

Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

4

K&R

- Editorial: Influencerwerbung und keine Aussicht auf Klarheit über Kennzeichnungspflicht · *Fabian Reinholz*
- 245 Ist die Meinungsfreiheit in deutschen Fußballstadien nach der Causa Hopp in Gefahr? · *Robert Golz*
- 248 Ist der Regierungsentwurf eines NetzDG 2.0 vom 19. 2. 2020 netzgerecht? · *Prof. Dr. Dr. Karl-Heinz Ladeur*
- 253 Verarbeitung biometrischer Daten – sind die neuen Geschäftsmodelle zulässig? · *Conrad S. Conrad*
- 259 Belehrungspflicht über Herstellergarantien bei Fernabsatzverträgen (?)
Prof. Dr. Felix Buchmann und Fabian Großbach
- 263 Registrierungspflicht für Prepaid-SIM-Karten verstößt nicht gegen EMRK · *Jan Spittka*
- 267 Aktuelle Rechtsentwicklungen bei Suchmaschinen im Jahre 2019
Dr. Sebastian Meyer und Dr. Christoph Rempe
- 275 Länderreport Österreich · *Prof. Dr. Clemens Thiele*
- 281 BGH: Identifizierende Bildberichterstattung im Verwaltungsverfahren erlaubt mit Kommentar von *Martin W. Huff*
- 289 BGH: yelp.de: Kein Anspruch auf bestimmte Bewertungsdarstellung in Internet-Bewertungsportal
- 296 BGH: Zur Rechtmäßigkeit von Inbox-Werbung in E-Mail-Postfächern
- 306 OLG München: Kein Wiederherstellungsanspruch bei gelöschter Hassbotschaft in sozialem Netzwerk
- 314 OLG Stuttgart: Wettbewerbsverband klagebefugt bei fehlender Datenschutzerklärung

23. Jahrgang

April 2020

Seiten 245–324

UWG abstellt³³), sondern über die Garantiebedingungen i. S. d. § 479 Abs. 1 BGB. Das Weglassen *dieser* Information ist keine Bagatelle.

IV. Konsequenzen für Online-Händler

Es genügt nicht, dass ein Online-Händler in seinem eigenen Angebot auf das Wort „Garantie“ oder auf sonstige Hinweise verzichtet, die darauf schließen lassen, dass der Hersteller für eine bestimmte Beschaffenheit verschuldensunabhängig einstehen will³⁴, und damit von allen Sorgen befreit ist. Wenn er Produkte anbietet, für die der Hersteller selbst in der einschlägigen Werbung und für den Kundenkreis des Online-Händlers verfügbar eine Garantie bewirbt, so ist der Online-Händler verpflichtet, die vollständigen Garantiebedingungen des Herstellers verfügbar zu machen. Ob dies bereits als Nachforschungspflicht verstanden werden kann, ist Auslegungssache. Jedenfalls muss ein Online-Händler wissen, was er verkauft; dieser Kenntnisstand schließt das Vorliegen einer Hersteller-Garantie ein. Auch wenn dies zunächst als massive Belastung des Online-Händlers verstanden werden könnte, ist *diese* Verpflichtung noch im Rahmen des Möglichen. Wenn selbst ein potenzieller Kunde, der sich im üblichen Umfang vor dem Erwerb eines Produkts mit der Frage einer Herstellergarantie befassen kann, weil diese durch die Werbung, die sich an diesen Kunden richtet, hinreichend bekannt ist, dürfte auch ein Online-Händler von der Garantie des Herstellers Kenntnis haben.

Unmöglich hingegen wird für den Online-Händler die sich daraus ergebende Konsequenz, nämlich das Vorhalten einer rechtskonformen Garantieerklärung, auf deren Inhalt er keinen Einfluss hat. Wer allerdings aktiv auf die Garantieerklärung des Herstellers verlinkt, macht sich deren Inhalt auch zu eigen, so dass er für den Fall der Nichtkonformität mit § 479 Abs. 1 BGB auch persönlich dafür haftet und insbesondere auf Unterlassung in Anspruch genommen werden kann.³⁵ Der zweite Schritt in der 2-Stufen-Prüfung wird daher für Online-Händler das entscheidende Problem werden: Stellt sich in der ersten Stufe der Prüfung heraus, dass der Hersteller eine Garantie für ein bestimmtes Produkt anbietet und bewirbt, muss der Händler in der zweiten

Stufe prüfen, ob die Garantieerklärung § 479 Abs. 1 BGB genügt. Ohne juristische Kenntnisse wird ein Online-Händler hierzu kaum in der Lage sein. Im Zweifel muss er also das Produkt aus seinem Angebot nehmen.

