

Persönlichkeitsprofile und Datenökosysteme. Auf der Suche nach einem Rechtsgut für das Datenwirtschafts(völker)strafrecht

Sebastian Golla

I. Das neue Datenverbrechen

Für Datenschutzverstöße hat sich das Strafrecht lange Zeit kaum interessiert. Wenn überhaupt, waren eher der durch das Strafgesetzbuch fragmentarisch geschützte persönliche Lebens- und Geheimbereich oder die Daten-delikte nach den §§ 202a ff. Thema in Literatur und Rechtsprechung als das Datenschutzrecht im engeren Sinne. Dieses bezieht sich auf Risiken, die durch die Verarbeitung solcher personenbezogener Daten entstehen, welche nicht einem speziellen Geheim- oder Privatsphärenschutz zugeordnet sind.¹ Die hierauf gemünzten Straftatbestände der Datenschutzgesetze² führen auch heute noch ein Schattendasein. Nur selten bekommt es einmal ein Gericht mit diesen exotischen Regelungen zu tun.³ Geschieht dies, dann geht es tendenziell nicht um Fälle, in denen sich die komplexen Risiken moderner Datenverarbeitung realisieren oder um die Machenschaften datenmächtiger Unternehmen. Eher geht es um vergleichsweise geringfügige Verstöße aus dem Alltag – beispielsweise um das Ausspionieren von Privatpersonen mit GPS-Empfängern,⁴ das Veröffentlichen von Anschriften im Internet⁵ oder unberechtigte Abrufe aus dem Melderegister⁶.

1 Zu der Abgrenzung von Datenschutzrecht im engeren und im weiteren Sinne *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 25; *von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 17 ff.

2 § 42 BDSG und entsprechende Regelungen in den Landesdatenschutzgesetzen, welche im Wesentlichen für die öffentlichen Stellen der Länder gelten, so etwa § 34 DSG NRW, § 29 BW LDSG, § 29 BlnDSG.

3 In der Strafverfolgungsstatistik waren für das Jahr 2021 etwa 16 Verurteilungen nach § 42 BDSG ausgewiesen; Statistisches Bundesamt, Fachserie 10, Reihe 3, 2021, S. 93.

4 BGH, Urt. v. 4.6.2013 – 1 StR 32/13.

5 LG Marburg, Urt. v. 24.11.2006 – 8 Ns 2 Js 17479/04.

6 BayObLG, Besch. v. 26.10.2021 – 202 StRR 126/21.

In jüngerer Zeit lassen sich jedoch Fälle nachvollziehen, die deutlich machen, dass Verstöße gegen den Datenschutz doch ein Thema für eine vertiefte strafrechtliche Beschäftigung sein könnten. Wenn Menschen massenhaft unbefugt Daten abrufen und diese auswerten, um Einfluss auf Wahlen zu nehmen, erscheint schon die Datenverarbeitung, die diese Manipulation ermöglichen soll, in besonderem Maße missbilligenswert.⁷ Wenn Unternehmen mit datengetriebenen Geschäftsmodellen systematisch gegen Regeln des Datenschutzes verstoßen, um sich wirtschaftliche Vorteile zu verschaffen, stellt sich die Frage, ob dies nicht nur als Wettbewerbsverstoß, sondern womöglich schon als organisierte Datenkriminalität gelten sollte. Wenn staatliche Stellen moderne Überwachungstechnologien nutzen, um Bevölkerungsgruppen zu unterdrücken, provoziert dies gar die völkerstrafrechtliche Überlegung, ob es so etwas wie „Datenverbrechen gegen die Menschlichkeit“ gibt oder geben sollte.⁸

