausübung menschlicher Freiheiten ungeprüft Maschinen und ihren Algorithmen überlassen werden?[46] Sie nimmt die Entscheidungen in den Blick, die an einen solchen Score anknüpfen. Sie unterfallen grundsätzlich dem Anwendungsbereich der Vorschrift.[47] Gleichwohl ist die Bedeutung von Art. 22 DSGVO für die Grenzziehung des Profilings (wie auch von Big Data Prozessen allgemein) beschränkt. Denn die eigentliche Herausforderung, die Entscheidungskontrolle und die Entscheidungstechnikkontrolle, wird durch Art. 22 nur in geringem Maße aufgegriffen und einer Regelung zugeführt.

Die Vorschrift sieht zwar ein grundsätzliches Verbot rein automatisierter Einzelentscheidungen vor. Die zugrunde liegenden Verarbeitungsprozesse werden von ihrem Anwendungsbereich aber nicht erfasst. Weder regelt die Vorschrift die Frage, ob und unter welchen Voraussetzungen ein personenbezogenes Profil erstellt und verwendet werden darf, noch macht sie Vorgaben für einen nichtdiskriminierenden, transparenten und kontrollierbaren Einsatz von Algorithmen, zumal die Ausnahmen vom Verbot der Einzelentscheidung (bei den Vertragsbeziehungen und der Einwilligung) sogar noch weiter gefasst sind als dies schon unter der Datenschutz-Richtlinie der Fall war.[48]

---

[46] Scholz, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 22 Rn. 1.

[47] Scholz, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 22 Rn. 24; Buchner, in: Kühling/Buchner, DSGVO Kommentar, 2018, Art. 22 Rn. 22.

[48] Siehe Scholz, in: Simitis/Hornung/Spiecker genannt Döhmann (Hrsg.), DSGVO Kommentar, 2019, Art. 22 Rn. 11.

g) Zwischenfazit

Das Profiling ist eine der eingriffsintensivsten Maßnahmen der Datenverarbeitung, weil darin nicht nur die eigentliche Informationsverarbeitung, sondern zugleich auch die darauf basierende Entscheidungen beeinflusst werden. Da Entscheidungen aber nicht (mehr) angesehen werden kann, welche Informationen in sie eingeflossen sind, ist eine Kontrolle der vorangegangenen Schritte – wie des Profilings – von besonderer Bedeutung.

Die DSGVO arbeitet hier allerdings mit einer Reihe von blinden Flecken; an einer echten Entscheidungskontrolle fehlt es trotz des Verbots der automatisierten Einzelentscheidung in Art. 22 DSGVO an einer konsequenten Begleitung dieser Entscheidungen. Damit wird gleichzeitig auch das Feld der Big und Smart Data Anwendungen unreguliert gelassen.

IV. BIG DATA UND KÜNSTLICHE INTELLIGENZ

Profiling ist kaum durchführbar ohne die Mittel, die mit Begriffen wie «Big Data» umschrieben werden; Big Data liegt dem Profiling moderner Prägung fast immer zugrunde. Diese technischen Mittel führen dazu, dass auf der Basis vieler vorhandener, schnell verarbeitbarer Daten Korrelationen und Wahrscheinlichkeiten ermittelt werden. Dies erlaubt günstigenfalls die Bestätigung von Hypothesen, aufgrund derer die Auswertung erfolgt ist. Oftmals allerdings werden auch Befunde ins Geradewohl ermittelt. Big Data Anwendungen basieren also nicht zwingend auf einer mathematischen oder statistischen Validität.[49] Die erlangten Erkenntnisse können durchaus auch auf Zufälligkeiten beruhen, auf Umständen, für die keine Daten in die Auswertung eingeflossen sind, oder auf unzutreffender Gewichtung der Daten.

