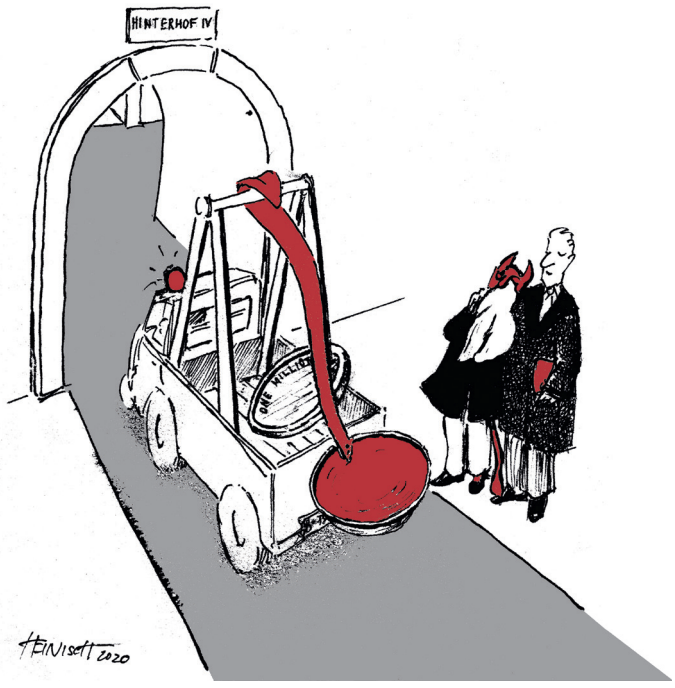
Berliner Anwaltsblatt

HEFT 9/2020 SEPTEMBER 69. JAHRGANG
HERAUSGEGEBEN VOM BERLINER ANWALTSVEREIN E.V.
www.BerlinerAnwaltsblatt.de



Abschöpfen von illegalem Vermögen

BerlinerAnwaltsVerein
ESV ERICH SCHMIDT VERLAG
03566

DAS NEUE DATENSCHUTZSTRAFRECHT – WEITERHIN EIN ZAHNLOSER TIGER?

Ist das Datenschutzstrafrecht durch die DSGVO und das BDSG-neu ein zeitgemäßes Rechtsgebiet geworden?

Karina Filusch

Seitdem die Datenschutzgrundverordnung (DSGVO) seit dem 25.5.2018 gilt, hörte man besonders eine Aussage häufig: Wer die DSGVO nicht umsetze, müsse als Konsequenz dafür bis zu 20 Millionen Euro oder 4 % seines weltweiten Umsatzes zahlen. – Klingt so, als würden Verstöße gegen das Datenschutzrecht nun härter als je zuvor bestraft. Doch was ist nach der neuen Gesetzeslage überhaupt strafbar?

VOR 20 JAHREN EIN ZAHNLOSER TIGER

Sanktionierungen gegen Datenschutzverstöße gibt es schon seit Inkrafttreten des Bundesdatenschutzgesetzes (BDSG) im Jahr 1977. Bereits 1999 konstatierte Dr. Thilo Weichert, in seiner Zeit bevor er Datenschutzbeauftragter in Schleswig-Holstein wurde (2004–2015), dass das Datenschutzstrafrecht ein zahnloser Tiger sei.[1] In einem Aufsatz besprach er ein Urteil des OLG Hamburg,[2] das über die Strafbarkeit einer Abfrage aus dem Fahrzeugregister durch einen Kriminalbeamten entschied, der für einen Bekannten, der eine Detektei betrieb, die Halterangaben zu drei Kfz-Kennzeichen abrief. Das OLG Hamburg lehnte die Strafbarkeit ab und begründete dies u. a. damit, dass es sich bei dem Fahrzeugregister um ein öffentliches Register handle und dass deshalb das Tatbestandsmerkmal „nicht offenkundige Daten" des § 43 BDSG in der damaligen Fassung nicht erfüllt worden sei. Die Daten seien offenkundig, da sie in einem öffentlichen Register aufgeführt seien, auf das private und öffentliche Stellen sowie Stellen aus dem Ausland Zugriff hätten. Das Gericht stützt sich in seiner Argumentation auf die Sphärentheorie, die bereits seit dem Volkszählungsurteil des BVerfG von 1983[3] nicht mehr angewandt werden würde. Eine derartige Auslegung des Begriffes „nicht offenkundig" würde, so Weichert, jedoch dazu führen, dass eine Vielzahl von Handlungen straffrei würde, wenn die Daten z. B. in Zeitungen, Rundfunk oder Fernsehen veröffentlich würden. Damit gäbe es praktisch kaum mehr private Daten. – Aus der Lektüre dieses Aufsatzes wird klar, dass die Anknüpfung an die Offenkundigkeit der Daten des damaligen BDSG – angesichts des damaligen Entwicklungsstandes des Internets – dieses zu keinem zeitgemäßen Gesetz machte. Gegen Ende des Aufsatzes resigniert auch Weichert und stellt fest, dass das Datenschutzstrafrecht kein Nebenstrafrecht sei, sondern sich sogar im strafrechtlichen Abseits befände.

