

Grundlagen eines Daten(wirtschafts)völkerstrafrechts: Ein Kommentar aus strafrechtstheoretischer Sicht

Jens Puschke

I. Einleitung

Die gesellschaftlichen und rechtlichen Veränderungen, die durch den Prozess der Digitalisierung bereits entstanden und im Entstehen begriffen sind, bilden die großen Themen unserer Zeit. Dabei changiert der Diskurs zwischen Herausforderungen, Versprechungen und Gefahren dieser Entwicklungen. Bei der Bearbeitung der Gefahren bzw. hiermit im Zusammenhang stehender Missbrauchshandlungen tritt auch das Strafrecht auf den Plan. Bestimmte Datenschutzverletzungen werden pönalisiert, um sie als Unrecht zu markieren und die Wahrscheinlichkeit ihres Eintretens zu verringern. Dies wird zunehmend bedeutsam, da durch die Computerisierung der Gesellschaft Daten nicht nur einen beachtlichen wirtschaftlichen Wert haben. Ihre Nutzung kann auch massive Rückwirkungen auf betroffene Personen, Handlungen, individuelle Teilhabemöglichkeiten und schließlich die Gesellschaft als Ganzes haben. Gefahren aus fehlenden Beherrschungsmöglichkeiten oder unregulierter Verwendung sind daher stets mitzudenken. Was allerdings einem Strafrecht zum Schutz von Daten unterfällt bzw. unterfallen sollte und wie es zu legitimieren und strafrechtstheoretisch zu systematisieren ist, bleibt bisher weitgehend ungeklärt. Angesichts der grenzüberschreitenden Dimension von Verletzungen des Datenschutzes sowie des bereits in der Vergangenheit unter Beweis gestellten besonders großen Missbrauchspotenzials in diesem wirtschaftlichen, sicherheitsbezogenen und für das menschliche Zusammenleben hochrelevanten Bereich erscheint es folgerichtig, auch die Frage aufzuwerfen, ob internationale oder gar völkerstrafrechtliche Regelungen von Nöten sind.¹

Der Beitrag möchte dieser Frage auf einer grundlegenden Ebene nachspüren. Er kommentiert dabei Perspektiven, die *Sabine Müller-Mall* und *Delphine Reinhardt* in ihren Beiträgen aufgegriffen haben. *Sabine Müller-*

1 Hierzu der Beitrag von *Geneuss/Werkmeister* in diesem Band.

*Mall*² stellt die Gefahren der Digitalisierung bzw. Algorithmisierung³ auf einer sehr grundlegenden Ebene in das Zentrum ihrer Betrachtungen. Es werden die Dynamiken dieser Entwicklungen und deren Risiken für die Autonomie und Freiheit auch auf einer gesamtgesellschaftlichen Ebene hervorgehoben. Dabei werden nicht nur die Erhebung und Verarbeitung von (personenbezogenen) Daten betrachtet. Vielmehr geht es um die Verschränkung von digitaler, sozialer und physischer Welt sowie um deren smarte Gestaltung.⁴ Smarten Techniken wird dabei das Potenzial zugeschrieben, in Konkurrenz zu einer normativen Gestaltung der Welt zu treten.⁵ Sie werden als Regierungstechnik angesehen, die Freiheitsräume beschränken oder ausschließen können.

Delphine Reinhardt erläutert in ihrem Beitrag technische Seiten digitaler Überwachung und nimmt konkrete Angriffsszenarien auf Privatheit und informationelle Selbstbestimmung in den Blick.⁶ Herausgehoben wird ein individuelles Schutzinteresse, das sich durch einfache Verallgemeinerung persönlicher Betroffenheit nicht hinreichend abbilden lässt. Vielmehr stellt sich insbesondere im Zusammenhang mit Überwachung durch wirtschaftliche Akteur*innen die Frage nach einer Abwägung mit anderen Interessen, wie Komfort, Teilhabe und Sicherheit, die zum Teil von potenziellen Überwachungsunterworfenen selbst vorgenommen werden muss. Angesprochen sind somit Aspekte einer Rechtfertigung von Datenverarbeitung durch eine informierte Einwilligung, aber auch einer „Privatheitsmüdigkeit“ sowie technische und rechtliche Möglichkeiten, Datenschutzaspekte vor diesem Hintergrund zu adressieren.