Die zu Big Data eingesetzten Algorithmen haben keine soziale Kompetenz, sie kennen normative Vorstellungen und Freiheitsrechte nicht und können komplexe Sinnzusammenhänge nicht erfassen. Sie operieren auf Basis eines vordefinierten Ziels und sind

[49] SCHOLZ, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 22 Rn. 10.

von bestimmten Grundannahmen abhängig. Damit führt ihr Einsatz keineswegs zwingend zu «richtigen», nicht einmal zu folgerichtigen Ergebnissen. Allein auf statistischen Wahrscheinlichkeiten beruhende Prognosen können sich als individuell falsch herausstellen; aus der Analyse an sich zutreffender Einzeldaten können fehlerhafte, unfaire, manipulative und diskriminierende Schlussfolgerungen gezogen werden, die die Freiheitsrechte des Einzelnen erheblich beeinträchtigen können.[50] Datenschutzrechtlich nicht abgebildet ist darüber hinaus, dass solche Zahlenwerte, wie sie durch Big Data ermittelt werden, häufig fehlerhaft verstanden und ihnen eine Objektivität, Neutralität und Verlässlichkeit zugewiesen wird, über die sie gerade nicht zwangsläufig verfügen.

Dies gilt auch für den Einsatz von Künstlicher Intelligenz, was auch immer man darunter genau und im Einzelnen verstehen mag[51]. Der Begriff beschreibt eine Vielzahl von technologischen Mitteln, deren verbale Annäherung an menschliche und biologische Kategorien («Intelligenz», «neuronale Netze», «selbstlernend») oftmals die technische Funktionsweise verschleiert und ihre Leistungsfähigkeit und Einsatzmöglichkeiten überbewertet. Typischerweise funktionieren solche Verfahren Künstlicher Intelligenz auf der Basis erheblicher Datenmengen, anhand derer bestimmte Muster identifizierbar gemacht werden. Es gibt allerdings auch einige Verfahren von Künstlicher Intelligenz, die ohne massenhafte Daten auskommt, insbesondere im Bereich der Simulation.

Ohne Trainingsdaten und ohne Einsatz von dahinterstehenden Datenauswertungsprozessen wäre der Einsatz von Künstlicher Intelligenz wenig ertragreich und wenig präzise. Erst die Verfügbarkeit massenhafter Daten und die zügige Analyse und Auswertung hat die grundsätzlich schon lange bekannten Verfahren mit einer neuen Durchschlagskraft ausgestattet. Big Data und Künstliche Intelligenz sind also oftmals miteinander verknüpft.

---

50 SCHOLZ, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 22 Rn. 10.

51 Zu Definitionen und Umschreibungen siehe z.B. Gesellschaft für Informatik, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, 2018, S. 30ff.; BREMAN, K&R 2019, S. 8ff. Siehe auch SCHWEIGHOFER, in: ROTOLO (Hrsg.), JURIX 2015: The Twenty-Eighth Annual Conference, Legal Knowledge and Information Systems, 2015, S. 191 ff.

Weder Big Data noch Technologien der Künstlichen Intelligenz werden von der DSGVO direkt adressiert. Sie können allenfalls indirekt unter den Anwendungsbereich einzelner Normen subsumiert werden. Wo der Einsatz geschieht, um Profiling zu ermöglichen, sind die hierzu bereits geschilderten rechtlichen Regelungen einschlägig.[52] Im Übrigens setzt die DSGVO vor allem durch ihre Grundprinzipien Grenzen, also das Prinzip der Zweckbestimmtheit, der Datenminimierung, der begrenzten Speicherung und der Transparenz, Art. 5 Abs. 1 DSGVO. Viel stärker als eine dadurch erfolgende Inputkontrolle der Daten, auf deren Basis dann die weiteren Schritte Künstlicher Intelligenz vorgenommen werden, bedarf es einer Verfahrenskontrolle. Da aber die hier verwendeten Daten zumeist anonymisiert bearbeitet werden, ist der Anwendungsbereich der DSGVO nicht eröffnet, ebenso wenig wie bei darauffolgenden, nicht auf Personen bezogenen Einschätzungen.

