

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Philipp Quiel

Durchsetzbare Rechte und wirksame Rechtsbehelfe

Seite 229

Stichwort des Monats

Sascha Kremer

Schrems II: Et hätt noch emmer joot jejange

Seite 230

Datenschutz im Fokus

Peter Hense

Verantwortung für arbeitsteiliges Handeln an der Schnittstelle von Zivil-, Straf-, Wettbewerbs- und Datenschutzrecht

Seite 236

Stefan Hessel, Lena Leffer und Karin Potel

Der Auftragsverarbeiter im Fokus der Datenschutzaufsicht: Wann ist seine Inanspruchnahme zulässig?

Seite 240

Fragen aus der Praxis

Dr. Carlo Piltz, Sandra Häntschel und Moritz zur Weihen

Die Weite des Auskunftsrechts nach Art. 15 DSGVO nach der aktuellen Rechtsprechung

Seite 243

Aktuelles aus den Aufsichtsbehörden

Benedikt Siebelmann

EDSA: Europäische Aufsichtsbehörden mit neuen Leitlinien zum Targeting von Nutzern sozialer Netzwerke

Seite 246

Rechtsprechung

Tim Wybitul und Dr. Isabelle Brams

Immaterieller Schadensersatz wegen Datenschutzverstößen

Seite 249

Jan Spittka und Katja Ruers

Business Process Outsourcing als gemeinsame Verantwortlichkeit

Seite 252

Dr. Martin Riemer

Datenauskunft nur gegen Vorlage einer Originalvollmacht

Seite 256

▪ Nachrichten Seite 233 ▪ Service Seite 260

Peter Hense

Verantwortung für arbeitsteiliges Handeln an der Schnittstelle von Zivil-, Straf-, Wettbewerbs- und Datenschutzrecht

Cuius commodum, eius periculum esse debet: Wer die Vorteile einer Sache genießt, der muss auch das Risiko tragen. Was als abstrakte lateinische Rechtsregel so leichtfüßig klingt, ist in der Praxis des Datenschutzrechts bis ins Detail umstritten. Fragen der Zurechnung und Gefahrtragung zählen zu den ältesten juristischen Streitpunkten. In der Wirtschaft stellen sie sich bei sämtlichen arbeitsteiligen Sachverhalten, bei denen ein Unternehmer sich im Rahmen seiner Tätigkeit Dritter bedient und diese Dritten Rechtsverletzungen begehen. Haftet der Unternehmer für diese Rechtsverletzungen und wenn ja, wie weitgehend? Zumindest für den wichtigen Bereich der Unterlassungsansprüche kennt die Rechtsprechung seit mehr als 100 Jahren eine klare Antwort auf diese Frage.

Aus großer Macht folgt große Verantwortung

Als der EuGH in den zwei berühmten Entscheidungen im Jahr 2018 (C-210/16 „Wirtschaftsakademie“ und C-25/17 „Jehovan todistajat“) die akademische Diskussion um die (gemeinsame) Verantwortlichkeit im Datenschutzrecht vom Kopf auf die Füße stellte, schauten viele – nicht zuletzt deutsche – Juristen und Unternehmen ungläubig auf die Rechtsprechung der Luxemburger Richter: Wie kann es sein, fragten sie sich, dass die Verantwortlichkeit für Datenverarbeitungen derart weit gefasst wird? Die Urteile wurden seziert, Begrenzungen hineininterpretiert, viele fruchtlose Aufsätze geschrieben und vertragliche Regelungen erdacht, um die befürchteten Folgen eines ungewollten Einstehenmüssens für rechtswidrige Handlungen zumindest abzuschwächen. Die Diskussionen um die gemeinsame Verantwortlichkeit und das Lamento über deren vermeintliche Uferlosigkeit erfasste große Teile der vielen frischgebackenen und wenigen altgedienten Datenschutzrechtsexperten. Dabei ist an der Entscheidungspraxis des EuGH nur wenig überraschend. Wer einen Dritten einschaltet und von dessen Handlungen profitiert, soll sich hinter dessen Tatbeitrag nicht verbergen dürfen und dem Betroffenen so die Durchsetzung seiner Rechte erschweren. Wendet man sich dem sachlichen Grund der gemeinsamen Verantwortung zu, so scheint aus dem Dunkel jahrtausendealter römisch-kanonischer Rechtsgeschichte der eingangs zitierte Rechtssatz auf: Wer die Vorteile gemeinsamer Arbeit genießen möchte, muss auch für die Folgen gemeinsamer Verletzung eintreten. Partizipation, so wollen es europäische Richter seit jeher, gilt eben in guten wie in schlechten Zeiten.