V. Fazit

Die gesetzeskonforme Information über eine Hersteller-Garantie erfolgt im Wege eines 2-Stufen Tests:

Verwendet ein Händler in seinem Angebot – gleich in welcher Form und an welchem Ort – Hinweise darauf, dass der Hersteller des Produkts für dessen Beschaffenheit und/oder Haltbarkeit eine Verpflichtung übernimmt, die über die gesetzliche Mängelhaftung hinausgeht, so handelt es sich um eine Garantie im Sinne des § 443 Abs. 1 BGB. Über die Bedingungen der Garantie muss er gemäß Art. 246 a § 1 Abs. 1 S. 1 Nr. 9 i. V. m. Art. 246 a § 4 Abs. 1 EGBGB vor Abgabe der Willenserklärung des Verbrauchers klar und verständlich informieren. Dies umfasst eine Garantieerklärung nach Maßgabe des § 479 Abs. 1 BGB.

Verwendet ein Händler in seinem Angebot keine solchen Hinweise, so treffen ihn dennoch die gleichen Verpflichtungen, wenn der Hersteller dies in der einschlägigen Werbung, die vor oder bei Abschluss des Kaufvertrags verfügbar war, erklärt hat. Nur dann können sie Teil der Vorstellung des Verbrauchers werden und damit seiner Kaufentscheidung zugrunde liegen. Entscheidend ist also, ob es zwischen dem Käuferkreis des Online-Händlers und dem Adressatenkreis der Hersteller-Werbung eine Schnittmenge gibt. Die Ausrichtung ist in jedem Einzelfall an den vorhandenen Indizien zu prüfen. Wird dann eine Garantie i. S. d. § 443 Abs. 1 BGB bejaht, muss im Rahmen der vorvertraglichen Information eine vollständige Garantieerklärung nach Maßgabe des § 449 Abs. 1 BGB vorgehalten werden.

33 OLG Frankfurt a. M., 21. 1. 2020 – 6 O 7/19, II. 1.

34 *Pammler*, in: Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB (Fn. 10), Rn. 16; BGH, 17. 3. 2010 – VIII ZR 253/08 (zu den konkretisierenden Anforderungen); OLG Köln, 15. 10. 2012 – 11 U 153/12 (unbedingte Wille zur Abgabe einer Garantie muss erkennbar sein).

35 BGH, 5. 12. 2012 – I ZR 88/11, K&R 2013, 487 ff.; BGH, 5. 12. 2012 – I ZR 146/11; K&R 2013, 584 ff.; BGH, 14. 4. 2011 – I ZR 133/09, K&R 2011, 501 ff.

RA Jan Spittka, Köln*

Registrierungspflicht für Prepaid-SIM-Karten verstößt nicht gegen EMRK

Zugleich Besprechung von EGMR, Entscheidung vom 30. 1. 2020 – Nr. 50001/12 – Breyer gegen Deutschland

I. Hintergrund der Entscheidung

Der EGMR¹ hatte über eine Individualbeschwerde nach Art. 34 EMRK der Beschwerdeführer *Jonas* und *Patrick Breyer*, letzterer bereits bekannt aus der EuGH-Entscheidung „Patrick Breyer gegen Bundesrepublik Deutschland“² zur Verarbeitung von IP-Adressen durch Website-Betreiber, gegen die Registrierungspflicht für Prepaid-

SIM-Karten nach § 111 TKG a. F. zu entscheiden. Nachdem die Beschwerdeführer im Jahr 2012 mit einer Ver-

* Mehr über den Autor erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 11. 3. 2020.

1 EGMR, 30. 1. 2020 – Nr. 50001/12, KuRL2020-263 (www.kommunikationunrecht.de, in englischer Sprache).

2 EuGH, 19. 10. 2016 – C-582/14, K&R 2016, 811 ff.

fassungsbeschwerde gegen die Registrierungspflicht vor dem BVerfG gescheitert waren,³ riefen sie den EGMR an und trugen vor, die entsprechende Regelung in § 111 TKG a. F. sei mit dem Recht auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK sowie der Freiheit der Meinungsäußerung nach Art. 10 EMRK nicht vereinbar. Im Kern argumentieren die Beschwerdeführer, die vorgenannten Vorschriften der EMRK gäben ihnen ein Recht auf anonyme Kommunikation mittels SIM-Karten für Mobilfunknetze. Die durch § 111 a. F. TKG vorgesehene Registrierungspflicht sei weder erforderlich noch verhältnismäßig, könne leicht umgangen werden und habe nicht belegbar zu einer Verringerung der Kriminalität beigetragen. Im Ergebnis handele es sich auch hier um eine unzulässige Form der Vorratsdatenspeicherung.

Gegenstand des Verfahrens vor dem EGMR war nicht die aktuelle Fassung der §§ 111-113 TKG, sondern die am 1. 1. 2008 in Kraft getretene Fassung,⁴ da diese Gegenstand der vorgenannten Verfassungsbeschwerde war. Der EGMR weist darauf hin, dass gegen die Vorschriften in der zum 30. 7. 2016 in Kraft getretenen Fassung,⁵ die u. a. zusätzlich zur Pflicht der reinen Datenerhebung eine Verifizierungspflicht für TK-Anbieter bei im Voraus bezahlten Mobilfunkdiensten beinhalten, noch eine Verfassungsbeschwerde vor dem BVerfG⁶ anhängig ist.