Werden allerdings Verfahren der Künstlichen Intelligenz und Auswertungen aus Big Data Verfahren auf Personen bezogen, liegt ein personenbezogenes Datum i.S.v. Art. 4 Abs. 1 DSGVO vor, und die Regelungen der DSGVO sind vollumfänglich anwendbar. Damit kann eine Kontrolle der Verwendung erfolgen, regelmäßig nicht allerdings des Inputs, der Auswertung und der dahinterstehenden mathematischen Verfahren. Was das bedeutet lässt sich an folgendem Beispiel erläutern: Eine Eigenschaft wird fehlerhaft mit einer anderen Eigenschaft verknüpft, z.B. eine Gewaltbereitschaft mit dem Umstand, dass jemand als Teenager an Masern erkrankt war.[53] Wenn diese Person nun an einer Demonstration teilnimmt, wird sie von der Polizei in besonderer Weise überwacht, um im Falle von Gewalt sofort eingreifen zu können. Es leuchtet unmittelbar ein, dass eine solche Überwachung die Versammlungsfreiheit, wie sie z.B. in Art. 8 Abs. 1 GG geregelt ist, erheblich beeinträchtigt. Die überwachte Person erlebt – wenn überhaupt – lediglich die gesteigerte Überwachung durch die Polizei, z.B. eine Durchsuchung des mitgeführten Rucksacks auf Waffen. Aus Sicht der Polizei ist dieses Vorgehen nur folgerichtig, da die Auswertung ergeben hat, dass eine erhöhte Gewaltbereitschaft vorliegt. Tatsächlich aber mag die Verbindung der beiden Eigenschaften nicht

[52] Siehe bereits unter II.

[53] Nach Kenntnis der Autorin gibt es keinerlei solche Verknüpfung dieser Eigenschaften; das Beispiel ist willkürlich gewählt.

zutreffen, so dass die Person tatsächlich gar nicht gewaltbereit ist, oder mag die Person gar nicht an Masern erkrankt gewesen sein. Weder kann die Polizei das von sich aus feststellen noch gelingt es der Person, diesen Zusammenhang aufzudecken. Denn die Polizei erfährt lediglich die Auswertung «gewaltbereit», und entsprechend kann ein Auskunftsanspruch der Person auch nur darauf gerichtet sein.

Was es also bedarf: Einer stärkere Kontrollierbarkeit der algorithmischen Vorgehensweise von ihren Anfängen bis zu ihrer Verwendung. Diese muss, wie sich am Beispiel zeigt, über die Vorgaben in Art. 22 DSGVO hinausgehen.

Ein anderes Problem stellt sich in der intensiven Sammlung von Datenmengen, die sich in zwei Problembereiche gliedern lässt. Zum einen ist wegen der Notwendigkeit von Trainingsdaten eine Zugänglichkeit zu solchen entscheidend, um überhaupt viele Verfahren der Künstlichen Intelligenz einsetzen zu können. Das wiederum bedeutet einen Wettbewerbsnachteil, wenn diese Daten nicht frei verfügbar sind. Zum anderen wird für den Einsatz von Künstlicher Intelligenz eine Datenmenge benötigt, die dem Grundsatz der Datenminimierung und der Zweckbindung aus Art. 5 Abs. 1 lit. b DSGVO fundamental widerspricht. Auch hier müssen Grenzen gezogen werden, um zu verhindern, dass die Grundlagen von Künstlicher Intelligenz dazu führen, dass der Einzelne der Macht der Daten ausgesetzt ist, über die er keine Kontrolle mehr hat.

Angesichts der bereits weit verbreiteten Nutzung Künstlicher Intelligenz und Big Data Anwendungen ringen die Europäische Union und die Mitgliedstaaten derzeit um einen nachhaltigen Einsatz Künstlicher Intelligenz und datenintensiver Anwendungen. Dies geschieht zum Teil gemeinschaftlich, zum Teil aber auch in diversen Alleingängen. Immer neue Gutachten und Stellungnahmen bereiten die Diskussion vor;[54] eine Entscheidungsreife kann aber noch nicht angenommen werden, ebenso wenig wie sich derzeit absehen lässt, worauf die Erwägungen sich richten.