Dabei ist es kein leichtes Unterfangen, die dem Datenschutzrecht zugrunde liegenden Schutzgedanken sinnvoll mit dem System des Strafrechts zu verbinden. Der Konflikt ist vorgezeichnet: Während das Datenschutzrecht einen weiten Ansatz wählt, um auch diffuse Risiken von Datenverarbeitungen zu erfassen, hat das Strafrecht fragmentarischen Charakter und ist dem Schutz bestimmter Rechtsgüter verpflichtet. Es stellt sich daher schon grundsätzlich die Frage, ob sich das Datenschutzrecht in seiner aktuellen Konzeption, die auf dem Recht auf informationelle Selbstbestimmung fußt, eignet, zur Grundlage strafrechtlicher Regelungen gemacht zu werden. Dieser Beitrag betrachtet zunächst den Konflikt zwischen dem fragmentarischen Prinzip des strafrechtlichen Rechtsgüterschutzes und der weitreichenden Konzeption der informationellen Selbstbestimmung (II.). Darauf aufbauend untersucht er konkrete Ansätze, um beruhend auf spezifischeren Rechtsgütern neue Konzepte eines Datenschutzstrafrechts zu entwickeln (III.). Er schließt mit einem Fazit (IV.).

II. Der Schutz der informationellen Selbstbestimmung durch das Strafrecht

Das Strafrecht dient nach einer weit verbreiteten Auffassung dem Schutz von Rechtsgütern.⁹ Eine Strafvorschrift muss ein bestimmtes Rechtsgut

7 S. den Beitrag von Tobias Reinbacher in diesem Band.

8 S. den Beitrag von Caroline Böck und Matthias C. Kettemann in diesem Band.

9 Neumann/Saliger, in: NK-StGB, 6. Aufl. 2023, vor § 1 Rn. 108 m.w.N.

schützen, damit man sie auslegen und anwenden kann. Das Rechtsgut bildet auch die Grenze des zulässigen strafrechtlichen Schutzes. Wenn ein Verhalten kein geschütztes Rechtsgut beeinträchtigt, dann kann es auch nicht strafbar sein. Was genau ein Rechtsgut ist, ist im Einzelnen umstritten.¹⁰ Für die Zwecke dieses Beitrags soll es allerdings ausreichen, unter Rechtsgütern angelehnt an das Bundesverfassungsgericht elementare Werte des Gemeinschaftslebens zu verstehen.¹¹

Für das Datenschutzstrafrecht ist das Konzept des strafrechtlichen Rechtsgüterschutzes besonders interessant, weil es im Datenschutzrecht eine lebhafte Diskussion darüber gibt, was genau seine Regelungen schützen.¹² So fahnden Autoren unter anderem im Text der europäischen Datenschutzgrundverordnung nach Begriffen, die treffend beschreiben, was das Schutzgut ihres Rechtsgebietes sein könnte. Dahinter steht der Gedanke, dass Daten von der Rechtsordnung nicht selbstzweckhaft geschützt werden können. Aus Sicht des strafrechtlichen Rechtsgüterschutzes ließe sich die Frage formulieren: Welche elementaren Werte des Gemeinschaftslebens stehen dahinter, dass die Verarbeitung personenbezogener Daten grundsätzlich nicht erlaubt ist und einer Rechtsgrundlage bedarf?

Die naheliegendste Antwort auf diese Frage ist wahrscheinlich der Verweis auf die verfassungsrechtlichen Grundlagen des Datenschutzrechts. Die Regelungen der DSGVO fußen auf dem europäischen Datenschutzgrundrecht aus Art. 8 EU-Grundrechtecharta. Die deutschen Datenschutzgesetze sind von dem Recht auf informationelle Selbstbestimmung geprägt, das das Bundesverfassungsgericht vor vierzig Jahren aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) hergeleitet¹³ und seitdem zum Gegenstand zahlreicher Entscheidungen gemacht hat. Verfassungsmäßig gewährleistete Rechte lassen auf strafrechtlich schutzfähige Rechtsgüter schließen.

Doch nicht jedes verfassungsmäßig gewährleistete Recht ist auch unbedingt ein taugliches Rechtsgut, das von einem Straftatbestand geschützt werden kann. Wie sollte beispielsweise ein Straftatbestand, für den sich kein spezifischeres Rechtsgut benennen ließe als die allgemeine Hand-

10 Vgl. *Swoboda*, Die Lehre vom Rechtsgut und ihre Alternativen, ZStW 122 (2010), S. 24 ff.

11 Vgl. BVerfGE 27, 18, 29.

12 *Engeler*, Der Konflikt zwischen Datenmarkt und Datenschutz, NJW 2022, S. 3398, 3399; *Veil*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, S. 686, 690 jeweils m.w.N.