Mehrheit von Schädigern in Strafrecht und Zivilrecht

Die Tatbeiträge von Mittätern und Gehilfen werden im Strafrecht (§ 25 Abs. 2 StGB) wie im Zivilrecht (klarstellend: § 840 BGB) emotionslos allen Beteiligten zugerechnet. Kennt das Strafrecht systemimmanent noch bestimmte

Grenzen der Zurechnung und geht bei fehlendem Tatplan von einer Nebentäterschaft aus, so schreitet das Zivilrecht hier wesentlich robuster zur Sache. Jenseits der gesamtschuldnerischen Haftung auch bei Nebentäterschaft ordnet das Gesetz sogar bei einem *non liquet*, also mehreren möglichen Kausalverläufen, eine Gesamtschuld an (§ 830 Abs. 1 S. 2 BGB). *In dubio pro reo* ist im Zivilrecht unangebracht. Das Risiko der Unaufklärbarkeit eines Schadenshergangs ist nämlich am ehesten den Schädigern anzulasten, nicht den Geschädigten. Ansonsten stellt das deutsche Deliktsrecht in § 830 Abs. 1 und 2 BGB keine hohen Hürden auf, um einen weiteren Schädiger (auch: Anstifter oder Gehilfe) als Mittäter haften zu lassen: Jede Form einer Hilfeleistung kommt in Betracht, selbst Vorbereitungs-handlungen und psychische Beihilfe genügen, um in den Genuss der vollen Mithaftung zu kommen. Einzige Voraussetzungen gemeinschaftlicher deliktischer Haftung als Teilnehmer sind der bedingte Vorsatz hinsichtlich der Förderung der Haupttat sowie das Bewusstsein deren Rechtswidrigkeit (grundlegend: BGHZ 180, 134, Tz. 14 – *Halzband*, zuletzt BGH, Urteil v. 20.2.2020, I ZR 193/18, Tz. 30 – *Kundenbewertungen auf Amazon*). Das Berliner Kammergericht fasst es deutlich zusammen (Urteil v. 11.12.2015, 5 U 31/15 – *UBER Black*): „Einzelheiten der Haupttat muss der Gehilfe nicht kennen. Er braucht weder genaue Kenntnis von der Person des Täters zu haben, noch zu wissen, wann, wo, zu wessen Nachteil und unter welchen besonderen Umständen die Tat ausgeführt wird.“ Strafrecht und Zivilrecht haben demnach längst Mittel und Wege gefunden, der typischen postdeliktischen Verantwortungsdiffusion entgegenzuwirken.

Schnittstellen von Datenschutzrecht, Strafrecht, Zivilrecht

Zivilrechtliche Flankierung und Ausgestaltung datenschutzrechtlicher Ansprüche

Es ergibt für mit dem Datenschutzrecht befaste Juristen und rechtlich Interessierte Sinn, sich intensiv mit dem Zu-