[54] Hervorzuheben ist hier der interdisziplinäre Ansatz in: Gesellschaft für Informatik, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, 2018.

V. DATENVERARBEITUNG IN SOZIALEN NETZWERKEN

1. Allgemeines

Erhebliche Aufmerksamkeit hat die Datenverarbeitung in Sozialen Netzwerken erlangt. Mit den neuen Informationsintermediären haben sich in vielen Rechtsbereichen neue Fragestellungen ergeben, vom Einsatz sog. Softwareagenten[55] über die veränderten vertraglichen Beziehungen, in denen die Leistung wesentlich durch den Kunden selbst generiert wird,[56] und die Marktmacht einzelner Anbieter aufgrund von ökonomischen Netzwerkeffekten[57] bis hin zu den vielfältigen Problemen, die sich aus der neuen Austauschbeziehung «Daten gegen Dienst»[58] für das Datenschutzrecht ergeben haben[59].

Die DSGVO hat diese Problembereiche zwar gesehen, sie waren sogar ein nicht nur untergeordneter Anlass für die Neuregelung des europäischen Datenschutzes.[60] Dennoch hat sie – unter dem Konzept der Technikneutralität[61] – darauf verzichtet, für die Sozialen Netzwerke eigenständige Regelungen einzuführen. Dies mag in angrenzenden Bereichen wie dem Vertrags- oder Wettbewerbsrecht zutreffend sein, im Bereich des Datenschutzes ist dies angesichts der Geschäftsmodelle der meisten Sozialen Netzwerke kaum hinnehmbar. Denn die vermeintliche Kostenlosigkeit von Anbietern wie Facebook, LinkedIn, Google und anderen beruht wesentlich darauf, dass die von den Nutzern zur Verfügung gestellten Daten ausgewertet und für vielfältigste

---

55 SORGE, Softwareagenten, 2015; BÜTTNER, Automatisierte Verhandlungen in Multi-Agenten-Systemen, 2010.

56 Vgl. SPIECKER GENANNT DÖHMANN, AnwBl. 2011, S. 256f.

57 Siehe nur die Entscheidung des Bundeskartellamts vom 06.02.19.

58 KLEMENT, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 7 Rn. 63.

59 Vgl. SPIECKER GENANNT DÖHMANN, K&R 2012, S. 717ff.

60 Vgl. ALBRECHT, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 186.

61 HORNUNG/SPIECKER GENANNT DÖHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 241.

Anwendungen eingesetzt werden.[62] In der Folge müssen die Rechtsgrundlagen und rechtlichen Rahmenbedingungen aus allgemeinen Normen destilliert werden, wird die Türe weit für die Aushandlungsprozesse in bereichsspezifischen Teilregelungen wie in der künftigen ePrivacy-Verordnung geöffnet und läuft die DSGVO damit immer wieder Gefahr, dass ihr Gehalt und ihre Systematik unterlaufen werden. Faktisch wird die Konkretisierungsleistung durch andere Akteure als den Gesetzgeber erbracht.[63]

2. Datenschutzvorgaben

Die Datenverarbeitungen in Sozialen Netzwerken sind – auch angesichts der Breite der Geschäftsmodelle – so vielfältig, dass sie in einem Überblicksbeitrag gar nicht und auch in ausführlicheren Darstellungen nur unzureichend erfasst werden können. Daher soll hier lediglich auf einige wenige zentrale Problemlagen abgestellt werden.

a) Rechtsgrundlage

Als Rechtsgrundlage für Datenverarbeitungen einschließlich der Auswertung, Weitergabe und des Transfers außerhalb des europäischen Rechtsraums ist die Interessenabwägung nach Art. 6 Abs. 1lit. f DSGVO die wichtigste materiell-rechtliche Vorgabe.[64] Dabei ist zu beachten, dass unter der DSGVO auch die Daten, welche von den Datensubjekten selbst veröffentlicht wurden, ihr unterfallen – unter der Datenschutz-Richtlinie gab es hierüber Uneinigkeit, weil vielfach vertreten wurde, dass aufgedrängte Informationen nicht vom Begriff der Verarbeitens erfasst seien. Nunmehr stellt aber Art. 4 Nr. 2 DSGVO in der Legaldefinition klar, dass jeder Vorgang gemeint ist, der irgendwie

---

62 KLEMENT, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 7 Rn. 60; etwa zur Werbung mittels des Facebook-Modells: EHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Anhang 3 zu Art. 6 Rn. 47.

