Zum Status quo des Datenschutzstrafrechts: Grenzen für Datenmacht?

Dominik Brodowski

Dieser Beitrag untersucht, ob und inwieweit der bestehende Kanon materiell-strafrechtlicher Bestimmungen ausreichend ist, um schwerwiegende systematische Datenschutzverletzungen durch staatliche und wirtschaftliche Akteure[1] zu adressieren. Hierzu wird das materielle Datenschutzkriminalstrafrecht (I.) und Datenschutzsanktionenrecht (II.) ebenso überblicksartig skizziert wie weitere Straftatbestände, die Datenschutzverletzungen miterfassen (III.). Zwar bedürfen materiell-strafrechtliche bzw. sanktionenrechtliche Regelungen bei Regime- und Wirtschaftskriminalität in besonderem Maße einem engen Zusammenspiel mit dem Prozessrecht, doch ist eine hinreichende materiell-rechtliche Grundlage notwendige Voraussetzung für eine jede Rechtsdurchsetzung. Daher werden auf Basis der lex lata Schlaglichter auf mögliche Regelungsmodelle für ein materielles Daten(völker)strafrecht geworfen (IV.).

I. Status quo des Datenschutzstrafrechts im engeren Sinne

Mit dem Inkrafttreten der DSGVO[2] am 25. Mai 2018 (Art. 99 Abs. 2 DSGVO), die als unmittelbar anwendbares Unionsrecht die datenschutzrechtlichen Rechte und Pflichten im Rahmen ihres weiten, aber nicht allumfassenden Anwendungsbereichs[3] konturiert, wurde zugleich die Rechtsdurchsetzung des Datenschutzstrafrechts umgestaltet und europäisiert: Die

1 Zur Phänomenologie *Werkmeister*, Erste Überlegungen zum Begriff der „politischen Datenwirtschaftsstraftat", GA 2021, S. 570 ff.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU Nr. L 119 v. 4.5.2016, S. 1, zuletzt ber. Abl. EU Nr. L 74 v. 4.3.2021, S. 35.

3 Zur Konturierung des sachlichen und räumlichen Anwendungsbereichs siehe Art. 2 und 3 DSGVO.

ultima ratio im Werkzeugkasten der Datenschutz-Aufsichtsbehörden ist nunmehr die Verhängung einer europäisierten Geldbuße nach Art. 83 DSGVO (näher unten II.). Zugleich haben aber einige Mitgliedstaaten, darunter Deutschland, die Möglichkeit der Öffnungsklausel in Art. 84 DSGVO genutzt[4] und halten Straftatbestände des Kriminalstrafrechts vor, um „beispielsweise bei schweren Verstößen gegen diese Verordnung […]" die Verhängung „wirksame[r], verhältnismäßige[r] und abschreckende[r] Sanktionen" (Erw.-Gr. 152 DSGVO), einschließlich Freiheitsstrafen, zu ermöglichen.

I. Licht und Schatten bei § 42 BDSG

Entgegen Kritik aus der Literatur[5] und zwischenzeitlichen rechtspolitischen Impulsen[6] befindet sich die zentrale datenschutzrechtliche Strafvorschrift unverändert im BDSG, seit der Neufassung 2018 in dessen § 42.

a. Erste Annäherung an den objektiven Grundtatbestand

Auf den ersten Blick ist der in dieser Strafvorschrift enthaltene Grundtatbestand[7] – Abs. 2 Nr. 1 – in der Tat weit gefasst und erfasst jegliches Verhalten, mit dem „personenbezogene Daten, die nicht allgemein zugänglich sind, […] verarbeitet" werden, „ohne hierzu berechtigt zu sein". Taugliches Tatobjekt sind somit „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen" (Art. 4 Nr. 1 DSGVO). Unbeschadet ihrer analogen oder digitalen Speicherform – anders als im IT-Kernstrafrecht (z.B. bei § 202a Abs. 1 StGB) – ist nicht erforderlich, dass es sich um Daten i.S.d. § 202a Abs. 2 StGB handelt. Im Hinblick auf die viel besungene „Fragmentarität" und Subsidiarität strafrechtlichen Schutzes sind jedoch allgemein zugängliche Daten ausgeklammert, also Daten, „die von jedermann zur Kenntnis genommen werden können, ohne dass der

4 Instruktiv hierzu Sydow/Marsch/*Popp*, DSGVO | BDSG, 3. Aufl. 2022, Art. 85 DSGVO Rn. 1 ff., insb. Rn. 4.

5 Statt aller *Wybitul*/*Reuling*, Umgang mit § 44 BDSG im Unternehmen: Die weitreichenden zivilrechtlichen Folgen einer unscheinbaren Strafnorm, CR 2010, S. 829, 832; *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 235 ff.

6 Zuletzt BT-Drs. 19/31115, S. 7; zuvor BT-Drs. 19/28777.

7 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 4.