In der angegriffenen Fassung verpflichtet § 111 TKG geschäftsmäßige Anbieter von Telekommunikationsdiensten, die von ihnen vergebenen beziehungsweise bereitgestellten Rufnummern, Anschlusskennungen, Mobilfunkendgerätenummern und Kennungen von elektronischen Postfächern sowie die zugehörigen persönlichen Daten der Anschlussinhaber wie Namen, Anschriften und Geburtsdaten – einschließlich zudem der Daten des Vertragsbeginns – zu erheben und zu speichern. Die Pflicht zur Datenerhebung besteht hierbei unabhängig davon, ob die Daten für die Erfüllung des Vertrages mit dem Kunden, z. B. zur Abrechnung, überhaupt erforderlich sind und erfasst daher auch vorausbezahlte Mobilfunkkarten und Internetzugangsleistungen (sog. Prepaid-SIM-Karten).

Die Vorschrift soll eine Datenbasis für die in §§ 112, 113 TKG a. F. geregelten Auskunftsverfahren schaffen. Durch § 112 TKG a. F. wird ein automatisiertes Verfahren zur Erteilung von Auskünften aus den nach § 111 TKG a. F. gespeicherten Daten geschaffen. Danach haben Anbieter, die Telekommunikationsdienste für die Öffentlichkeit erbringen, die von § 111 TKG a. F. erfassten Daten nach Maßgabe einer die technischen Details regelnden Rechtsverordnung so bereit zu stellen, dass sie von der Bundesnetzagentur (BNetzA) ohne Kenntnisnahme der Anbieter abgerufen werden können (§ 112 Abs. 1 TKG a. F.). Die BNetzA hat diese Datensätze auf Ersuchen näher bezeichneter Behörden im automatisierten Verfahren abzurufen und diesen zu übermitteln (vgl. § 112 Abs. 4 TKG a. F.). Zu den berechtigten Behörden gehören insbesondere die Strafverfolgungsbehörden, die Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr, das Zollkriminalamt, die Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst und der Bundesnachrichtendienst, Notrufabfragestellen, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) sowie Behörden der Zollverwaltung für Zwecke der Schwarzarbeitsbekämpfung (vgl. § 112 Abs. 2 TKG a. F.).

Ein manuelles Verfahren für Auskünfte aus den nach § 111 TKG a. F. gespeicherten Daten regelt § 113 TKG a. F. Im

Gegensatz zu dem automatisierten Auskunftsverfahren sieht dieses eine Verpflichtung zur Auskunftserteilung durch die Telekommunikationsunternehmen selbst vor. Ebenso wie im automatisierten Auskunftsverfahren ist über die Auskunftserteilung gegenüber den Datenbetroffenen Stillschweigen zu wahren (vgl. § 113 Abs. 1 S. 4 TKG a. F.). Erweitert ist auch der Kreis der auskunftsberechtigten Behörden. § 113 Abs. 1 S. 1 TKG a. F. enthält für allgemeine Auskünfte keine enumerative Aufzählung der auskunftsberechtigten Behörden, sondern umschreibt die Auskunftsberechtigung abstrakt aufgabenbezogen und damit uneingeschränkt für alle Behörden: Auskünfte sollen allgemein zulässig sein, soweit dies im Einzelfall für die Verfolgung von Straftaten und Ordnungswidrigkeiten, die Gefahrenabwehr und die Erfüllung nachrichtendienstlicher Aufgaben erforderlich ist.

II. Inhalt und Begründung der Entscheidung

Im Ergebnis sieht der EGMR weder in den §§ 111-113 TKG a. F. noch in deren Auslegung durch das BVerfG eine Verletzung der Art. 8, 10 EMRK. Der als Vertreter Liechtensteins an den EGMR entsandte Richter *Carlo Ranzoni* teilte diese Mehrheitsentscheidung allerdings nicht und verfasste eine abweichende Stellungnahme (*dissenting opinion*).

1. Mehrheitsentscheidung

Obwohl sich die Individualbeschwerde der Herren *Breyer* formal lediglich gegen die Registrierungspflicht von Prepaid-SIM-Karten nach § 111 TKG a. F. und nicht gegen §§ 112, 113 TKG a. F. richtet, bezieht der EGMR auch die Zugriffsrechte der BNetzA und der übrigen Behörden in die Bewertung mit ein, da das Gericht der Auffassung ist, man könne eine Datenspeicherung nicht unter Ausklammerung der weiteren Datennutzung bewerten.