63 HORNUNG/SPIECKER GENANNT DÖHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 241.

64 Vgl. HORNUNG/SPIECKER GENANNT DÖHMANN, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Einleitung Rn. 251.

in Zusammenhang mit personenbezogenen Daten steht, auch wenn er atypisch ist.[65] Ferner besteht unter der DSGVO Einigkeit darüber, dass auch Daten, die in Sozialen Netzwerken allgemein zugänglich und öffentlich einsehbar sind, weil sie nicht durch geschützte Bereiche ausgesondert werden, grundsätzlich dem Schutz der DSGVO unterfallen: Auch sie sind und bleiben personenbezogene Daten.

Natürliche Personen sind auch und gerade in der Öffentlichkeit «privat», auch wenn sie die Veröffentlichung aktiv betrieben haben. Denn die DSGVO schützt nicht allein «Privatheit» oder «Abgeschiedenheit» im Sinn eines «Allein-gelassen-Werdens», sondern in einem weiteren Verständnis die informationelle Selbstbestimmung und Individualität des Einzelnen in all ihren Facetten.[66] Damit unterscheidet sich das europäische Datenschutzrechtsverständnis ganz erheblich von anderen Konzepten, etwa der US-amerikanischen Privacy.

b) Gemeinsame Verantwortlichkeit

Soziale Netzwerke agieren auf einem Plattformsystem: Sie stellen eine Infrastruktur bereit und überlassen es den Nutzern, wie diese inhaltlich genutzt wird. Dies hat dazu geführt, dass sich Soziale Netzwerke lange als reine Infrastrukturanbieter verstanden sehen wollten. Da sie aber auf der Basis dieser Plattform erhebliche Tätigkeiten entwickelt haben, die Daten ihrer Nutzer für ihre Zwecke zu nutzen, kann davon kaum die Rede sein. Sie gelten längst als Verantwortlicher im Sinne von Art. 4 Abs. 7 DSGVO.

Der EuGH hat die Verantwortlichkeit aber erheblich ausgedehnt. Konnte sich bisher derjenige, der die Leistungen einer Plattform für eigene Zwecke nutzte, hinter die Verantwortlichkeit der Plattform zurückziehen, ist dies nun nicht mehr ohne weiteres möglich. Wer die Plattform eines anderen nutzt, kann gemeinsamer Verarbeiter im Sinne von Art. 26 DSGVO sein.[67] Dazu bedarf es nicht etwa weit reichender Gestal-

---

65 Vgl. ROßNAGEL, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 2 Rn. 11.

66 KARG, in: SIMITIS/HORNUNG/SPIECKER GENANNT DÖHMANN (Hrsg.), DSGVO Kommentar, 2019, Art. 4 Nr. 1 Rn. 31.

67 EuGH C-210/16 – ULD Schleswig-Holstein.

tungsmöglichkeiten; vielmehr kann genügen, dass einzelne Datenverarbeitungsmodalitäten zumindest mit beeinflusst und genutzt werden können. In der Konsequenz ist nicht nur der Plattformbetreiber zur Einhaltung der DSGVO verpflichtet, sondern auch derjenige, der Anwendungen darüber anbietet und sich dabei datenschutzrechtlich relevante Leistungen der Plattform zu Eigen macht.[68]