13 BVerfGE 65, 1.

lungsfreiheit (Art. 2 Abs. 1 GG), die Anforderungen des strafrechtlichen Bestimmtheitsgebotes erfüllen können? Die Grundrechte auf Datenschutz und informationelle Selbstbestimmung gehen zwar nicht so weit wie die allgemeine Handlungsfreiheit, der Umfang ihres Schutzbereiches ist aber dennoch beträchtlich. Ein Grund dafür ist, dass der Schutz von Daten dem Schutz einer Vielzahl anderer Rechte und Interessen dient. Das Bundesverfassungsgericht hat zum Recht auf informationelle Selbstbestimmung formuliert:

„[Es] flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen.“¹⁴

Diese Formulierung macht deutlich, warum das informationelle Selbstbestimmungsrecht sich in seiner reinen Gestalt kaum sinnvoll von einer Strafnorm schützen ließe. Ein Recht, das schon eingreift, bevor benennbare Rechtsgüter konkret bedroht sind, eignet sich nicht, um den Anwendungsbereich eines Straftatbestandes einzugrenzen oder als Grundlage für dessen Auslegung. Ein Tatbestand, bei dem nicht klar ist, vor welchen Bedrohungen er schützen soll, könnte kaum den Anforderungen an die gesetzliche Bestimmtheit aus Art. 103 Abs. 2 GG genügen. Er dürfte angesichts der Weite einer möglichen Strafbarkeit und der Unklarheit der verfolgten Zwecke auch kaum verhältnismäßig sein.

Die geltenden Straftatbestände der Datenschutzgesetze sind vor diesem Hintergrund kritisch zu betrachten. Sie sind akzessorisch zu den Verhaltensnormen des Datenschutzrechts. Diese Verhaltensnormen gehen davon aus, dass eine Verarbeitung personenbezogener Daten grundsätzlich rechtswidrig ist. Nur ausnahmsweise kann sie zulässig sein.¹⁵ So will das Datenschutzrecht Risiken einhegen, die aus dynamischen technologischen Entwicklungen folgen. Dieser Ansatz ist nachvollziehbar. Welche Risiken bei der Datenverarbeitung etwa heute durch den Einsatz lernfähiger Systeme entstehen, war vor fünfzig Jahren schwer absehbar. Damals wurden die Fundamente für das heutige Datenschutzrecht gelegt. Im Verwaltungsrecht und im Privatrecht mag sich mit diesem Ansatz auch sinnvoll arbeiten

14 BVerfGE 120, 274, 312.

15 Vgl. Art. 6 Abs. 1 DSGVO: „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist“.

lassen, im Strafrecht aber bereitet er Probleme. Die Straftatbestände der Datenschutzgesetze sind äußerst unbestimmt, was sie schwer anwendbar macht. Sie sind auch mit Blick auf ihre Verhältnismäßigkeit bedenklich. Die Literatur hat sich bereits mit diesen Problemen auseinandergesetzt.¹⁶ Die Regelungen bedürfen einer grundlegenden Reform.

III. Neue Ansätze für das Datenschutzstrafrecht

Es ließe sich noch viel zur Kritik des geltenden Datenschutzstrafrechts ausführen. Allerdings erscheint es an dieser Stelle vorzugswürdig, sich auf Möglichkeiten zur Fortbildung dieses Regelungsbereiches zu konzentrieren. Im Folgenden werden zwei Ansätze diskutiert, die Rechtsgüter und Regelungen des Datenschutzstrafrechts auch in Gestalt eines Daten(wirtschafts)völkerstrafrechts zu konkretisieren: Den Schutz von Persönlichkeitsprofilen (1.) und den Schutz von Datenökosystemen (2.).