Im Rahmen einer knappen Vorabprüfung kommt der EGMR zu dem Ergebnis, dass Prüfungsmaßstab im vorliegenden Fall allein das Recht auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK – in Form des datenschutzrechtlich geprägten „Right to Privacy“ – und nicht die Freiheit der Meinungsäußerung nach Art. 10 EMRK sei. Zwar erfolge die Speicherung der personenbezogenen Daten im Rahmen des § 111 TKG a. F. in einem telekommunikationsbezogenen Kontext, es gehe jedoch um die Speicherung von Bestandsdaten in Form von Telefonnummern, den Namen und Adressen, Geburtsdaten und Daten der Verträge. Obwohl sich der EGMR der Nähe dieser Daten zu konkreten Kommunikationsvorgängen durchaus bewusst ist, sieht das Gericht den Fokus auf der Datenspeicherung und nicht auf dem Abfangen von „Korrespondenz“ und einer damit verbundenen Beeinträchtigung der Meinungsfreiheit. Nach Auffassung des EGMR sei demnach im vorliegenden Fall nicht zu prüfen, ob und in welchem Umfang Art. 10 EMRK den Nutzern von Telekommunikationsdiensten ein Recht auf anonyme Nutzung zugesteht.

Das Gericht beginnt sodann unter Bezugnahme der relevanten bisherigen Rechtsprechung mit grundsätzlichen Ausführungen zur Auslegung des Art. 8 EMRK. Das Recht auf Achtung des Privatlebens beinhalte auch ein Datenschutzrecht in Form eines „right to privacy, with regard to

3 BVerfG, 24. 1. 2012 – 1 BvR 1299/05, K&R 2012, 274.

4 BGBl. 2007 I S. 3198.

5 BGBl. 2016 I S. 1818.

6 BVerfG, 1 BvR 1713/17.

automatic processing of personal data“, einschließlich eines Rechts auf informationelle Selbstbestimmung („Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such form or manner that their Article 8 rights may be engaged“). Der vorliegende Fall, in dem es allein um die Speicherung personenbezogener Daten gehe, sei von den bislang durch das Gericht entschiedenen Fällen noch nicht abgedeckt. Bei der Frage einer staatlichen bzw. staatlich angeordneten Datenspeicherung hätte der jeweilige Staat zwar einen gewissen Ermessensspielraum, dieser sei jedoch geringer, wenn das betroffene Recht intime oder Schlüsselrechte („intimate or key rights“) schütze. Soweit hinsichtlich der Auslegung noch kein Konsens zwischen den Mitgliedsstaaten des Europarates bestehe, sei der Ermessensspielraum weiter gefasst.

Sodann prüft der EGMR den Fall anhand der bekannten Dogmatik: Eingriff und Rechtfertigung (gesetzlich vorgesehen, legitimer Zweck und in einer demokratischen Gesellschaft notwendig).

a) Gesetzlich vorgesehen

Die Speicherung der personenbezogenen Daten der Nutzer mobiler Telekommunikationsdienste auf Grundlage des § 111 TKF a. F. könne als gesetzlich vorgesehen („in accordance with the law“) bewertet werden, da der Umfang der gespeicherten Daten eindeutig und vorhersehbar sei. Dies gelte auch für die behördlichen Zugriffsrechte nach §§ 112, 113 TKG a. F. Das vom BVerfG entwickelte „Doppeltürenmodell“, bestehend aus einer privaten Befugnis zur Datenweitergabe und einer staatlichen Befugnis zur Datenerhebung,⁷ sei hinreichend bestimmt.

b) Legitimer Zweck

Die seitens der Bundesregierung angeführten Zwecke der öffentlichen Sicherheit, Gefahrenabwehr, Strafverfolgung und Schutz der Rechte und Freiheiten anderer stellten legitime Zwecke für einen Eingriff in Art. 8 EMRK dar.

c) Notwendigkeit in einer demokratischen Gesellschaft

Im Rahmen der Notwendigkeit der Maßnahme in einer demokratischen Gesellschaft prüft der EGMR, ob und inwieweit die Maßnahme eine Reaktion auf eine dringende gesellschaftliche Notwendigkeit („pressing social need“) und verhältnismäßig ist.

Verbrechensbekämpfung, insbesondere im Hinblick auf organisierte Kriminalität und Terrorismus, und die damit verbundene Aufrechterhaltung der öffentlichen Sicherheit und der Schutz der Bürger seien in den heutigen europäischen Gesellschaften eine dringende gesellschaftliche Notwendigkeit. Vor dem Hintergrund der modernen Telekommunikationsmittel müssten auch die Ermittlungsbefugnisse für Strafverfolgungs- und Sicherheitsbehörden („law enforcement and national security agencies“) angepasst werden. Das Argument, die Einführung der Registrierungspflicht für Prepaid-SIM-Karten habe zu keinem empirischen Nachweis eines Rückgangs von Straftaten geführt, weist das Gericht mit dem Argument zurück, dass eine Umgehung niemals ausgeschlossen werden könne und die Mitgliedsstaaten hier einen gewissen Ermessensspielraum hätten.