sammenspiel der verschiedenen Rechtsgebiete zu befassen. Denn das Datenschutzrecht der alten Richtlinie 95/46/EG, der DSGVO und der spärlich transformierten ePrivacy-Richtlinie genießen keine Exklusivität für die Beurteilung von Lebenssachverhalten mit Datenverarbeitungsbezug. So wird von den datenschutzrechtlichen Sondervorschriften ausweislich des EuGH-Urteils C-40/17 in Sachen „*FashionID*“ eine „weitergehende Haftung“ nach nationalem (Delikts-)recht gerade nicht verdrängt. Im Gegenteil, die deutsche Rechtsprechung nimmt den Ball auf, gewährt Unterlassungsansprüche aus § 823 Abs. 1 i. V. m. § 1004 BGB gegen persönlichkeitsrechtsverletzende Verarbeitungen (vgl. nur OLG Frankfurt, Beschl. v. 19.02.2020 – 6 W 19/20; OLG Karlsruhe, Urt. v. 10.06.2020 – 6 U 129/18) und ordnet, wo dies plausibel erscheint, die Regeln der DSGVO als Schutzgesetze im Sinne von § 823 Abs. 2 BGB ein (OLG Köln, Urt. v. 14.11.2019 – 15 U 126/19). Anspruchskonkurrenz ist der Urzustand des Rechts und das Datenschutzrecht verdient hier, trotz und gerade wegen der fehlgeleiteten Diskussion um eine angebliche „Sperrwirkung“, keine Ausnahme.

Strafrechtliche Sanktionierung datenschutzrechtlicher Verstöße am Beispiel „Dark Patterns“

Die Rechtspraxis freut sich, dass durch „Dark Patterns“ in Cookie-Bannern Regelungen wie § 42 Abs. 2 Nr. 2 BDSG aus dem Schattendasein des Nebenstrafrechts ins Licht der Ermittlungsakten geholt werden. Dass das „Erschleichen von personenbezogenen Daten“ zum Zwecke der (Werbe-)Gewinnerzielung unter Strafe steht, kann eine wertvolle Erkenntnis darstellen für professionelle Compliance-Abteilungen in Unternehmen sowie eine heilsame Erfahrung für die unmittelbar handelnden Personen im Unternehmen oder bei beauftragten Agenturen. Sie alle mögen ihre individuellen Tatbeiträge im Rahmen eines Arbeitsverhältnisses oder Dienstvertrags erbracht haben, doch schützen zivilrechtliche Vereinbarungen gerade nicht vor strafrechtlicher Verfolgung. Im Gegenteil, aus der Verletzung strafrechtlicher Normen folgt zivilrechtlich mitunter das Verdikt der Nichtigkeit solcher Verträge (§ 134 BGB). Dass die strafrechtliche Seite des Datenschutzrechts deutlich schärfere Zähne hat, als die behördliche Aufsicht sie zu zeigen gewillt ist, können betroffene Personen als eine gute Nachricht verbuchen.

Ordnungswidrigkeitenrecht als Beschleuniger zur Durchsetzung von Betroffenenrechten

Deliktsrechtlich charmant ist wiederum die Verknüpfung von Strafnormen mit § 823 Abs. 2 BGB vor allem dort, wo Schutzgesetzverletzungen auch Unterlassungsansprüche auslösen können, da deren Durchsetzung gegenüber Leistungsansprüchen im Eilrechtsschutz deutlich privilegiert ist. So kann eine falsche Auskunft nach Art. 15 DSGVO neben der allfälligen Leistungsklage auch von einer einstweiligen Verfügung flankiert werden, da eine Verletzung von

Art. 15 DSGVO den Anwendungsbereich des Art. 83 Abs. 5 lit. b) DSGVO eröffnet und über § 41 Abs. 1 BDSG entsprechende Verstöße als Ordnungswidrigkeit sanktioniert sind. Da die Bußgeldbewehrung nach Auffassung der Rechtsprechung auch im Interesse der betroffenen Personen ist, stellen diese Normen auch Schutzgesetze dar, deren Verletzung einen Unterlassungsanspruch gegen den Verantwortlichen auslösen kann. Dessen Geltendmachung im Eilverfahren binnen weniger Tage fördert rechtskonformes Handeln wesentlich effektiver als das jahrelange Zuwarten auf eine Hauptsacheentscheidung auf Erteilung einer korrekten Auskunft. Wie diese Beispiele zeigen, ist die enge Verzahnung von Datenschutz-, Zivil- und Strafrecht nicht etwas Außergewöhnliches, sondern der Regelfall und das Datenschutzrecht fügt sich mit etwas gutem Willen harmonisch in den bestehenden nationalen Rechtsrahmen ein.