Beide Ansätze gehen davon aus, dass eine grundsätzlich neue Regelung zum Datenschutzstrafrecht zu treffen ist, die an Stelle von § 42 BDSG und den entsprechenden Vorschriften in den Landesdatenschutzgesetzen treten würde und im Strafgesetzbuch zu verankern wäre. Eine Verankerung im Kernstrafrecht hätte den Vorteil, dass der Regelungsgehalt der Vorschrift sich leichter unabhängig von außerstrafrechtlichen Verhaltensnormen bestimmen ließe und sie mehr Aufmerksamkeit von Seiten der Strafjustiz und der Bevölkerung erhalten würde als die vergleichsweise schwer auffindbaren und anwendbaren geltenden Straftatbestände der Datenschutzgesetze.

1. Der Schutz von Persönlichkeitsprofilen

Der erste dieser Ansätze ist eher individualistisch geprägt: Statt grundsätzlich jede Verarbeitung personenbezogener Daten für potentiell strafrechtlich relevant zu erachten, konzentriert sich der hier vorgestellte Ansatz darauf, vor der missbräuchlichen Erstellung und Verwendung von Persönlichkeitsprofilen schützen. Konkret ließe sich eine entsprechende Strafvorschrift etwa wie folgt fassen:

16 Golla (Fn. 1), S. 226 ff.; Kubiciel/Großmann, Doxing als Testfall für das Datenschutzstrafrecht, NJW 2019, S. 1050, 1054 ff.; exemplarisch anhand der Anwendung auf den Einsatz von AirTags Leffer/Weber, Technische und strafrechtliche Implikationen des unbemerkten Einsatzes von AirTags, DuD 2022, S. 137, 140 f.

§ 207 StGB-E – Erstellen von Persönlichkeitsprofilen¹⁷

(1) Wer sich oder einem anderen unbefugt personenbezogene Daten verschafft, die nicht allgemein zugänglich und dazu geeignet sind, die Leistungen einer Person bei der Arbeit, ihre wirtschaftliche Situation, ihren Aufenthaltsort oder ihren Gesundheitszustand systematisch zu analysieren oder vorauszusagen, um sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) ¹Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält. ²Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Diese Regelung lehnt sich stark an die bisherigen Straftatbestände der Datenschutzgesetze an, schränkt aber das Tatobjekt ein. Als Persönlichkeitsprofile werden hier Sammlungen personenbezogener Daten verstanden, die dazu geeignet sind, die Leistungen einer Person bei der Arbeit, ihre wirtschaftliche Situation, ihren Aufenthaltsort oder ihren Gesundheitszustand systematisch zu analysieren oder vorauszusagen. Allgemein zugängliche Daten sind dabei ausgeschlossen. Der Begriff des Persönlichkeitsprofils steht schon seit Beginn der Datenschutzdiskussionen in den 1960er- und 1970er-Jahren für eine diffuse Sorge vor den schädlichen Folgen, die durch die Anhäufung und Kombination von Daten durch einzelne Stellen entstehen können.¹⁸ In der Regel bezeichnet er eine Sammlung von Daten, die gewisse Schlüsse auf die Lebensführung eines Menschen zulassen.¹⁹ Persönlichkeitsprofile sollen typischerweise Prognosen darüber ermögli-

17 Vorschlag aus Golla (Fn. 1), S. 235; vgl. zu der Begrenzung des Datenschutzstrafrechts anhand der Gefahr der Bildung von Persönlichkeitsprofilen auch *Haft*, Zur Situation des Datenschutzstrafrechts, NJW 1979, S. 1194, 1197; *Herb*, Verweisungsfehler im Datenschutz-Strafrecht, Eine empirische Untersuchung der Datenschutz-Kriminalität mit Reformvorschlägen, 1986, S. 206.

18 Zu der Befürchtung der Erschaffung „einer total gelenkten Welt“ *van Rienen*, Frühformen des Datenschutzes?, 1984, S. 234.