WUCHSEN DEM TIGER SEITHER ZÄHNE?

Die Strafvorschrift enthielt noch bis 2001 das Tatbestandsmerkmal der „Daten, die nicht offenkundig sind", also jenen unbestimmten Begriff, den Weichert in seinem Aufsatz noch kritisierte. Erst 2001[4] wurde der Begriff reformiert. Das Tatbestandsmerkmal heißt seither bis heute „Daten, die nicht allgemein zugänglich sind". Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann.[5] – Heute weiß man, dass darunter keine Daten mehr aus behördlichen Registern fallen, wenn man zu deren Geltendmachung ein berechtigtes Interesse benötigt.[6]

Im Laufe der Zeit fanden auch andere Reformen statt: Die Bußgeld- und Strafvorschriften wechselten ihre Position innerhalb der §§ 41–44. Zwischen 1977 bis 2001 waren die Bußgeld- und Strafvorschriften getrennt geregelt, also ohne aufeinander zu verweisen. Bis 2001 sah die Strafvorschrift noch eine Strafschärfung vor, wenn die Tat gegen Entgelt oder mit Bereicherungsabsicht oder in Schädigungsabsicht begangen worden ist. Als ab 2001 die Bußgeldvorschriften ausgedehnt wurden, indem die Strafvorschriften in die Bußgeldvorschriften als Absatz 2 aufgenommen wurden, wurde die Strafschärfung zum Grundtatbestand der Strafvorschrift. Die Strafvorschriften waren seither deutlich kürzer und blieben unverändert bis zur Anwendbarkeit der DSGVO. Der Tatbestand wurde verwirklicht, wenn eine Ordnungswidrigkeit nach Absatz 2 (also der ehemaligen Strafvorschrift) vorsätzlich und gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht begangen wurde. Durch den nun neuen Grundtatbestand wurde der Anwendungsbereich der Strafvorschriften nun deutlich begrenzt, weil Datenschutzverstöße strafrechtlich nun nur noch geahndet werden konnten, wenn sie z. B in Bereicherungsabsicht

1 *Weichert*, NStZ 1999, 490.
2 HansOLG Hamburg, Beschluss v. 22.1.1998 – 2 Ss 105/97 – I 4/98.
3 BVerfGE 65, 1.
4 § 43 neu gef. m.W. v. 23.5.2001 durch G. v. 18.5.2001 (BGBl. I S. 904).
5 § 10 Absatz 5 Satz 2 BDSG-alt.
6 *Ehmann*, in Gola/Heckmann, BDSG-neu, § 42 Rn. 9.

begangen wurden. Gleichzeitig stieg der Strafrahmen seit Inkrafttreten von bis zu einem Jahr Freiheitsstrafe oder Geldstrafe auf bis zu zwei Jahre Freiheitsstrafe oder Geldstrafe. – Dieser Strafrahmen galt bis zur Reformierung aufgrund der DSGVO. Der heutige Strafrahmen wurde auf bis zu drei Jahre Freiheitsstrafe bei Taten nach Absatz 1 der aktuellen Strafvorschrift ausgedehnt, während für Taten nach Absatz 2 weiterhin bis zu zwei Jahre Freiheitsstrafe möglich sind. § 42 Absatz. 1 BDSG-neu regelt nun das gewerbsmäßige, wissentliche Übermitteln oder auf andere Weise Zugänglichmachen von personenbezogenen Daten, die nicht allgemein zugänglich sind, einer großen Zahl von Personen, ohne eine Berechtigung hierzu zu haben. Während § 42 Absatz 2 BDSG-neu die Verarbeitung ohne Berechtigung oder die Erschleichung von nicht allgemein zugänglichen personenbezogenen Daten durch unrichtige Angaben gegen Entgelt und in Bereicherungs- oder Schädigungsabsicht beinhaltet.

KANN DER TIGER NUN AUCH ZUBEISSEN?