Zugang zu den Daten rechtlich beschränkt ist".[8] Der Taterfolg – Verarbeitung – ist ebenfalls sehr weit gefasst und erfasst nach der Legaldefinition in Art. 4 Nr. 2 DSGVO „jeden […] Vorgang […] im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung," ja sogar „die Einschränkung, das Löschen oder die Vernichtung" solcher Daten. Letztere Trias ist zwar teleologisch zu reduzieren,[9] im Übrigen wird aber quasi jeglicher kausal und objektiv zurechenbar verursachte Umgang mit nicht allgemein zugänglichen personenbezogenen Daten erfasst. Das weitere normative Tatbestandsmerkmal[10] der fehlenden Berechtigung zeichnet wiederum die Grundkonstruktion des Datenschutzrechts – Verbot mit Eingriffsvorbehalt – strafrechtlich nach.

b. Komplikationen

Doch es ist reichlich Wasser in den Wein zu gießen:

So ist in sachlicher Hinsicht der Anwendungsbereich des § 42 BDSG gleich mehrfach begrenzt. Aufgrund seiner Lozierung in Teil 2 des BDSG ist die Vorschrift unmittelbar nur anwendbar auf Verarbeitungsvorgänge, die im von Art. 2 DSGVO vorgegebenen sachlichen Anwendungsbereich der DSGVO liegen.[11] Dabei ist weniger die Reduzierung auf „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen," (Art. 2 Abs. 1 DSGVO) das Problem, da die in diesem Sammelband thematisierten Verhaltensweisen in heutiger Zeit breitflächig Informationstechnik zur Datenakquise, -aufbereitung und -speicherung einsetzen. Ausgeklammert werden aber in Art. 2 Abs. 2 bis 4 DSGVO verschiedene Verarbeitungskontexte, insbesondere Datenverarbeitungen zum Schutz der nationalen

8 BGH NJW 2013, S. 2530, 2533 zu § 44 BDSG a.F.

9 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 46; a.A. Kühling/Buchner/*Bergt*, 3. Aufl. 2020, § 42 BDSG Rn. 32; Sydow/*Heghmanns,* § 42 BDSG Rn. 18.

10 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 36, 47; Auernhammer/*Golla,* 7. Aufl. 2020, § 42 BDSG Rn. 11.

11 Siehe hierzu oben bei und mit Fn. 3.

Sicherheit, die nicht in den Anwendungsbereich des Unionsrechts fallen (Art. 2 Abs. 2 lit. a DSGVO), die Gemeinsame Außen- und Sicherheitspolitik (Art. 2 Abs. 2 lit. b DSGVO) und der Bereich der Straftatverhütung und -verfolgung (Art. 2 Abs. 2 lit. d DSGVO). Für den letztgenannten Bereich ordnet zwar § 84 BDSG die entsprechende Geltung des § 42 BDSG an, ebenso § 85 SGB X für „Sozialdaten" im Sozialverwaltungsverfahren. Entsprechende Verweisungen fehlen aber für sonstiges nicht unionsrechtlich determiniertes Staatshandeln, insbesondere für den Bereich der Nachrichtendienste.[12] Hinzu tritt, dass die Datenverarbeitung durch öffentliche Stellen der Länder nur subsidiär durch das BDSG geregelt wird (vgl. § 1 Abs. 1 Satz 1 Nr. 2 BDSG),[13] was den Anwendungsbereich des § 42 BDSG weiter schmälert.[14]

Sodann machte man es sich etwas zu einfach, wenn man das „Wer" im Tatbestand als Kennzeichen eines Allgemeindelikts missverstehen würde:[15] Nur „Verantwortliche" i.S.d. Art. 4 Nr. 7 DSGVO sind originäre Adressaten der unionsrechtlichen Verhaltensnormen. Da die Strafvorschrift diese Maßgaben flankiert, werden durch sie lediglich diese „Verantwortlichen" adressiert,[16] d.h. nur diejenigen (natürlichen) Personen, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheide[n]". Im unternehmerischen Kontext lassen sich durch eine Anwendung der Tatbestandsergänzung des § 14 StGB (nur) die dort genannten Führungspersonen erfassen,[17] indes nur mit argumentativen Klimmzügen auch die „faktischen" Geschäftsführer*innen.[18]

Hinsichtlich des Tatobjekts – personenbezogene Daten – ist problematisch, ob auch die Deanonymisierung personenbezogener Daten erfasst wird, da Ausgangspunkt eines solchen Verarbeitungsvorgangs gerade *nicht* personenbezogene Daten zu sein scheinen. In diesem Sinne erfassen einige landesrechtliche Bestimmungen die Deanonymisierung personenbezogener

12 Zur umstrittenen Reichweite des Art. 2 Abs. 2 lit. a DSGVO siehe BeckOK-DSR/*Bäcker,* 43. Ed. 2023 Art. 2 DSGVO Rn. 7 ff. m.w.N.

13 Zu Landesdatenschutzgesetzen siehe unten I.2.

14 Zur über § 14 StGB vermittelten persönlichen Anwendbarkeit bei Unternehmen siehe sogleich bei und mit Fn. 16.

15 So wohl Kühling/Buchner/*Bergt*, 3. Aufl. 2020, § 42 BDSG Rn. 3; *Piltz*, BDSG Praxiskommentar für die Wirtschaft, 2017, § 42 BDSG Rn. 10; Sydow/*Heghmanns*, § 42 BDSG Rn. 7.

16 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 15.

17 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 16.