Damit sind zwei Perspektiven auf die Gefahren von Digitalisierung dargelegt. Es stehen sowohl individuelle wie überindividuelle gesellschaftliche Schutzinteressen im Raum, an die es möglicherweise auch strafrechtlich heranzutreten gilt. Entsprechend stellt sich aus einer strafrechtswissenschaftlichen Sicht die Frage, in welchem Verhältnis das Strafrecht zu diesen Entwicklungen steht bzw. in der Zukunft stehen kann. Herausgearbeitet

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

3 *Müller-Mall*, Freiheit und Kalkül – Die Politik der Algorithmen, 2020, S. 10 ff.

4 *Müller-Mall*, in diesem Band, S. 37 f.

5 S. auch *Günther*, Von normativen zu smarten Ordnungen?, in Forst/Günther (Hrsg.), Normative Ordnungen, 2021, S. 523 ff.; s. konkret für sog. „Impossibility Structures“ *Rademacher*, Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JZ 2019, S. 702 ff.; grundlegend zu „Impossibility Structures“ auch *Rich*, Should We Make Crime Impossible?, Harvard Journal of Law & Public Policy (36) 2013, S. 795 ff.

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

werden sollen Grundlagen für ein (strafrechtliches) Konzept, um Gefahren im Zusammenhang mit der Digitalisierung einzudämmen. Ohne einen strafrechtstheoretisch systematisierenden Blick auf die in Rede stehenden Perspektiven lässt sich der im vorliegenden Band angelegte Anspruch eines Völkerstrafrechts als Schutzkonzept gegen schwerwiegende systematische Datenschutz(menschenrechts)verletzungen nicht einordnen und bewerten.

II. Strafrecht als Datenschutzgefahr

Ein erstes Schlaglicht soll jedoch auf Entwicklungstendenzen des Strafrechts im Allgemeinen geworfen werden. Denn dies zeigt, dass das Strafrecht aktueller Prägung in vielen Bereichen eher Teil und auch Motor der als gefährlich beschriebenen Entwicklung sein kann und Rechtfertigungen hierfür liefert. Das verwundert wenig, ist das Strafrecht als Macht-, Kontroll- und Überwachungsinstrument geradezu prädestiniert, auf zur Verfügung stehende Daten und Techniken in diesem Sinne zurückzugreifen. Das betrifft ganz basal die technische strafprozessuale Überwachung zur Sachverhaltsaufklärung, etwa wenn Telekommunikationsdaten vielzähliger Personen im Rahmen einer Funkzellenabfrage zur Standortbestimmung genutzt werden. Auch eine automatisierte Strafverfolgung durch den Einsatz von KI, etwa bzgl. Kinderpornografie, ist zu erwähnen.⁷ Dies gilt aber insbesondere vor dem Hintergrund der zunehmend präventiven Ausrichtung des Strafrechts und der Verschmelzung von Strafrecht, Kriminalprävention und Gefahrenabwehr.⁸ Das Bestreben, konformes Verhalten zu erzeugen, Risiken zu steuern und Rechtsgutsverletzungen präventiv zu unterbinden, zeigt sich des Weiteren im materiellen Strafrecht, etwa in einer Vorverlagerung der Strafbarkeit. Diese ist durch strafprozessuale Überwachungsansinnen mitinitiiert und wird flankiert durch entspre-

7 Hierzu *Gercke*, Die Entwicklung des Internetstrafrechts, ZUM 2021, S. 921, 922 ff.; vgl. den Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (sog. Chatkontrollen), Brüssel, den 11.5.2022 – COM (2022) 209 final.