Gemeinsam allein: Kann das Datenschutzrecht vom Wettbewerbsrecht lernen?

Effektivitätserwägungen statt strikter Dogmatik bei der Anwendung von Art. 26 DSGVO

Für die Feststellung einer gemeinsamen Verantwortlichkeit geht der EuGH zunächst von einer weiten Auslegung des Begriffs des „Verantwortlichen“ aus, um aus Perspektive der betroffenen Person effektiven Grundrechtsschutz zu gewährleisten. Hohe Anforderungen an die „Gemeinsamkeit“ der Verantwortung stellt das Gericht nicht. Schien in C-210/16 – *Wirtschaftsakademie* noch eine gewisse Mitwirkung durch Einstellung des Analysetools („Parametrierung“) gefordert worden zu sein, so zieht der EuGH in C-40/17 – *Fashion ID* die Kreise deutlich weiter und lässt die faktische Implementierung von Programmcode auf der eigenen Website genügen, um eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO zu begründen, wenn und soweit dadurch eine Verarbeitung veranlasst wurde. Aus dem Schutzgedanken heraus, für die betroffenen Personen die Art. 7 und 8 der GRCh zur vollen Geltung zu bringen und Rechtsdurchsetzung weitgehend zu erleichtern, ergibt dieses rustikale Vorgehen durchaus Sinn. Es kollidiert nur mit dem *laissez passer*, welches der Aufbau komplexer Onlineprojekte mit Bausteinen Dritter üblicherweise mit sich bringt. Denn plötzlich sitzen Beteiligte unterschiedlicher Größe und Gewichtung gemeinsam in einem Boot, die miteinander bisher wenig zu tun hatten und müssen nun füreinander einstehen, mangels anderweitiger Regelungen auf der von § 426 Abs. 1 und 2 BGB bedingten gleichen Augenhöhe. Besonders schmerzlich muss dieses Empfinden für marktbeherrschende Technologie-Dienstleister wie Facebook, Google oder Adobe sein, die sich beim besten Willen nicht in ein Boot mit Millionen von Joint Controllern setzen wollen; zumal das nationale Gesellschaftsrecht auch an das Entstehen einer GbR (OHG) aus Gründen des Gläubigerschutzes ähnliche, niedrige Anforderungen wie Art. 26 DSGVO stellt und eine

solche gesellschaftsrechtliche Verbindung nach Deutschland hinein möglicherweise unangenehme zivilprozessuale Folgen haben könnte.

Kriterien der wettbewerbsrechtlichen Beauftragtenhaftung für Zurechnung bei arbeitsteiligem Wirtschaften

Bereits seit 1909 kennt das UWG eine Norm, deren Sinn und Zweck es ist, zu verhindern, dass sich Unternehmer durch den Hinweis auf für sie handelnde Mitarbeiter oder sonstige Dritte, auch völlig fremde Unternehmen, ihrer Verantwortung entziehen können (heute: § 8 Abs. 2 UWG, Parallelnormen: § 14 Abs. 7 MarkenG, § 99 UrhG). Die Vorschrift verschärft die Verantwortung des Unternehmensinhabers gegenüber den allgemeinen zivilrechtlichen Vorschriften. Es bedarf weder einer schuldrechtlichen Sonderverbindung wie bei § 278 BGB noch gestattet das Recht einen Entlastungsbeweis wie in § 831 BGB. Der Inhaber des Unternehmens haftet unabhängig von dem Wissen um die Verletzungshandlung seines Mitarbeiters oder Beauftragten. Die Verantwortlichkeit des Unternehmensinhabers tritt selbst dann ein, wenn die Verletzungshandlung gegen seinen Willen begangen wird. Es handelt sich um eine verschuldensunabhängige Erfolgshaftung, die voraussetzt, dass der Mitarbeiter oder Beauftragte eine rechtswidrige Verletzungshandlung begangen hat (BGH, Urteil v. 05.04.1995, I ZR 133/93 – *Franchise-Nehmer*). Begrenzendes Merkmal ist nach gefestigter Rechtsprechung jedoch der „innere Zusammenhang“, so dass unternehmensfremde, auch rein eigennützige Handlungen des Beauftragten nicht der Geschäftsorganisation des „Betriebsinhabers“ zuzurechnen sind (BGH, Urteil v. 7.10.2009, I ZR 109/06 – *Partnerprogramm*).