Sodann nimmt der EGMR eine umfassende Verhältnismäßigkeitsprüfung im Sinne einer Abwägung zwischen

öffentlichen und privaten Interessen vor. Hinsichtlich der Speicherung der Bestandsdaten nach § 111 TKG a. F. kommt das Gericht zu dem Ergebnis, dass diese Speicherung hinsichtlich der Eingriffsintensität zwar nicht trivial sei, aber dennoch nur von begrenztem Umfang. Hierbei wird insbesondere darauf abgestellt, dass weder höchstpersönliche Daten gespeichert werden, noch diese Daten zur Bildung von Persönlichkeitsprofilen oder zur Verfolgung der Bewegung von Mobilfunknutzern genutzt werden können. Hierin liege ein wesentlicher Unterschied zu den bisherigen Vorratsdatenspeicherungsfällen „Digital Rights Ireland und Seitlinger u. a.“⁸ sowie „Tele2 Sverige und Tom Watson u. a.“⁹. Es gehe gerade nicht um die Speicherung von Verkehrs- und Standortdaten, weshalb keine Rückschlüsse auf Datum, Uhrzeit, Dauer der Kommunikation sowie Kommunikationspartner bzw. von Angaben zu Standort während und Häufigkeit der Kommunikation gezogen werden können. Eine abweichende Bewertung ergäbe sich auch nicht aus der Berücksichtigung der behördlichen Zugriffsrechte nach §§ 112, 113 TKG. Hier erkennt der EGMR zwar an, dass grundsätzlich eine heimliche Überwachung vorliegen kann, diese aber durch den vom BVerfG geforderten Anfangsverdacht kompensiert werde. Zudem falle die Überprüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten im Rahmen der §§ 111 - 113 TKG a. F. in den Aufgabenbereich der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, was zu einer Sicherung der Rechte der Betroffenen beitrage. Alles in allem habe die Bundesrepublik ihren Ermessensspielraum bei der Ausgestaltung der Registrierungspflicht für Prepaid-SIM-Karten damit nicht überschritten.

2. Dissenting Opinion des Richters Ranzoni

Richter *Ranzoni* hat sich der Mehrheitsauffassung der fünften Kammer des EGMR nicht angeschlossen und eine abweichende Stellungnahme verfasst. Auch Richter *Ranzoni* wendet allein Art. 8 EMRK als Prüfungsmaßstab an. Er bewertet die Eingriffsintensität des § 111 TKG a. F. (i. V. m. §§ 112, 113 TKG a. F.) jedoch deutlich schwerer als seine Kolleginnen und Kollegen und kommt zu dem Ergebnis, dass die Registrierungspflicht für Prepaid-SIM-Karten unverhältnismäßig ist.

Zwar seien die gespeicherten Daten für sich genommen zwar wenig belastend. Die Registrierungspflicht führe dazu, dass eine Vielzahl von Behörden auf einfachem Weg Zugang zu einer großen Anzahl an Daten bekommen würde. Die Zugriffsrechte seien weder auf Fälle des Terrorismus oder vergleichbarer schwererer Straftaten oder Fälle der nationalen Sicherheit beschränkt, noch läge eine Beschränkung auf entsprechende Behörden vor. Selbst die Zollverwaltung und die BaFin hätten Zugang.

Ein umfassendes Register aller Mobilfunknutzer sei ein wesentlicher Schritt für weitere, deutlich eingriffsintensivere Maßnahmen, wie sie Gegenstand der Fälle „Digital Rights Ireland und Seitlinger u. a.“¹⁰ sowie „Tele2 Sverige und Tom Watson u. a.“¹¹ waren. Nur Anonymität könne Schutz vor Repressalien oder unerwünschter Aufmerk-

⁷ Siehe hierzu *Mantz/Sassenberg*, NJW 2014, 3537, 3540 m. w. N.

⁸ EuGH, 8. 4. 2014 – C-293/12, EuGH, 8. 4. 2014 – C-594/12, K&R 2014, 405.

⁹ EuGH, 21. 12. 2016 – C-203/15, EuGH, 21. 12. 2016 – C-698/15, K&R 2017, 105.

¹⁰ EuGH, 8. 4. 2014 – C-293/12, EuGH, 8. 4. 2014 – C-594/12, K&R 2014, 405.

¹¹ EuGH, 21. 12. 2016 – C-203/15, EuGH, 21. 12. 2016 – C-698/15, K&R 2017, 105.

samkeit bieten und damit Gedanken- und Informationsfreiheit gewährleisten.

Zudem übt Richter *Ranzoni* Kritik am Doppeltürenmodell des BVerfG. Dadurch, dass auf Seiten der Behörden auch allgemeine Ermittlungsbefugnisse, wie z. B. § 163 StPO, ausreichen würden, läge kein ausreichender Schutz personenbezogener Daten vor. Auch läge keine hinreichende Kontrolle vor: „The double-door can be easily opened by those keys, but there is nobody waiting on the other side of the door to check which items pass the door and are subsequently used“. Darüber hinaus stellt Richter *Ranzoni* die Interpretation der Entscheidung „Minitro Fiscal“¹² durch die Kammer in Frage. In „Minitro Fiscal“ sei es nur um eine beschränkte Datenverarbeitung über einen sehr beschränkten Zeitraum gegangen. Vorliegend handele es sich um eine anlasslose Datenspeicherung über einen langen Zeitraum. Die Gefahr eines Missbrauchs sei bei einer derart großen Datenmenge (rund 35 Millionen Datensätze) schlicht zu groß.