19 Vgl. mit Ansätzen zur Definition des Begriffs *Baeriswyl*, Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut, RDV 2000, S. 6, 7; *Peifer*, Persönlichkeitsrechte im 21. Jahrhundert – Systematik und Herausforderungen, JZ 2013, S. 853, 858; *Wittig*, Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, S. 59.

chen, wie sich Menschen in Zukunft verhalten werden. Solche Prognosen können Personen stark beeinträchtigen. Dies ist dann der Fall, wenn sie zur Grundlage wichtiger Entscheidungen gemacht werden – etwa über die Vergabe eines Kredits, die Einladung zu einem Bewerbungsgespräch oder den Abschluss eines Versicherungsvertrages. Werden derartige Entscheidungen auf Grundlage rechtswidriger Datenverarbeitungen vorbereitet, erscheint dies als strafwürdig. Das in § 207 StGB-E konkret gewählte Begriffsverständnis lehnt sich an den Begriff des „Profiling“ nach Erwägungsgrund 71 Satz 2 DSGVO an und soll damit auch eine internationale Anschlussfähigkeit ermöglichen.²⁰

Der Ansatz eines Profiling-Tatbestandes hat es für sich, dass er auf ein konkreteres Rechtsgut verweisen kann als das bisherige Datenschutzstrafrecht. Der Schutz vor der Erstellung von Persönlichkeitsprofilen gibt der Vorschrift eine wesentlich klarere Zielrichtung vor, als wenn sie grundsätzlich jeglichen Umgang mit personenbezogenen Daten einbeziehen würde. Zugleich kann eine derartige Regelung an eine datenschutzrechtliche Tradition anknüpfen, ohne auf weitreichende Verweisungen auf fachspezifische Regelungen angewiesen zu sein. Schließlich lässt sich bei diesem Ansatz auch der Vermögenswert von Daten für die strafrechtliche Bewertung berücksichtigen. Für ein Persönlichkeitsprofil als Sammlung von Daten, die spezifischen Anforderungen genügt, lässt sich in vielen Fällen ein konkreter Marktwert beziffern.

Freilich lassen sich gegen den Profiling-Ansatz auch Einwände vorbringen. Dass er noch stark an das informationelle Selbstbestimmungsrecht angelehnt ist, ist nicht nur ein Vorteil. Auch eine Regelung wie § 207 StGB-E bleibt tatbestandlich weit und ist in hohem Maße individualistisch geprägt. Bei der Erstellung eines Persönlichkeitsprofils geht es nach wie vor darum, dass Daten zu einer einzelnen Person zusammengetragen werden. Es fragt sich, ob sich auf diese Weise aktuelle und strafrechtlich besonders relevante Risiken von Datenverarbeitungen passgenau abbilden lassen. Gerade im Kontext eines Datenwirtschaftsvölkerstrafrechts erschiene es eher angemessen, auf systematische Datenschutzverletzungen abzustellen, die eine Vielzahl von Personen betreffen, als auf – wenn auch besonders schwerwiegende – Verletzungen von Einzelnen.

20 Zu dem Begriff im internationalen Kontext *Golla* (Fn. 1), S. 243.

2. Der Schutz von Datenökosystemen

Der zweite hier vorgestellte Ansatz ist deshalb weniger auf den Schutz von Individuen fokussiert. Er betrifft die systematische und kumulative Begehung von Datenschutzverstößen. Gerade Unternehmen der Datenwirtschaft können derartige Verstöße mit einer Vielzahl von Verletzten begehen. Was dieses Verhalten potentiell strafwürdig macht, ist nicht die Intensität der Beeinträchtigung eines Einzelnen. Es ist die systematische Verletzung des Rechts gegenüber vielen, die zu einem Geschäftsmodell wird. § 42 Abs. 1 BDSG berücksichtigt diesen Gedanken bereits ansatzweise. Er stellt es unter gewissen Umständen unter Strafe, die Daten „einer großen Zahl von Personen“ zu verarbeiten. Wann in diesem Kontext eine große Zahl von Personen vorliegt, ist aber schwer zu bestimmen.²¹ Es ist generell problematisch, schwerwiegende Datenschutzverstöße quantitativ zu bestimmen.²² Was eine „große Zahl von Personen“ ist, ist auch im Zusammenhang mit anderen Straftatbeständen umstritten²³ und erscheint bei Datenverarbeitungen besonders stark kontextabhängig.