18 Hierzu NK-WSS/*Brodowski*, 2. Aufl. 2022, § 13 StGB Rn. 26 m.w.N.

Daten mit einem eigenständigen Verbot.[19] Indes: Wenn sich Daten deanonymisieren lassen, waren sie vorher nicht anonymisiert, sondern lediglich pseudonymisiert; um Tatobjekt des § 42 BDSG sein zu können, genügt es, „wenn die zur Identifizierung nötigen zusätzlichen Informationen zugleich Gegenstand der Tat sind und/oder dem Täter sowie dem (potenziellen) Empfänger der Informationen bekannt sind".[20]

Die fehlende Berechtigung als zentrales normatives Tatbestandsmerkmal wiederum wirft die Frage auf, wie umfassend die einzelnen datenschutzrechtlichen Kautelen durch § 42 Abs. 2 Nr. 1 BDSG abgesichert werden:[21] Führt bereits ein kleiner Fehler in der Beachtung von Formvorschriften dazu, dass eine datenschutzrechtliche Einwilligung unwirksam ist und daher auch i.S.d. § 42 Abs. 2 Nr. 1 BDSG die Berechtigung zur Verarbeitung fehlt? Führt eine unzureichende Gewährleistung der IT-Sicherheit (vgl. Art. 32 DSGVO) oder die unterbliebene Bestellung eines Datenschutzbeauftragten (vgl. Art. 37 DSGVO) dazu, dass die Berechtigung für die Datenverarbeitung entfällt? Vieles spricht insoweit zwar für eine teleologische Reduktion;[22] der Normenklarheit zuträglich ist dies aber nicht.

Ein weiteres Problemfeld des § 42 Abs. 2 Nr. 1 BDSG liegt im Erfordernis einer Bereicherungsabsicht:[23] Anders als das Betrugsstrafrecht setzt diese Strafvorschrift objektiv keinen konkreten Vermögensschaden voraus, auf den sich die Bereicherungsabsicht „stoffgleich" beziehen könnte. Das macht das Substrat der Bereicherung schwerer greifbar und führt insbesondere dazu, dass hier auch von dritter Seite für die Datenverarbeitung geleistete Honorare oder Provisionen erfasst werden – allerdings nur, soweit diese Zahlungen usw. *unmittelbar* mit der rechtswidrigen Datenverarbeitung im Zusammenhang stehen.[24]

Das Hauptproblem dürfte schließlich – neben der fehlenden Bekanntheit des § 42 BDSG in der Strafrechtspraxis – darin liegen, dass es sich bei dieser Strafvorschrift um ein absolutes Strafantragsdelikt handelt (§ 42 Abs. 3

19 Z.B. § 27 Abs. 1 Nr. 1 Alt. 7 SaarlDSG.
20 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 23.
21 *Werkmeister* (Fn. 1), S. 580.
22 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 38.1.
23 Die Alternativen der Entgeltlichkeit (als objektives Tatbestandsmerkmal) und vor allem der Schädigungsabsicht dürften für ein Daten(wirtschafts)völkerstrafrecht von geringerer Relevanz sein.
24 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 42 BDSG Rn. 51; zu § 44 BDSG a.F. instruktiv *Golla* (Fn. 5), S. 182.

BDSG):[25] Ein form- und fristgerecht gestellter Strafantrag einer antragsberechtigten Person oder Stelle – „die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde" – ist zwingende Strafverfolgungsvoraussetzung und, anders als bei relativen Strafantragsdelikten, auch nicht bei einem besonderen öffentlichen Interesse an der Strafverfolgung verzichtbar. Das ist bei Datenschutzverstößen besonders problematisch: Es handelt sich nicht selten um Summationsdelikte, von denen die einzelnen Individuen nur geringfügig betroffen sind. Daher dürfte deren individuelle Motivation zum Stellen eines Strafantrags – sofern sie von ihrer Schädigung überhaupt Kenntnis erlangen – nur gering sein.

c. Zusammenführung

Es zeigt sich somit, dass dem Grundtatbestand eine klare Fokussierung fehlt: Innerhalb seines – begrenzten – Anwendungsbereichs ist er sehr weit gefasst und erfasst, vorbehaltlich teleologischer Reduktionen, nahezu beliebige Datenschutzverstöße, soweit sie nur „nicht allgemein zugängliche personenbezogene Daten" betreffen. Das Strafantragserfordernis wiederum trägt dazu bei, dass die Strafverfolgung in diesem Bereich nur erratisch – positiv gewendet: fragmentarisch – erfolgt. Der Tatbestand ist somit keine normenklare Typisierung schweren Unrechts und damit weit von einem idealtypischen Straftatbestand entfernt.

Auch die Qualifikation in § 42 Abs. 1 BDSG teilt dieses Schicksal: Sie ist zwar enger zugeschnitten, weil sie als Tatobjekt „nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen" verlangt und nur deren wissentliche und unberechtigte Übermittlung bzw. Zugänglichmachung erfasst. Doch auch hier stellen sich dieselben Fragen der Relevanz von Verstößen gegen datenschutzrechtliche Kautelen und vor allem das Problem des Strafantragserfordernisses.

In der Konsequenz von alledem liegt es, dass § 42 BDSG in der Praxis nahezu bedeutungslos ist: 2021 gab es lediglich 19 Aburteilungen wegen dieses Deliktes, darunter 16 Verurteilungen. Die Sanktionen bewegten sich dabei im unteren bis untersten Bereich, mit sechs Verurteilungen zu bis zu 30 Tagessätzen und zehn Verurteilungen zu 31 bis 90 Tagessätzen.[26]

---

25 Weitere Kritik bei *Bergt,* DuD 2017, S. 555, 556, 561; tendenziell auch Paal/Pauly/*Frenzel,* 3. Aufl. 2021, § 42 BDSG Rn. 9, 11; *Golla* (Fn. 5), S. 213 ff.