III. Beurteilung der Entscheidung

Der EGMR musste sich einmal mehr mit der – gerade im Bereich der Telekommunikation – schwierigen Abwägung zwischen informationeller Selbstbestimmung und den Sicherheitsinteressen des Staates befassen. Bereits im für das Recht auf informationelle Selbstbestimmung grundlegenden *Volkszählungsurteil* von 1983 hat das BVerfG klargestellt, dass dieses Recht nicht grenzenlos gewährt wird und (nur) soweit beschränkt werden darf, als es zum Schutz öffentlicher Interessen unerlässlich ist.¹³ Dass man die Gewichtung der unterschiedlichen Interessen in diesem Konflikt auch im konkreten Einzelfall durchaus unterschiedlich bewerten kann, zeigt die abweichende Stellungnahme des Richters *Ranzoni*.

Die Frage, inwieweit Art. 8 EMRK das Recht auf (einfache) anonyme Nutzung mobiler Kommunikationsmittel durch einen Anspruch auf nicht registrierte im Voraus bezahlte Mobilfunkdienste gibt, verneint der EGMR vorliegend, indem er die deutsche Registrierungsspflicht mit Blick auf einen gewissen staatlichen Ermessensspielraum bei Strafverfolgung und Gefahrenabwehr für zulässig erklärt. Diese Registrierungsspflicht ist seit 2016 noch einmal durch die Ausweispflicht in § 111 Abs. 1 S. 3 TKG verschärft worden. Es ist also wieder schwerer geworden, sich eine SIM-Karte auf den Namen „Donald Duck“¹⁴ zu besorgen. Die Ausweispflicht war jedoch nicht Gegenstand des Verfahrens.

Gleichzeitig macht der EGMR zu Recht deutlich, dass bereits die Speicherung personenbezogener Daten (ohne konkrete Nutzung) einen rechtfertigungsbedürftigen Eingriff in Art. 8 EMRK darstellt. Unter den Bedingungen der automatisierten Datenverarbeitung gab es schon 1983 kein „belangloses“ Datum mehr.¹⁵ Das gilt heutzutage umso mehr. Zudem betont das Gericht, dass es im Rahmen der Verhältnismäßigkeitsprüfung eine erhebliche Rolle spielt, ob lediglich Bestandsdaten (also Rufnummern, Anschlusskennungen, Mobilfunkendgerätenummern sowie die zugehörigen persönlichen Daten der Anschlussinhaber wie Namen, Anschriften und Geburtsdaten, einschließlich der Daten des Vertragsbeginns) gespeichert werden oder aber Verkehrs- und Standortdaten, die eine langfristige Überwachung der Bewegungen und des Kommunikationsverhaltens des Mobilfunkteilnehmers bis hin zur Bildung von Persönlichkeitsprofilen ermöglichen, verarbeitet werden. Die Entscheidung kann daher nicht als Carte blanche für eingriffsintensivere

Maßnahmen und auf gar keinen Fall als Argument für die Zulässigkeit einer generellen, anlasslosen und uneingeschränkten Vorratsdatenspeicherung von Verkehrsdaten,¹⁶ wie sie derzeit in §§ 113 a ff. TKG vorgesehen und bereits wiederum Gegenstand eines EuGH-Verfahrens ist.¹⁷ Jede über die reine Speicherung von Bestandsdaten hinausgehende Maßnahme muss im konkreten Fall vor dem Hintergrund der Verhältnismäßigkeit eingehend geprüft werden. So wie es kein absolutes Recht auf Datenschutz gibt, existiert auch kein absolutes Recht auf Sicherheit in Form staatlicher Überwachung. In einem demokratischen Rechtsstaat rechtfertigt der Zweck eben nicht alle Mittel.