Um den Ansatz einer Strafbarkeit systematischer und massenhafter Datenschutzverletzungen weiterzuverfolgen, müssten klarere tatbestandliche Kriterien gefunden werden, um diese einzugrenzen. Statt an den Schutz der informationellen Selbstbestimmung des Einzelnen anzuknüpfen, könnte ein derartiger Straftatbestand auf den Schutz von Datenökosystemen oder Dateninfrastrukturen²⁴ zielen. Dabei beziehen sich diese Begriffe nicht auf Umgebungen zur Datenverarbeitung im rein technischen Sinne. Unter einem Datenökosystem lässt sich eine kommunikative Umgebung verstehen, in der sich Personen frei entfalten können, ohne dem systematischen Missbrauch ihrer Daten ausgesetzt zu sein. Konkret könnte dies etwa ein soziales Netzwerk oder ein großes Online-Spiel sein. In den letzten Jahren wurden außerhalb des Strafrechts zunehmend Regelungen wie das Netzwerkdurchsetzungsgesetz oder der Digital Services Act geschaffen bzw. auf den Weg gebracht, die der wichtigen Rolle von Online-Plattformen für die Kommunikation und die Entfaltung der Persönlichkeit in einer digitalisierten Welt Rechnung tragen. Diese Gesetzgebungsakte zielen auf die Regulierung von Systemen und Geschäftsmodellen wie etwa jenen großen

21 Vgl. *Brodowski/Nowak*, in: BeckOK Datenschutzrecht, 43. Ed. 2023, § 42 Rn. 29.

22 S. den Beitrag von *Delphine Reinhardt* in diesem Band.

23 So bei § 306b Abs. 1 Var. 2 StGB (Besonders schwere Brandstiftung) und § 263 Abs. 2 Nr. 2 Var. 2 StGB (Besonders schwerer Betrug).

24 S. den Beitrag von *Sabine Müller-Mall* in diesem Band.

sozialen Netzwerken, die in der Lage sind, Menschen mit ihrer Datenmacht unterwerfen.

Tatbestandlich auf systematische oder massenhafte Datenschutzverletzungen begrenzte Strafvorschriften für den Umgang mit Daten durch die Betreiber von solchen Datenökosystemen oder durch Dritte, die von außen in diese eingreifen, könnten sich dazu eignen, die digitale Freiheitsentfaltung in diesem Bereich abzusichern. Sowohl der Anwendungsbereich als auch der Kreis der erfassten Tathandlungen wären im Vergleich zu § 42 BDSG und den entsprechenden Vorschriften der Landesdatenschutzgesetze anzupassen.

Auch dieses Modell eines Datenschutzstrafrechts als Schutz der Entfaltung in Datenökosystemen hat freilich seine Tücken. Wenn es hauptsächlich die Machenschaften von Unternehmen der Datenwirtschaft erfassen soll, stellen sich Zurechnungsfragen. Das Strafrecht kann nur natürliche Personen sanktionieren. Die Verantwortung einer einzelnen Person in einem Unternehmen für systematische Datenschutzverstöße muss erst einmal festgestellt werden. Es besteht die Gefahr, dass einer Strafbarkeit durch Verantwortungsdiffusionen entgangen wird. Unter Umständen ist das von Art. 83 DSGVO bereits etablierte Bußgeldmodell auch schon ausreichend, um gegen die Machenschaften großer Digitalunternehmen vorzugehen. Diese Sanktionen treffen Unternehmen direkt; und zumindest die Behörden einiger europäische Staaten haben bereits hohe Geldbußen gegen große Internetunternehmen verhängt. Niederlassungen großer Internetkonzerne mussten im europäischen Ausland wegen systematischer Datenschutzverstöße Summen im zwei- und dreistelligen Millionenbereich zahlen; zuletzt verhängte die irische Datenschutzbehörde sogar ein Bußgeld in Höhe von 1,2 Milliarden Euro gegen den Facebook-Konzern Meta wegen der Weitergabe von Nutzerdaten in die USA.²⁵ In Deutschland erklärte derweil das Landgericht Berlin ein Bußgeld in Höhe von etwa 14,5 Millionen Euro gegen die Deutsche Wohnen SE für unwirksam.²⁶ Ein Grund dafür war die fehlende Feststellung eines vorwerfbaren Verhaltens einer natürlichen Person in dem Bußgeldbescheid. Der Fall wirft ein Schlaglicht auf komplexe Fragen im Zusammenhang mit der Reichweite des Haftungssystems von Art. 83 DSGVO. Nach einer Vorlage des Kammergerichts²⁷ hat