Es wird deutlich: In den letzten vier Jahrzehnten hat sich allerhand getan im Datenschutzstrafrecht. Doch haben diese Veränderungen – insbesondere die Änderungen durch die DSGVO – dazu beigetragen, dass das Datenschutzstrafrecht nun ein zeitgemäßes Gesetz ist, das der aktuellen Entwicklung standhält? Hier einige Knackpunkte.

Die erste Schwierigkeit ergibt sich bereits aus der Frage, wer Adressat*in der Norm ist. Die neue Strafvorschrift ist nun im Lichte der DSGVO auszulegen, da sie ihre Daseinsberechtigung aus einer der 69 Öffnungsklauseln der DSGVO speist. Der mit „Sanktionen" übertitelte Art. 84 DSGVO ermöglicht es den Mitgliedstaaten, nämlich selbst Regelungen zu treffen. Wie die Mitgliedstaaten diese Sanktionen ausgestalten, also ob diese strafrechtlich oder verwaltungsrechtlicher Natur sind, bleibt ihnen überlassen.[7] In Deutschland entschied man sich für eine strafrechtliche Regelung in § 42 BDSG-neu. Wenn die strafrechtliche Regelung nun aber im Lichte der DSGVO gesehen werden muss, wären Adressat*innen der Norm nur verantwortliche Stellen und Auftragsverarbeiter*innen i. S. d. DSGVO. Den persönlichen Schutzbereich kann man aus Art. 3 Absatz 1 DSGVO herauslesen. Damit wäre die Strafvorschrift kein Jedermanns-Gesetz mehr, sondern könnte nur noch durch Verantwortliche und Auftragsverarbeiter*innen begangen werden.[8] Dadurch wäre der Kreis der Täter*innen sehr eng zu verstehen, was die Strafbarkeit in vielen Fällen schon an diesem Punkt ausschließen würde.

Ein weiterer Knackpunkt ist, dass die Daten, die bereits im Internet veröffentlich wurden, unter „allgemein zugängliche" Daten fallen[9] (Definition siehe oben) und somit aus dem Straftatbestand der Norm herausfallen. Dies ist vor allem problematisch bei Daten, die im Darknet[10] kursieren und später einer breiten Öffentlichkeit zugänglich gemacht werden.

Auch unklar ist noch, wie der Begriff des Zugänglichmachen durch Übermittlung oder auf andere Weise des Absatzes 1 zu verstehen ist, denn er ist in der DSGVO nicht definiert und es ist unklar, ob auf die sehr weite Begriffsbestimmung der „Verarbeitung" nach Art. 4 Nr. 2 DSGVO zurückgegriffen werden darf,[11] was wiederum zu Problemen im Bereich des im Strafrecht geltenden Bestimmtheitsgebots nach Art. 103 Absatz 2 Grundgesetz führen würde. Auch Absatz 2 weist Problemfelder auf: Danach müsste eine Verarbeitung ohne Berechtigung vorliegen, wobei dies die Verarbeitung ohne datenschutzrechtlichen Erlaubnistatbestand bedeutet, was angesichts der Unbestimmtheit des Erlaubnistatbestandes des Art. 6 DSGVO erneut ein Problem der Bestimmtheit des Tatbestandes darstellt.[12]

Und ein Problem, das die Strafvorschrift schon seit 1977 in sich birgt: Es handelt sich um ein absolutes Antragsdelikt, das bei Fehlen eines Antrags das Tätigwerden der Strafverfolgungsbehörden auch bei Vorliegen eines öffentlichen Interesses ausschließt. Immerhin kann seit der Fassung der Strafvorschrift im Jahr 2001 die/der Bundesbeauftragte für den Datenschutz Antrag stellen.

BEISS-TEST AM BEISPIEL VON DOXING UND DEEPFAKES

Angesichts der oben erläuterten Probleme stellt sich die Frage, ob Handlungen, die aus unserer modernen Internet-Gesellschaft hervorgehen, nach dem BDSG-neu überhaupt pönalisiert werden können. Ein Beispiel ist das sogenannte Doxing. Doxing setzt sich aus den Begriffen „docx" (von der Datei-Endung von Dokumenten) und „dropping" zusammen.[13] Darunter versteht man die gezielte Recherche nach personenbezogenen Daten, die dann ohne Erlaubnis im Internet veröffentlicht werden.[14] Es kann sich beispielsweise um Daten von Personen aus Politik, dem öffentlichen Leben oder von Ex-Partner*innen handeln. Die Erlangung der Daten kann sowohl legal durch die Herausgabe der betroffenen Person als auch durch Hacken erlangt werden,[15] was einen vor das oben geschilderte Problemthema Darknet stellt. Die Strafbarkeit wäre hier schon wegen der allgemeinen Zugänglichkeit der Daten abzulehnen. Aus dem Tatbestand des § 42 Absatz 1 BDSG-neu fällt das Doxing heraus, weil es in den meisten Fällen schon nicht gewerbsmäßig erfolgt.[16] Absatz 2 anzuwenden wird problematisch aufgrund der Unbestimmtheit der Tatbestandsmerkmale „Verarbeitung" und „ohne Berechtigung". Weiterhin findet Doxing meist ohne Zahlung von Entgelt und nicht in Bereicherungsabsicht statt. Einzig das Merkmal der