Die Entscheidung des EGMR gegen ein Recht auf anonyme Nutzung mobiler Kommunikationsmittel ist sicherlich vertretbar. Selbstverständlich sind die sichersten personenbezogenen Daten solche, die nie erhoben bzw. gespeichert wurden. Bereits 1824 führte *Leopold Joseph Neustetel* in seiner Kritik am Büchernachdruck aus: „Würde jeder Dritte fremde Rede nach Gefallen bekannt machen dürfen, so ist nichts gewisser, als dass die freie Rede in und außer Hause, in Wort und Schrift, größtenteils würde verstummen müssen“.¹⁸ Dass bereits das Gefühl einer Überwachung nicht nur zu Unbehagen, sondern auch dazu führen kann, dass andere Grundrechte nur eingeschränkt oder gar überhaupt nicht mehr ausgeübt werden, ist mittlerweile höchststrichterlich anerkannt.¹⁹ Ob ein solches Gefühl des ständigen Überwachtwerdens jedoch bereits durch die Pflicht zur namentlichen Registrierung von SIM-Karten erzeugt wird, darf zu Recht bezweifelt werden. Umgekehrt führt die Registrierungsspflicht jedenfalls dazu, dass Kriminellen und Terroristen der Zugang zu anonymen SIM-Karten erschwert wird. Das Argument der Beschwerdeführer, die Einführung der Registrierungsspflicht für Prepaid-SIM-Karten habe zu keinem empirischen Nachweis eines Rückgangs von Straftaten geführt, ist insoweit nicht zielführend. Zum einen ist es nicht möglich, eine Entwicklung ohne Registrierungsspflicht zu bewerten, zum anderen führt dieses Argument nur zu einer Rechtfertigung von Verschärfungen, wie sie durch die Ausweispflicht beim Kauf von im Voraus bezahlten Mobilfunkdiensten erfolgte.

Allerdings muss man auch Richter *Ranzoni* zugestehen, dass er den Finger in die wunden Punkte einer massenweisen Speicherung personenbezogener Daten legt. Die nach §§ 112, 113 TKG a. F. zugriffsberechtigten Behörden sind in der Tat sehr weit gefasst und auch hinsichtlich der Zwecke keineswegs auf die Bekämpfung von Terrorismus und anderer vergleichbarer schwerer Straftaten, ja noch nicht einmal auf Abwehr und Verfolgung von Straftaten überhaupt beschränkt. Zugriffsmöglichkeiten auf eine riesige Datenbank ohne richterliche Kontrolle bieten in jedem Fall ein erhebliches Missbrauchspotential, insbesondere, wenn man berücksichtigt, wie großzügig manche Polizeibehörden den Anfangsverdacht auslegen. Der EGMR weist zwar zu Recht auch auf die Kontrollbefugnisse der

12 EuGH, 2. 10. 2018 – C-207/16, K&R 2018, 700.

13 BVerfG, 15. 12. 1983 – 1 BvR 209/83 u. a., NJW 1984, 419, 422.

14 Siehe Bundesministerium des Inneren, Informationen zur „PrePaid“-Regelung v. 1. 6. 2016, S. 1, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/prepaidhintergrund-infoaustausch-terrorbek.pdf?__blob=publicationFile&v=1.

15 BVerfG, 15. 12. 1983 – 1 BvR 209/83 u. a., NJW 1984, 419, 422.

16 Siehe hierzu *Hammer/Müllmann*, K&R 2020, 103.

17 BVerfG, 25. 9. 2019 – 6 C 12/18, K&R 2019, 819.

18 *Neustetel*, Der Buchnachdruck nach dem römischen Recht betrachtet, 1824, S. 47.

19 BVerfG, 15. 12. 1983 – 1 BvR 209/83 u. a., NJW 1984, 419, 422; BVerfG, 2. 3. 2010 – 1 BvR 256/08 u. a., K&R 2010, 248, 249; EuGH, 8. 4. 2014 – C-293/12, EuGH, 8. 4. 2014 – C-594/12, K&R 2014, 405, 407.

Datenschutzbehörden hin, welche diese in Einzelfällen auch gegenüber TK-Unternehmen²⁰ und auch Polizeibeamten²¹ ausüben; dass die Datenschutzbehörden bei ihrer ohnehin knappen personellen Ausstattung jedoch in der Lage sind, jeden Missbrauchsfall bei 35 Millionen Datensätzen ahnden zu können, ist illusorisch.

IV. Ausblick

Der Staat ist aufgrund des nicht zu verneinenden Missbrauchspotentials der nach § 111 TKG a.F. angelegten Datenbanken nicht aus der Verantwortung entlassen, für die Sicherheit von und den verantwortungsvollen Umgang mit personenbezogenen Daten zu sorgen, die er durch TK-Unternehmen erheben und speichern lässt. Auch eine Ausweitung der Zugriffsbefugnisse ist hierbei kritisch zu beobachten. Überwachungsmaßnahmen im Bereich Telekommunikation sollten in jedem Fall nicht zu einem Standard-Tool für Behörden aller Art werden.

Das Urteil des EGMR ist sicher nicht die letzte Gerichtsentscheidung im Spannungsfeld zwischen Datenschutz

und staatlichen Sicherheitsinteressen. Die Beschwerdeführer haben die Möglichkeit, gemäß Art. 44 Abs. 2 lit. b EMRK die Verweisung an die Große Kammer des EGMR zu beantragen. Wie schnell aus einer abweichenden Stellungnahme eines Richters eine Mehrheitsentscheidung werden kann, hat bereits der Fall „Bărbulescu gegen Rumänien“²² gezeigt. Darüber hinaus wird sich das BVerfG noch mit den §§ 112, 113 TKG²³ und der EuGH – mal wieder – mit der anlasslosen Vorratsdatenspeicherung von Verkehrsdaten²⁴ befassen müssen. Da hier andere Maßstäbe gelten, bleibt es also spannend.