Diese Rechtsprechung hat erhebliche Rückwirkungen auf die Plattformen und ihre Ausgestaltung. Die Trennung von Nutzer und Anbieter war schon in anderer Hinsicht in Frage gestellt, da ja die Inhalte der Nutzer die Leistungsfähigkeit der Anbieter bestimmte.[69] Nun aber werden die Grenzen zwischen Infrastruktur und Inhalten, zwischen Grunddienst und Add-On-Dienst, weitgehend aufgelöst. In der Folge trifft denjenigen, der einen Add-On-Dienst über eine Plattform anbietet, die Verpflichtung zur Vergewisserung deren datenschutzrechtlicher Vorgaben und Einordnung, wenn er eine solche auswählt, und wie er deren Angebote nutzt.[70]

c) Systemische Digitalisierung

Mit dem Begriff der systemischen Digitalisierung werden Phänomene erfasst, die sich aus der besonderen Leistungsfähigkeit von automatisierten Plattformen ergeben.[71] Damit werden einerseits die Erscheinungen gebündelt, welche die Technologie der Digitalisierung als solche hervorgerufen hat und die bereits seit ihren Anfängen in ihren Auswirkungen auf die Gesellschaft und das Recht diskutiert wird, etwa von *Steinmüller*[72] oder *Simitis*[73]. Der Begriff des «systemischen» fügt diesem Problemkomplex eine weitere Dimension hinzu, die sich erst in den letzten Jahren zunehmend herausgebildet hat, nämlich

---

68 Vgl. SPIECKER GENANNT DÖHMANN, GRUR 2019, S. 341, 347.

69 SPIECKER GENANNT DÖHMANN, K&R 2012, S. 717.

70 Vgl. SPIECKER GENANNT DÖHMANN, GRUR 2019, S. 341, 347.

71 SPIECKER GENANNT DÖHMANN, GRUR 2019, 341, 349; SPIECKER GENANNT DÖHMANN, CR 2016, S. 698.

72 Etwa W. STEINMÜLLER, ZVglRWiss 1982, S. 106 ff.; DERS., DVR 1981, S. 37 ff.; DERS./TITTLBACH, NfD 1980, S. 135 ff.

73 Siehe nur SIMITIS – SIMITIS, BDSG-Kommentar, 8. Auflage 2014, Einleitung; DERS., Automation in der Rechtsordnung – Möglichkeiten und Grenzen, 1967; DERS., Deutscher Juristentag 48, T35-43 (Mainz 1970); DERS., NJW 1971, S. 673 ff.

die Verbindung der verschiedenen IT-basierten technischen Möglichkeiten durch Vernetzung, die zu einer Systemisierung geführt hat. Ein wesentlicher technischer Ansatzpunkt, aber längst nicht alleiniger, ist das Internet und die sich aus dieser globalen und nahezu jedermann leicht und kostengünstig erreichbaren Verbindung ergebenden Herausforderungen für das Recht. Diese haben im Weiteren, in Verbindung mit Künstlicher Intelligenz, dazu geführt, dass ein eigenständiges, abgegrenztes System mit eigenen Systembedingungen auf der Basis von Vernetzung und Digitalisierung entstehen kann.[74] Dieses ist zumeist nicht mehr in Ende-zu-Ende-Verbindungen untergliedert, sondern die Systeme basieren vielmehr auf Plattformen, die ihrerseits diverse Anwendungen und Mehrwert-Dienstleistungen miteinander verbinden. Längst gehören Soziale Netzwerke zu solchen Plattformen: Sie bieten Add-On-Dienste aller Art an und ermöglichen so oftmals überhaupt erst den Zugang zu diesem Dienst. Sie ermöglichen damit erst die Netzwerkstrukturen; sie entwickeln die viralen Kontenpunkte, über die Interaktionen und Vernetzungen möglich werden. Auf der Basis der Plattformen werden die Verknüpfungen überhaupt erst durchführbar. [75] Systemische Digitalisierung bedeutet qualitativ mehr als nur die Zusammenführung von Digitalisierung und Vernetzung, weil sie auf der Basis systemischer Verknüpfungen erfolgt und damit den Systemcharakter in den Mittelpunkt rückt.[76]