Übertragung wettbewerbsrechtlicher Kriterien auf das Datenschutzrecht

Das Reichsgericht schuf in seiner legendären „Alpina-Uhren“-Entscheidung (RGZ 151, 237 ff.) die Grundlage für die derzeitige wettbewerbsrechtliche Rechtsprechung zur Beauftragtenhaftung in Deutschland. Die Parallelen bei der Interessenlage zwischen Art. 26 DSGVO und § 8 Abs. 2 UWG sind, bei einigen Unschärfen im Detail, unübersehbar: Die Verhinderung von Verantwortungsdiffusion durch Arbeitsteilung. Der „Bauherr“ komplexer technischer Anwendungen, die personenbezogene Daten verarbeiten, stellt fest, dass er die Verantwortung für das Gesamtprojekt „Website“ oder „App“ nicht einfach an Dritte auslagern kann, sondern dass er für alle eingebauten Funktionen und Gewerke auch datenschutzrechtlich einstehen muss. Anders als Art. 26 DSGVO, dessen Anwendungsbereich noch konturenlos erscheint und den selbst die aktuellen „Guidelines 07/2020 on the concepts of controller and processor in the GDPR“ des EDPB trotz zahlreicher Anwendungsbeispiele nicht hinreichend bestimmen können, bietet das seit über 100 Jahren bewährte

wettbewerbsrechtliche Konzept der Beauftragtenhaftung ein Mindestmaß an Konturen. Mit der Abgrenzung der Geschäftsbereiche legt es auch ein praktikableres Kriterium zugrunde, als die Versuche des EuGH, die einmal in *Wirtschaftsakademie* geöffnete „Büchse der Pandora“ über ein Abstellen auf einzelne technische Datenverarbeitungsvorgänge zu begrenzen. Das kurze Plädoyer für eine Übernahme der Kriterien des Wettbewerbsrechts ins Datenschutzrecht und damit für einen Schritt in Richtung Harmonisierung ausgehend von historisch bewährtem nationalem Recht, kommt nicht von ungefähr. Datenschutzverstöße können nach herrschender und überzeugender Meinung auch als Wettbewerbsverstöße geahndet werden. Spätestens nach einer (positiven) Entscheidung des EuGH zur Vorlagefrage (BGH I ZR 186/17 – *App-Zentrum*) ist eine Entscheidung über eine einheitliche Auslegung der Kriterien im Datenschutz- und Wettbewerbsrecht sinnvoll. Es ließe sich nur schwer begründen, die Anwendung von Art. 26 DSGVO zu verneinen, die Datenschutzverstöße dann aber über § 8 Abs. 2 UWG oder § 2 Abs. 1 UKlaG doch wieder zuzurechnen.

Fazit

„Datenschutzrecht ist mehr als DSGVO“ lautet eine moderne Binsenweisheit. Die Kenntnis des nationalen Rechts und das Zusammenspiel mit europäischen Vorschriften ist unerlässlich, um rechtssicher beraten und handeln zu können. Nicht immer muss dabei das Rad neu erfunden werden. Bekannte und bewährte Konzepte, wie die Kausalitätsvermutung bei unaufklärbaren Sachverhalten, die Gesamtschuld des Deliktsrechts sowie die verschuldens- und kenntnisunabhängige Erfolgshaftung des Wettbewerbsrechts sind historische Konzepte, die sich in guten wie in schlechten Zeiten der Wirtschaftsrechtsgeschichte geformt und bewährt haben. Ein Blick auf diese Normen kann auch im Datenschutzrecht mitunter die Rechtsfindung erleichtern.

Autor: Peter Hense ist Rechtsanwalt und Partner bei SPIRIT LEGAL Rechtsanwälte in Leipzig. Seine Tätigkeitsschwerpunkte liegen im Technologie-, Daten- und Wettbewerbsrecht sowie der Prozessführung (Privacy Litigation).