8 Hierzu *Puschke*, Sicherheitsgesetzgebung ohne Zweck. Die Vorratsdatenspeicherung von Verkehrsdaten der Telekommunikation als Prototyp einer verfehlten neuartigen Sicherheitsarchitektur, in Festschrift Eisenberg, 2018, S. 695, 696 ff.

chende Befugnisse.⁹ Zusätzlich werden kriminalpräventiv Gefährdungen und sog. Gefährder*innen in den Blick genommen. Ein derartig präventiv ausgerichtetes Strafrecht und hierauf bezugnehmende Regelungssysteme sind strukturell in besonderem Maße angewiesen auf datenbasierte Prognoseinstrumente, die notwendig selektives Vorgehen steuern und auch legitimieren. Die von *Sabine Müller-Mall* dargelegte Produktion zukunftsbezogener vermeintlicher Wahrheiten¹⁰ sind ein Baustein hierzu. So lassen sich etwa terroristische Gefährdungen als Unrecht konstruieren und verbunden mit weiterer umfassender Datenerhebung und -auswertung verfolgen, bevor ein gemutmaßter Anschlag auch nur am Horizont erscheint. Gefährliche Orte und Personen werden mit dem Instrument des Predictive Policing als Bedrohung ausgemacht und angegangen.¹¹ Auf der Ebene der juristischen Entscheidung können datenbasierte Gefährlichkeitsprognosen und Vergleiche mit Entscheidungen in ähnlich gelagerten Fällen unterstützen.¹² Das Strafrecht bzw. die Strafverfolgung bedient sich selbst smarterer Techniken, die auf Big Data basieren, und rechtfertigt ihre Nutzung. Die hiermit einhergehenden Risiken der Produktion eindeutiger, kaum hinterfrag- und angreifbarer, vermeintlich wahrer Ergebnisse, die Risiken einer diskriminierenden Datennutzung und die Reduktion des Normativen zugunsten des Faktischen treffen auch die Strafverfolgung. Fernziel ist dabei die allumfassende Prädiktion, die Abweichung von Anfang an unmöglich macht.¹³ Dieser Befund weist auf eine gewisse Widersprüchlichkeit bei

9 S. etwa *Brodowski/Jahn/Schmitt-Leonardy*, Gefahrenträchtiges Gefährderrecht, GSZ 2017, S. 7, 11; *Hellfeld*, Vorbereitung einer schweren staatsgefährdenden Gewalttat, 2011, S. 175, 182; *Paeffgen*, in NK-StGB, 6. Aufl. 2023, § 89a Rn. 1 ff.; vgl. auch *Pawlik*, Der Terrorist und sein Recht, 2008, S. 33 f. sowie *Puschke*, Interventionsstrafrecht, in *Lange/Wendekamm* (Hrsg.), Die Verwaltung der Sicherheit, 2018, S. 215 ff.

10 *Müller-Mall* (Fn. 3), S. 38, 40, 42.

11 S. zum Überblick und zur Kritik *Singelstein*, Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NSTZ 2018, S. 1 ff.; eingehend zum personenbezogenen Predictive Policing *Sommerer*, Personenbezogenes Predictive Policing, 2020; zu einer Bestandsaufnahme für den deutschsprachigen Raum *Bode/Seidensticker* (Hrsg.), Predictive Policing, 2020.

12 Vgl. hierzu auch *Wisser*, Pandora's Algorithmic Black Box: The Challenges of Using Algorithmic Risk Assessments in Sentencing, *American Criminal Law Review* (56) 2019, S. 1811.