20 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Pressemitteilung v. 9. 12. 2019, BfDI verhängt Geldbußen gegen Telekommunikationsdienstleister.

21 Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Pressemitteilung v. 18. 7. 2019, LfDI Baden-Württemberg verhängt erstes Bußgeld gegen Polizeibeamten.

22 EGMR, 5. 9. 2017 – Nr. 61496/08, ZD 2017, 571.

23 BVerfG, 1 BvR 1713/17.

24 BVerfG, 25. 9. 2019 – 6 C 12/18, K&R 2019, 819.

RA Dr. Sebastian Meyer, LL.M. und RA Dr. Christoph Rempe, Bielefeld*

Aktuelle Rechtsentwicklungen bei Suchmaschinen im Jahre 2019

Der Bericht gibt einen Überblick über die rechtlichen Entwicklungen im Zusammenhang mit Suchmaschinen. Berücksichtigt sind gerichtliche Entscheidungen, wissenschaftliche Aufsätze und sonstige Veröffentlichungen aus dem letzten Jahr. Der Bericht knüpft damit an den Überblick des Vorjahres (K&R 2019, 221) an.

I. Einleitung

Das vergangene Jahr stand im Zeichen mehrerer Entscheidungen des EuGH und des BVerfG zum Recht auf Vergessenwerden, die in der Fachliteratur umfassend kommentiert worden sind. Ein weiterhin aktuelles Thema ist außerdem die Reichweite der Haftung von Suchmaschinenbetreibern als Intermediäre, die regelmäßig Gegenstand von gerichtlichen Verfahren ist und in der Literatur kontrovers diskutiert wird. Andere datenschutzrechtliche Themen im Zusammenhang mit der Nutzung von Suchmaschinen werden dagegen trotz der steigenden Bedeutung der DSGVO-Bestimmungen mit Ausnahme einzelner Aspekte kaum diskutiert.

II. Marktentwicklung

Google als marktstärkster Suchmaschinenanbieter sieht sich immer weiter gehender Regulierungsverlangen ausgesetzt. Auf diese Weise soll versucht werden, die Ausnutzung und den Ausbau der marktbeherrschenden Stellung zu unterbinden.

1. Markt für Suchmaschinen und Marktanteile

Im Markt für Suchmaschinen gibt es weiterhin keine Bewegung. Google verfügt unverändert über einen Markt-

anteil in Deutschland von knapp 95 %; der einzige echte verbliebene Konkurrent auf dem deutschen Markt ist Bing! von Microsoft mit einem Marktanteil von knapp 3 %.¹ Alle anderen Suchmaschinen, die offiziell noch angeboten werden, greifen letztlich auf die Ergebnisse von Google (T-Online, web.de, GMX, AOL) oder Bing! (Yahoo!) zurück.² Im internationalen Kontext nähern sich die Werte weiter an; Google dominiert auch hier mit einem globalen Marktanteil von 92 %, die restlichen Anteile verteilen sich weitgehend auf Bing!, Baidu (China) und Yandex (Russland).³ Zu der überwältigenden Marktmacht von Google trägt insbesondere die hohe Verbreitung auf mobilen Geräten bei. Dort liegt der Marktanteil für Deutschland bei mehr als 98 % und weltweit immer noch über 95 %.⁴

Ein Nischendasein führt weiterhin die Suchmaschine DuckDuckGo, die für sich in Anspruch nimmt, anders als die übrigen Suchmaschinen keine Informationen über die Nutzer zu sammeln.⁵ Das Motto der Suchmaschine, bei der es sich technisch um eine Kombination aus einer Meta-

* Die Autoren sind Rechtsanwälte in der Sozietät BRANDI Rechtsanwälte. Mehr über die Autoren erfahren Sie auf S. VIII. Alle zitierten Internetquellen wurden zuletzt abgerufen am 6. 3. 2020.

1 Auswertung laut Statcounters GlobalStats, abrufbar unter <https://gs.statcounter.com/search-engine-market-share/all/germany#yearly-2017-2020>.

2 Vgl. die Auswertung der Suchmaschinen unter <https://seo-summary.de/suchmaschinen/>.

3 Auswertung laut Statcounters GlobalStats, abrufbar unter <https://gs.statcounter.com/search-engine-market-share#yearly-2017-2020>.

4 Vgl. dazu die verschiedenen Auswertungen unter <https://seo-summary.de/suchmaschinen/und> <https://gs.statcounter.com/search-engine-market-share/mobile/germany/2019>.

5 Die Suchmaschine ist erreichbar unter <https://duckduckgo.com/>; vgl. dazu auch CHIP Online v. 20. 10. 2019, https://www.chip.de/news/DuckDuckGo-Sichere-Google-Alternative-auf-Rekordkurs_108191162.html und BKartA, 8. 9. 2015 – B6-126/14.