25 S. www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.

26 LG Berlin, Beschl. v. 18.2.2021 – 526 OWi LG 212 Js-OWi 1/20 (1/20).

27 KG, Besch. v. 6.12.2021 – 3 Ws 250/21.

der Europäische Gerichtshof in diesem Fall mittlerweile entschieden, dass die Verhängung einer Geldbuße gegen eine juristische Person als Verantwortliche nicht der Voraussetzung unterliegt, dass festgestellt wurde, dass der Verstoß von einer identifizierten natürlichen Person begangen wurde.²⁸

IV. Fazit

Mit ihrem kleinteiligen, akzessorischen Ansatz und ihrer Stellung im Nebenstrafrecht haben die geltenden Straftatbestände der Datenschutzgesetze schlechte Chancen, einen Beitrag zu leisten, um schwerwiegenden Datenschutzverletzungen in der heutigen Zeit entgegenzuwirken. Dabei sind gerade die Gefahren des Missbrauchs der Datenmacht großer Konzerne sehr ernst. Zwar besteht bereits die Möglichkeit, hohe Bußgelder gegen Unternehmen zu verhängen. Auch das Strafrecht sollte aber besonders sozialschädliches Verhalten in diesem Bereich erfassen.

Um der Bedeutung der Materie gerecht zu werden, sollte das Datenschutzstrafrecht auch unter Berücksichtigung des geschützten Rechtsguts grundlegend überarbeitet und aktualisiert werden. Dieser Bereich sollte nicht einer Regelung im Nebenstrafrecht überlassen bleiben. Vielmehr wären eine internationale Verständigung über Regelungen zur Strafbarkeit von Datenschutzverstößen und eine Verankerung im Strafgesetzbuch wünschenswert.

Das Datenschutzrecht hat einen großen Anwendungsbereich und arbeitet mit weitgehenden Verboten. Das Strafrecht kann diese Muster nicht übernehmen. Es kann nicht allen Datenschutzverstößen Rechnung tragen und muss sich hier ganz besonders auf seine fragmentarische Natur besinnen. Eine Zuspitzung des Datenschutzstrafrechts auf systematische und schwerwiegende Verstöße könnte auch dazu beitragen, dass anstatt alltäglicher Bagatellen zunehmend gesamtgesellschaftlich relevante Fälle des Datenmissbrauchs zum Gegenstand der Strafverfolgung gemacht würden.

Systematische Datenschutzverstöße nachzuvollziehen und zu verfolgen, die durch große Unternehmen und im internationalen Kontext begangen werden, erfordert außerdem einen großen technischen und organisatorischen Aufwand. Eine strafrechtliche Regelung, die deren Unrechtsgehalt treffender zum Ausdruck bringt als der bisherige § 42 BDSG, wäre hierfür aber ebenfalls ein wichtiger Schritt.

28 EuGH, Urt. v. 5.12.2023 – C-807/21.

Durch eine klare, eigenständige Beschreibung strafwürdigen Unrechts würde das Datenschutzstrafrecht nicht nur dazu beitragen, dieses Unrecht angemessen zu ahnden. Es würde auch wichtige gesellschaftliche Anliegen verdeutlichen und damit seiner kommunikativen Funktion gerecht werden. Der Schutz vor kriminellen Profiling oder gefährlichen Eingriffen in Datenökosysteme sind zwei Beispiele für Beschreibungen dieser Anliegen, die der Strafgesetzgeber in Erwägung ziehen sollte.