Für das Recht bedeutet systemische Digitalisierung eine der größten vorstellbaren Herausforderungen, geht damit doch der Verlust der Zuordnung von Verantwortung und somit von Rechten und Pflichten und von Kontrollierbarkeit einher. Wer Adressat des Rechts ist, ist nicht länger bestimmbar in einem solchen System, weil die Kontrolle über Steuerung, über Input und Output im System durch automatisierte Prozesse erfolgt, deren Einzelentscheidungen nicht mehr nachvollziehbar sind,[77] und denen es an Kausalität fehlt[78]. Die Verbindung von Netzwerk und System führt dazu, dass es weder eine eindeutige Mittel- noch eindeutige Zweckverantwortung mehr gibt. Denn bei fortschreitendem Maschinenlernen und damit konsequenter Weiterentwicklung der Algorithmen und ihrer Muster scheitert eine eindeutige Zuschreibung. Ein System, in dem

74 Spiecker genannt Döhmann, CR 2016, S. 698.

75 Spiecker genannt Döhmann, GRUR 2019, S. 341.

76 Spiecker genannt Döhmann, GRUR 2019, S. 341, 349.

77 Spiecker genannt Döhmann, GRUR 2019, S. 341, 349.

78 Spiecker genannt Döhmann, GRUR 2019, S. 341, 349; CR 2016, S. 698, 700.

eine Black Box existiert, ist rechtlich kaum noch einzuhegen. Denn die einzelnen Beiträge und damit Anteile an Verantwortung sind nicht mehr ermittelbar und nicht mehr voneinander unterscheidbar.[79]

VI. FAZIT UND AUSBLICK

Die DSGVO hat eine Reihe von Neuerungen gebracht, vor allem im Bereich von Vollstreckung und Verfahren. Gerade für die datenschutzrechtlich hochproblematischen Bereiche von Profiling, Big Data, Künstlicher Intelligenz und Sozialen Netzwerken fehlt es an spezifischen Regelungen; zur Beurteilung ist auf die allgemeinen Vorschriften der DSGVO zurückzugreifen. Diese vermögen in vielen Bereichen eine rechtliche Beurteilung zu leisten; so sind insbesondere die Grundsätze aus Art. 5 Abs. 1 DSGVO und hier besonders die der Fairness, der Datenminimierung sowie der Zweckbindung von Bedeutung. Angesichts der abstrakten Regelungsstruktur und dem Verzicht auf technikspezifische Regulierung in der DSGVO wird noch viel Präzisierung durch die Gerichte, allen voran den EuGH, zu leisten sein. Ein erster großer Schritt, um künftig eine gesellschaftskonforme Weiterentwicklung der Digitalisierung zu gewährleisten, ist allerdings getan. Eine konsequente Umsetzung und Durchsetzung der DSGVO kann die Maxime der Machbarkeit durch die Technik wieder vermehrt ablösen durch eine Maxime der Normativität durch das Recht. Dies wird helfen, ein level-playing-field für Informationsanbieter weltweit zu etablieren und Machtasymmetrien durch die Verfügbarkeit von Daten und die Verfügbarkeit der Informationstechnologie zu verringern und zu vermeiden.

Damit aber alleine ist es nicht getan. Ansätze der Privacy-by-Design müssen ausgefüllt werden, und dazu bedarf es einer Kompetenz nicht nur juristischer, sondern auch informatischer Art – ergänzt um ein Verständnis, wie die ökonomischen Anreize wirken und welche Dynamik wirkt. *Erich Schweighofer* wird hier gebraucht, um eine Brücke zu schlagen und dem «legal tech» ein Antlitz zu verschaffen, das klassische Problemlagen in den Blick nimmt, aber neue Informatik integriert. Herzlichen Glückwunsch, alles Gute und ein weiterhin intensives Wirken!

[79] SPIECKER GENANNT DÖHMANN, GRUR 2019, S. 341, 349; CR 2016, S. 698, 700.