26 Statistisches Bundesamt, Strafverfolgungsstatistik 2021, S. 92, 264 abrufbar unter www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloa

2. Landesdatenschutzgesetze am Beispiel des § 27 SaarlDSG

Ebenfalls als bloße Scheinriesen erweisen sich landesdatenschutzrechtliche Strafvorschriften wie z.B. § 27 Abs. 4 SaarlDSG – eine Vorschrift, die sich auf die „in Absatz 1 genannten Handlungen" bezieht. Dort heißt es, dass „[o]rdnungswidrig handelt, wer entgegen der [DSGVO], diesem Gesetz oder einer anderen Rechtsvorschrift zum Schutz personenbezogener Daten geschützte personenbezogene Daten, die nicht offenkundig sind, unbefugt […] verwendet […]." Damit erweckt diese Vorschrift den irrigen Eindruck, sie erfasse quasi alle Datenschutzverstöße, obgleich der Anwendungsbereich solcher Landesdatenschutzgesetze deutlich begrenzter ist als derjenige des BDSG.[27] Hinzu tritt in der konkreten Ausgestaltung das Problem, dass das Tatobjekt unbestimmt, ja unbestimmbar ist: Dem SaarlDSG ist nicht zu entnehmen, welche personenbezogenen Daten im Sinne dieser Vorschrift „geschützt", welche hingegen nicht geschützt sind.[28] Doch auch wenn § 27 SaarlDSG nicht wegen mangelnder Bestimmtheit verfassungswidrig wäre, würde die Vorschrift – wie vergleichbare weitere Landesdatenschutzgesetze – an den Problemen der fehlenden Herausarbeitung eines strafrechtlichen Unrechts und am absoluten Strafantragserfordernis leiden.

II. Status quo des Datenschutzstrafrechts im weiteren Sinne

Im weiteren Sinne als Datenschutzstrafrecht bezeichnen lässt sich das europäisierte Sanktionenrecht, das aus der Verknüpfung von Art. 83 DSGVO und § 41 BDSG resultiert und insbesondere datenverarbeitende Unternehmen mithilfe der Androhung und Verhängung erheblicher Geldbußen unmittelbar adressiert (1.). Indessen sind auch hier Beschränkungen des Anwendungsbereichs, in vielerlei Hinsicht ungeklärte Tatbestandsvoraussetzungen und vor allem defizitäre Möglichkeiten zur Rechtsdurchsetzung zu konstatieren (2.).

---

ds-Strafverfolgung-Strafvollzug/strafverfolgung-2100300217004.pdf?__blob=publicationFile.

27 Marsch/Wohlfahrt/*Brodowski*, § 27 SaarlDSG Rn. 5.

28 Marsch/Wohlfahrt/*Brodowski*, § 27 SaarlDSG Rn. 19.

1. Europäisierte Geldbußen wegen Verstößen gegen die DSGVO als Quasi-Strafrecht

Anders als die wohl meisten Harmonisierungsinstrumente der EU nutzt die DSGVO nicht primär die Regelungstechnik, die Mitgliedstaaten zu verpflichten, wirksame, abschreckende und zugleich verhältnismäßige Sanktionen für Verstöße gegen Unionsrecht vorzusehen.[29] Stattdessen enthält die DSGVO selbst – wie eine Handvoll weiterer Unionsrechtsakte – in Art. 83 die zentralen Maßgaben zu den tatbestandlichen Voraussetzungen einer Sanktion sowie zu den angedrohten Rechtsfolgen. Konkret droht Art. 83 Abs. 5 DSGVO die Verhängung von Geldbußen von bis zu 20 Mio EUR oder, bei Unternehmen, von bis zu 4 % deren Jahresumsatzes bei Verstößen (u.a.) gegen „die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9" an; bei Verstößen (u.a.) gegen „die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43" ist der Sanktionsrahmen halb so hoch (Art. 83 Abs. 4 DSGVO). In Ermangelung eines europäischen „Allgemeinen Teils" und einer Verfahrensordnung sind diese flankierenden Bestimmungen der Regelung durch den nationalen Gesetzgeber überlassen; Deutschland hat sich, mit geringen Modifikationen, für einen Generalverweis auf das OWiG entschieden (§ 41 BDSG).[30]

Mit Ausnahme der Bezeichnung – Rechtsfolge sind „Geldbußen", nicht „Geldstrafen" – handelt es sich bei dem europäisierten Datenschutz-Sanktionenrecht um Quasi-Strafrecht:[31] In garantierechtlicher Dimension ist evident, dass es sich um repressive Sanktionen von einer erheblichen Schwere handelt; *nota bene* kann in Deutschland gegen natürliche Personen maximal eine *Geldstrafe* von etwa halber Höhe (10,8 Mio EUR) verhängt werden (§ 40 Abs. 1, Abs. 2 Satz 2 StGB). Prozedural ist – zumindest in Deutschland – der Weg zu den auch in Strafsachen zuständigen Gerichten der ordentlichen Gerichtsbarkeit eröffnet, und funktional treten hier Geldbußen als Äquivalent eines neuen Regelungssystems an die Stelle einer

29 Art. 84 DSGVO sieht dies nur für „andere Sanktionen […] – insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen –" vor.

30 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 41 BDSG Rn. 3.

31 Zum Begriff *Franssen*/*Harding* (Hrsg.), Criminal and Quasi-Criminal Enforcement Mechanisms in Europe. Origins, Concepts, Future, 2022; zum hier angewendeten mehrdimensionalen Ansatz der Abgrenzung *Brodowski*, Supranationale europäische Verwaltungssanktionen: Entwicklungslinien – Dimensionen des Strafrechts – Legitimität, in Tiedemann u.a. (Hrsg.), Die Verfassung moderner Strafrechtspflege, 2016, S. 141, 154 ff.

klassischen Geldstrafe – angesichts der Höhe der Geldbußen auch mit dem klaren Ziel eines „Tadels" im Sinne einer Reputationsminderung.