7 Erwägungsgrund 152 S. 2 der DSGVO.
8 Vgl. *Kubiciel/Großmann*, NJW 2019, 1050 (1053).
9 Vgl. *Ehmann*, in Gola/Heckmann, BDSG-neu, § 4, Rn. 9.
10 Vgl. *Kubiciel/Großmann*, NJW 2019, 1050 (1052).
11 Vgl. *Ehmann*, in Gola/Heckmann, BDSG-neu, § 42 Rn. 10.
12 *Ehmann*, in Gola/Heckmann, BDSG-neu, § 42 Rn. 19.
13 Ähnlich: *Kubiciel/Großmann*, NJW 2019, 1050 (1050).
14 *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Auflage 2018, 830.
15 Zitiert nach: *Kubiciel/Großmann*, NJW 2019, 1050 (1050–1051).
16 *Kubiciel/Großmann*, NJW 2019, 1050 (1055).

Schädigungsabsicht käme hier in Betracht. Die Schädigungsabsicht muss nicht vermögensmäßiger Natur sein, sondern kann auch eine Ehrverletzung und Bloßstellung gegenüber anderen oder der Öffentlichkeit darstellen.[17] – Wenn man nicht schon vorher aus der Prüfung herausfällt, könnte die Schädigungsabsicht in einigen Fällen noch bejaht werden, obwohl es den Handelnden beim Doxing nicht primär um die Schädigung der Person geht, sondern vielmehr um das Veröffentlichen bestimmter Informationen. – Eine Verurteilung wegen Doxing nach § 42 BDSG-neu wird also schwierig.

Ein anderes Problemfeld eröffnen die sogenannten Deepfakes. Deepfakes kann man kurz beschreiben als manipulierte Foto-, Video- und Audioaufnahmen, die kaum als Fälschung erkennbar sind.[18] Eine Person kann somit in eine Situation versetzt werden, in der sie Dinge sagt und tut, die sie weder gesagt noch getan hat.[19] Hier stellt sich auch das Problem, ob das Tatbestandsmerkmal der allgemein zugänglichen Daten verletzt wurde, da die Deepfakes auf öffentlich zugänglichem Bild- und Audiomaterial beruhen und oft die Schädigungsabsicht nicht das primäre Ziel ist.[20] Der Begriff der „Verarbeitung" ist wegen seiner Unbestimmtheit auch an dieser Stelle problematisch.

FAZIT: EIN TIGER MIT BEISS-SCHIENE

Die Neuregelung des § 42 BDSG-neu gegenüber der Vorgänger-Norm stellt eine Erweiterung der Handlungen dar, die nun pönalisiert werden können. Jedoch stellt die Ungewissheit über die Adressat*innen der Norm, die Unbestimmtheit der Begriffe sowie das zwingende Erfordernis, dass die Taten entweder gewerbsmäßig (Absatz 1) oder gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht (Absatz 2) begangen werden müssen, ein Hindernis für die Strafbarkeit dar. Es gibt also noch viele ungeklärte Fragen, die in den letzten zwei Jahren teils schon in Kommentierungen und Aufsätzen thematisiert wurden, aber leider noch keine Rechtsprechung, die Klarheit bringen könnte. Unser Tiger wird also noch eine Weile hungern müssen …

Karina Filusch, LL. M., Rechtsanwältin, externe Datenschutzbeauftragte und Dozentin an der HWR Berlin für die Vorlesungen Strafprozessrecht und polizeiliche Datenerhebung und -verarbeitung, www.kanzlei-filusch.de und www.datenschutzbeauftragte-berlin.eu

17 Zitiert nach: *Ehmann*, in Gola/Heckmann, BDSG-neu, § 42 Rn. 24.
18 *Lantwin*, MMR 2020, 78 (78).
19 *Boylan*, Will Deep-Fake Technology Destroy Democracy?, The New York Times, 17.10.2018, https://nyti.ms/2AeDZqv (abgerufen am 9.7.2020)
20 *Lantwin*, MMR 2020, 78 (80).