2. Komplikationen

Hinsichtlich der Effektivität der Rechtsdurchsetzung wäre es indes zu kurz gegriffen, allein auf die Bußgeldstatistiken zu verweisen, die zum Teil von beeindruckenden Sanktionierungen zu berichten wissen.[32] Denn augenfällig ist eine disparate Intensität der Rechtsdurchsetzung, vor allem aber die ausgesprochen geringe Zahl an Gerichtsverfahren, in denen die zahlreichen Streitfragen zur Auslegung der Tatbestände erörtert und damit das Datenschutzsanktionenrecht weiterentwickelt werden könnten.[33] Lediglich die Frage der Anwendbarkeit der §§ 30, 130 OWiG – mit der Konsequenz, dass ein Unternehmen nur sanktioniert werden kann, wenn ein individuelles Fehlverhalten einer Leitungsperson nachgewiesen werden kann – hat der EuGH inzwischen verneint.[34] Weitere zentrale Streitfragen harren hingegen weiterhin der gerichtlichen Aufarbeitung, etwa, ob die Aufsichtsbehörden ein Verfolgungsermessen haben,[35] ob auch Führungspersonen und Mitarbeiter*innen von Unternehmen mittels §§ 9, 14 OWiG mit Geldbußen sanktioniert werden können[36] und wie die Geldbußen zu bemessen sind.[37]

---

32 Siehe hierzu den Überblick www.enforcementtracker.com.

33 Verwaltungsverfahren, die in einen Bußgeldbescheid münden, eignen sich bereits wegen der mangelnden Publizität (vgl. VG Stuttgart NVwZ 2023, S. 280) hierzu nicht.

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

35 So (u.a.) Plath/*Becker*, 2. Aufl. 2018, § 41 BDSG Rn. 4; BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 41 BDSG Rn. 41; Paal/Pauly/*Frenzel*, 3. Aufl. 2021, Art. 83 DSGVO Rn. 10 ff.; Gola/Heckmann/*Ehmann*, 3. Aufl. 2022, § 41 BDSG Rn. 14 ff.; Sydow/Marsch/*Heghmanns*, DSGVO | BDSG, 3. Aufl. 2022, § 41 BDSG Rn. 28; *Golla*, Das Opportunitätsprinzip für die Verhängung von Bußgeldern nach der DSGVO, CR 2018, S. 353; *Bülte*, Das Datenschutzbußgeldrecht als originäres Strafrecht der Europäischen Union?, StV 2017, S. 460, 463; *Martini*/*Wenzel*, „Gelbe Karte" von der Aufsichtsbehörde: die Verwarnung als datenschutzrechtliches Sanktionenhybrid, PinG 2017, S. 92, 94; a.A. *Bergt*, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, S. 555 ff.; Kühling/Buchner/*Bergt*, 3. Aufl. 2020, Art. 83 DSGVO Rn. 30 ff. sowie § 41 BDSG Rn. 19; *Albrecht*, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, S. 88, 96.

36 *Eckhardt*/*Menz*, Bußgeldsanktionen der DS-GVO, DuD 2018, S. 139, 143; Plath/*Becker*, 2. Aufl. 2018, § 41 BDSG Rn. 7; BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 41 BDSG Rn. 13; *Piltz*, BDSG Praxiskommentar für die Wirtschaft, 2017, § 43 Rn. 9; Specht/Mantz DatenschutzR-HdB/*Born*, § 8 Rn. 22; a.A. Gola/Heckmann/*Go-*

Vor allem aber zeigt sich auch in Art. 83 Abs. 4 und 5 DSGVO eine unzureichende Fokussierung: Diese Vorschrift erfasst tatbestandlich gleichermaßen leichteste Verstöße gegen Formvorschriften der Einwilligung wie schwerwiegende systematische Datenschutzverletzungen. Zwar eröffnet der weite Sanktionsrahmen Möglichkeiten der Differenzierung, doch ist diese Weite ein Störfaktor, um zielgenau gravierendes Datenschutzunrecht als solches zu adressieren. Zudem könnte die fehlende unmittelbare Inpflichtnahme der Entscheidungsträger*innen selbst – diese lässt sich allenfalls mittels §§ 9, 14 OWiG konstruieren[38] – abträglich sein, um schwersten Datenschutzverletzungen wirkungsvoll zu begegnen.

III. Strafrechtlicher Datenschutz als Rechtsreflex oder als miterfasste Rechtsverletzung anderer Straftatbestände

Ergänzend ist der Frage nachzugehen, ob weitere Straftatbestände, die unmittelbar andere Schutzrichtungen aufweisen bzw. andere Rechtsgüter zu schützen suchen, schwerwiegende systematische Datenschutzverletzungen miterfassen. Das wäre nämlich ein Argument dafür, dass ein spezifisches Daten(wirtschafts)(völker)strafrecht entbehrlich wäre.

1. Verletzung des persönlichen Lebens- und Geheimbereichs

In einem weiteren Sinne erfassen insbesondere die Vorschriften des 15. Abschnitts im Besonderen Teil des StGB (§§ 201 ff. StGB) Verhaltensweisen, die zwar nicht zwingend, aber doch häufig mit einer Verletzung der informationellen Selbstbestimmung einhergehen. So schützt das absolute Antragsdelikt (vgl. § 205 Abs. 1 Satz 1 StGB) des § 201 StGB die Vertraulichkeit des nichtöffentlich gesprochenen Wortes, indes nur in Bezug auf die Aufnahme, den Gebrauch und die Verbreitung einer Aufnahme, nicht aber die Folgenutzung der durch eine solche Vertraulichkeitsverletzung gewonnenen Erkenntnisse. Die gleiche Fokussierung auf Aufnahme, Gebrauch und Verbreitung findet sich auch in § 201a StGB hinsichtlich der Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch

la, 3. Aufl. 2022, Art. 83 DSGVO Rn. 8; Auernhammer/*Golla*, 7. Aufl. 2020, § 41 BDSG Rn. 5, 7; *Bülte*, StV 2017, S. 460, 467 f.

37 BeckOK-DSR/*Brodowski*/*Nowak*, 43. Ed. 2023, § 41 BDSG Rn. 22 m.w.N.

38 Zum diesbezüglichen Meinungsstreit siehe soeben bei und mit Fn. 36.

Bildaufnahmen. Der Schutz von Privatgeheimnissen (§ 203 StGB) erstreckt sich zwar auch auf deren Verwertung (§ 204 StGB); diese absoluten Antrags- (§ 205 Abs. 1 Satz 1 StGB) und Sonderdelikte für Berufsgeheimnisträger greifen aber nur, wenn ihnen in dieser Eigenschaft Geheimnisse oder sensible Informationen anvertraut oder sonst bekanntgeworden sind.

Die in §§ 202a ff. StGB lozierten Straftatbestände des IT-Strafrechts wiederum bezwecken einen formell ausgestalteten Schutz der Vertraulichkeit informationstechnischer Systeme und der darin gespeicherten Daten – seit 2015 auch mittels § 202d StGB vor einer weiteren Perpetuierung. Indessen ist das Schutzobjekt – Daten i.S.d. § 202a Abs. 2 StGB – formal und nicht inhaltsbezogen bestimmt; der Schutz erstreckt sich nicht nur auf sensible und vertrauliche Informationen, sondern gleichermaßen auch auf belanglose oder öffentlich bekannte Daten.[39] Den weiteren in § 202a Abs. 1 StGB enthaltenen Tatbestandsmerkmalen der Zugangssicherung und deren Überwindung hat die Rechtsprechung zwar nahezu jegliche Bedeutung genommen.[40] Da die Tatbestände des IT-Strafrechts jedoch bei einer freiwilligen Preisgabe von Informationen[41] oder bei einer andersartigen Datenerhebung (z.B. Verhaltensbeobachtung) nicht greifen und zudem der überschaubare Strafrahmen (§ 202a Abs. 1 StGB: Freiheitsstrafe bis zu drei Jahren oder Geldstrafe) nicht nach materiellen Kriterien differenziert, taugen die §§ 202a ff. StGB ebenfalls nicht dazu, schwerwiegende systematische Datenschutzverletzungen durch staatliche und wirtschaftliche Akteure zu adressieren.

39 *Brodowski*, Hacking 4.0 – Seitenkanalangriffe auf informationstechnische Systeme. Zugleich ein Beitrag zur Theorie und Dogmatik des IT-Strafrechts, ZIS 2019, S. 49, 54 f.; Schönke/Schröder/*Eisele,* 30. Aufl. 2019, § 202a Rn. 3; MK-StGB/*Graf*, 4. Aufl. 2021, § 202a Rn. 12 f.; LK/*Hilgendorf*, 13. Aufl. 2023, § 202a Rn. 7 ff.; SK/*Hoyer,* 9. Aufl. 2017, § 202a Rn. 1.

40 BGH StV-Spezial 2021, S. 136, 137 f. Rn. 18 ff., mit abl. Anm. *Hassemer*; ebenfalls kritisch *Klaas*, „White Hat Hacking" – Aufdecken von Sicherheitsschwachstellen in IT-Strukturen, MMR 2022, S. 187, 188 dort Fn. 7.

41 Schönke/Schröder/*Eisele*, 30. Aufl. 2019, § 202a Rn. 24; MK-StGB/*Graf*, 4. Aufl. 2021, § 202a Rn. 70; LK/*Hilgendorf*, 13. Aufl. 2023, § 202a Rn. 25, 38; SK/*Hoyer*, 9. Aufl. 2017, § 202a Rn. 17.

2. Weitere Straftatbestände

Auch weitere, an verschiedener Stelle lozierte Straftatbestände adressieren allenfalls punktuell Verhaltensweisen, die sich (auch) als schwerwiegende systematische Datenschutzverletzungen begreifen lassen:

Der sogenannte Feindeslisten-Tatbestand (§ 126a StGB) erfasst das Verbreiten (auch allgemein zugänglicher, arg. ex § 126a Abs. 2 StGB) personenbezogener Daten „in einer Art und Weise […], die geeignet und nach den Umständen bestimmt ist, diese Person oder eine ihr nahestehende Person der Gefahr" auszusetzen, dass diese durch ein Verbrechen oder ein Vergehen „gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert" verletzt wird.[42] Damit ist dieser Tatbestand sehr eng geführt auf die Herbeiführung einer konkreten Gefahr einer selbst – markant – strafrechtswidrigen Folgenutzung.

Der Straftatbestand der Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht (§ 353b StGB) greift materiell nur bei Geheimnissen (Abs. 1) oder geheimhaltungsbedürftigen Nachrichten oder Gegenständen (Abs. 2) und personell nur für die darin genannten Personen (Sonderdelikt); die Verletzung des Steuergeheimnisses (§ 355 StGB) ist materiell zwar weiter ausgestaltet (auch personenbezogene Daten, Abs. 1 Nr. 1, und Betriebs- oder Geschäftsgeheimnisse, Abs. 1 Nr. 2), aber personell und situativ auf Steuer(straf)verfahren eingegrenzt. Vergleichbares gilt für § 353d StGB (Verbotene Mitteilungen über Gerichtsverhandlungen). Umgekehrt ist der persönliche Anwendungsbereich bei § 23 GeschGehG zwar weit gefasst (teils Allgemeindelikt, teils Sonderdelikt), materiell ist dieser Tatbestand aber auf Geschäftsgeheimnisse begrenzt (Legaldefinition in § 2 Nr. 1 GeschGehG). Vergleichbar inhaltlich begrenzt ist § 184k StGB (Verletzung des Intimbereichs durch Bildaufnahmen). § 33 KunstUrhG ist – unabhängig von der umstrittenen Frage der Anwendbarkeit des KunstUrhG neben der DSGVO –[43] auf das Verbreiten oder öffentlich zur Schau stellen eines Bildnisses begrenzt und als absolutes Antragsdelikt ausgestaltet.

42 Zusammenfassend zu diesem Tatbestand *Korenke/Kühne*, Die Verbreitung von Feindeslisten, NK 2022, S. 457 ff.

43 Zu dieser Streitfrage BeckOK-DSR/*Stemmer*, 43. Ed. 2022, Art. 7 DSGVO Rn. 26.

IV. Regelungsmodelle für das Daten(völker)strafrecht

Für sich genommen – und auch in ihrer Summe – erfassen somit die (Straf-)Tatbestände des geltenden Rechts nicht das, was von *Geneuss* und *Werkmeister* als Daten(wirtschafts)völkerstrafrecht skizziert wurde.[44] Indes: Dieser Überblick kann Anhaltspunkte dafür liefern, welche Regelungsmodelle oder Bausteine für „Muster"-Tatbestände für ein solches Daten(wirtschafts)völkerstrafrecht zur Verfügung stehen, ohne sich zu diesem frühen Zeitpunkt bereits für oder gegen einzelne Modelle auszusprechen.

Unter Regelungsmodellen sind hierbei „logisch, systematisch und teleologisch bruchlose, gleichsam idealtypische Regelung eines typischen Sachverhalts [zu verstehen]. Strafrechtsdogmatisch gesprochen enthalten Regelungsmodelle Modelltatbestände, die im Unterschied zu den oftmals unvollkommenen Tatbeständen des positiven Rechts keine logischen, systematischen oder teleologischen Brüche aufweisen. Regelungsmodelle sind also einerseits abstrakter als positive Tatbestände des Besonderen Teils, andererseits konkreter als die im Allgemeinen Teil herausgearbeiteten ‚Deliktstypen' wie Verletzungs-, Gefährdungs-, Erfolgs- oder Tätigkeitsdelikte."[45] Solche Regelungsmodelle sind – in Ergänzung oder sogar als Ersatz für eine rechtsgutsfixierte Auslegung[46] – nicht nur Hilfsmittel zur Analyse der *lex lata*, sondern auch und vor allem für die Legistik, „für die Kriminalpolitik und die wissenschaftliche Kriminalpolitikberatung".[47]

1. Verarbeitungsstufe

Eine erste Grundentscheidung liegt darin, an welcher „Verarbeitungs-" bzw. „Nutzungsstufe" ein Daten(wirtschafts)völkerstrafrecht ansetzen soll: So verfolgt das deutsche und europäische Datenschutzrecht das Regelungsmodell, bereits früh und umfassend die Erhebung bzw. Generierung von Daten und zusätzlich deren Weiterverbreitung zu regulieren. Theoretische Alternative für ein Daten(wirtschafts)völkerstrafrecht wäre es, erst eine

44 Siehe den Beitrag von *Geneuss/Werkmeister* in diesem Band, sowie zuvor *Werkmeister* (Fn. 1), S. 570 ff.

45 *Vogel*, Wirtschaftskorruption und Strafrecht – Ein Beitrag zu Regelungsmodellen im Wirtschaftsstrafrecht, FS Weber, S. 395, 398.

46 Vgl. *Brodowski* (Fn. 39), S. 51. Zum „Rechtsgut" eines Datenwirtschaftsvölkerstrafrechts siehe *Werkmeister* (Fn. 1), S. 570 ff.

47 *Vogel* (Fn. 45), S. 398.

Weiterverarbeitung, Transformation oder sogar erst die Nutzung von Daten – personenbezogen oder nicht – zu sanktionieren, wenn dies die Autonomie menschlichen Verhaltens verletzt oder gefährdet. Dies würde zum Ausdruck bringen, dass nicht die erhobenen personenbezogenen Daten *selbst* als Mittel zur Verhaltensmodifikation genutzt werden („X hat am 14.3.2023 eine Packung Taschentücher gekauft"), sondern die aus aggregierten Daten gezogenen Schlüsse („Das Einkaufsverhalten von X deutet darauf hin, dass sie an Heuschnupfen leidet, sodass sie für personalisierte Werbung für Antiallergika empfänglich sein könnte"). Auf die Spitze getrieben wäre, bezogen auf den wirtschaftlichen Kontext, auch ein betrugsstrafrechtliches Regelungsmodell denkbar: Nicht die Datennutzung als solche wird strafrechtlich sanktioniert, sondern eine intransparente wirtschaftliche Verwertung, bei der eine Seite die Datennutzung nicht offenlegt und daher den Verletzten zu einer wirtschaftlich für diesen nachteiligen Verfügung veranlasst.

2. Tat- bzw. Schutzobjekt

Eine zweite zentrale Komponente ist das von (Modell-)Tatbeständen eines Daten(wirtschafts)völkerstrafrechts zu erfassende Tat- bzw. Schutzobjekt. Das geltende Recht weist hier eine kaum noch überschaubare Vielfalt auf:

Dies beginnt bei Daten i.S.d. § 202a Abs. 2 StGB, die jeglichen Inhalt haben können, sich aber wegen der Speicher- oder Übermittlungsform besonders leicht weiterverarbeiten lassen. Manche Tatbestände begrenzen die tauglichen Tatobjekte weiter, z.B. auf besonders zugangsgesicherte Daten (§ 202a Abs. 1 StGB) oder auf Daten rechtswidrigen Ursprungs (§ 202d Abs. 1 StGB). Das Datenschutzstrafrecht wiederum setzt bei Daten (nicht notwendigerweise i.S.d. § 202a Abs. 2 StGB) einen Personenbezug voraus, indes ohne nach besonderen Kategorien (Art. 9 Abs. 1 DSGVO) inhaltlich zu differenzieren. Zumeist aber verlangen die Tatbestände eine faktische Vertraulichkeit der Informationen („nicht allgemein zugänglich", so in § 42 BDSG, nicht aber in §§ 126a Abs. 1, 355 Abs. 1 Satz 1 Nr. 1 StGB).

Andere Tatbestände verlangen zwar keinen Personenbezug, aber eine besondere materielle Vertraulichkeit, sprich einen „geheimen" Inhalt (z.B. §§ 203, 204, 353b, 355 Abs. 1 Nr. 2 StGB; § 23 GeschGehG), wobei dies meist mit einem Anvertrauen der Information in einem besonderen Vertrauensverhältnis einhergeht (ausgesprochen deutlich in §§ 203, 204 StGB). Weitere Normen beziehen sich auf spezifische Medien (z.B. Bildaufnahmen,

§§ 184k, 201a StGB, § 33 KunstUrhG, oder Tonaufnahmen, § 201 StGB) oder auf einen besonderen Ursprung der Informationen (z.B. Wohnungen, § 201a Abs. 1 Nr. 1 StGB, oder Gerichtsakten, § 353d StGB).

Denkbar wäre es schließlich auch, auf einen wirtschaftlichen Wert – oder wirtschaftliche Nutzbarmachung – des Tatobjekts abzustellen. Ansatzweise findet sich ein solches Regelungsmodell in § 42 BDSG, soweit dieser Tatbestand ein gewerbsmäßiges Handeln (Abs. 1), ein Handeln gegen Entgelt oder in Bereicherungsabsicht (Abs. 2) voraussetzt.

3. Fehlende Berechtigung

Dritte wesentliche Stellschraube solcher (Modell-)Tatbestände ist es, die Voraussetzungen zu definieren, unter denen eine Verarbeitung und Nutzung der Daten berechtigt bzw., negativ gewendet, nicht vom Tatbestand erfasst sein soll. Dies bezieht sich zum einen auf Situationen, in denen eine Verarbeitung oder Nutzung auch gegen den Willen der betroffenen Personen erfolgen darf: Man denke etwa in strafrechtlichem Kontext an die Erhebung vertraulicher personenbezogener Daten im Wege einer Online-Durchsuchung (§ 100b StPO). Inwieweit sollen Verstöße gegen die strafprozessrechtlichen Vorschriften, etwa eine Überdehnung des Tatverdachts, dann materiell-strafrechtlich durchschlagen und zur Strafbarkeit des anordnenden Spruchkörpers bzw. der ausführenden Polizeibeamten führen?[48] Zum anderen ist angesichts der sehr detaillierten Vorgaben an die Einholung einer datenschutzrechtlichen Einwilligung einerseits, der Freigiebigkeit vieler Personen im Umgang mit ihren personenbezogenen Daten andererseits zu hinterfragen, inwieweit die klassische Einwilligungs- und Einverständnis-Dogmatik einer Modifikation bedarf: Wie weit sollen sich Aufklärungsmängel, Irrtümer und Unvorsichtigkeiten der betroffenen Personen materiell-strafrechtlich auswirken?

4. Mit-Denken der Rechtsdurchsetzung

Ein solches Denken in Regelungsmodellen und materiell-rechtlichen Stellschrauben erlaubt es schließlich, auch das Prozessrecht mitzudenken: Wel-

48 Für eine Übertragung des aus § 113 StGB bekannten „strafrechtlichen Rechtmäßigkeitsbegriffs" *Brodowski*, Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, 2016, S. 543 ff.

che Tatbestandsmerkmale lassen sich forensisch feststellen und prozessual nachweisen, welche würden den unpraktikablen Nachweis belangloser Nebensächlichkeiten erfordern, welche würden den Fokus zielgerichtet auf den Kern dessen richten, was schwerwiegende systematische Datenschutzverletzungen durch staatliche und wirtschaftliche Akteure ausmachen? Das sind (weitere) Prüffragen, an denen sich zukünftig konkrete Regelungsvorschläge eines Daten(völker)strafrechts messen lassen sollten.