13 Hierzu etwa *Burchard*, Von der „Strafrechts“ordnung der Prädiktionsgesellschaft zur Strafrechts„ordnung“ des liberalen Rechtsstaats, in *Forst/Günther* (Hrsg.), Normative Ordnungen, 2021, S. 553 ff.; *Rademacher* (Fn. 5), S. 702 ff.; s. auch *Singelstein*, Die Sicherheit der Zukunft – Künstliche Intelligenz und soziale Kontrolle. Vom Predictive Policing zum Social Scoring, in *Festschrift Dölling*, 2023, S. 963, 964 ff.

einer Erweiterung des Strafrechts mit Blick auf grundlegende Gefahren der Digitalisierung hin, die es im Blick zu behalten gilt.¹⁴

III. Daten als Materie des (Völker)Strafrechts

Dennoch erscheint die Frage berechtigt, ob es ein Daten(wirtschafts)völkerstrafrecht braucht bzw. anhand welcher Kriterien ein solches konzipierbar erscheint. In diesem Beitrag soll die Frage der Schutzrichtung im Zentrum stehen. Die aufgezeigten Perspektiven eines individuellen sowie gesellschaftsbezogenen Schutzes sind hierfür zu konkretisieren.¹⁵ Diese können zwar ineinandergreifen, sind aber nicht in eins zu setzen.

1. Individueller Datenschutz durch das Strafrecht

Eine individuelle Ausrichtung eines Datenschutzstrafrechts soll primär personenbezogene Daten und die dahinterstehenden Rechte auf informationelle Selbstbestimmung und Privatheit schützen. Diese Schutzrichtung basiert auf Grund- und Menschenrechtsstandards, die sich aus Art. 2 Abs. 1 i.V.m. Art. 1 GG sowie Art. 8 EMRK herauslesen lassen. Ein hierauf ausgeichtetes Strafrecht kann als klassisches Datenschutzstrafrecht verstanden werden, wie es auch in Deutschland etabliert und hinsichtlich der Verhaltensnormen datenschutzrechtlich in Teilbereichen ausbuchstabiert ist. Dieses Recht ist inhaltlich europäisch durch die DSGVO geprägt und national durch die Nutzung der Öffnungsklausel des § 84 DSGVO mit Sanktionen unterlegt. Für Deutschland ist § 42 BDSG die zentrale, wenngleich in der Praxis weitgehend unbedeutende Strafvorschrift. Flankiert wird es durch eine Vielzahl weiterer Regelungen im Straf- und Ordnungswidrigkeitenrecht.¹⁶

Ziel dieses Datenschutzstrafrechts ist es, personenbezogene Daten vor unberechtigtem Zugriff und unberechtigter Verwendung zu schützen.¹⁷ Die

14 Dies kann in Anlehnung an *Kölbel*, Die dunkle Seite des Strafrechts. Eine kriminologische Erwiderung auf die Pönalisierungsbereitschaft in der strafrechtswissenschaftlichen Kriminalpolitik, NK 2019, S. 249 ff. als eine (weitere) dunkle Seite (zukünftigen) Strafrechts angesehen werden.

15 S. zu zwei Schutzrichtungen auch von *Ungern-Sternberg*, in diesem Band, S. 88 ff.

16 S. eingehend hierzu *Brodowski*, in diesem Band, S. 60 ff.

17 Zu weiteren Schutzrichtungen s. *Brodowski*, in diesem Band, S. 68 ff.

adressierten Missbrauchshandlungen erfolgen dabei vornehmlich gegen oder ohne den informierten Willen der Dateninhaber*innen. Die Schutzdimension geht jedoch über den unberechtigten Zugriff auf die Daten hinaus. Sie betrifft auch die ggf. in der Zukunft liegenden Verwendungsmöglichkeiten mit ihren Auswirkungen auf Teilhabe, Freiheit und Gleichheit und entspricht insofern der im Recht auf informationelle Selbstbestimmung enthaltenen vorgelagerten Freiheits- und Gleichheitssicherung.¹⁸ Dennoch verletzt bereits der unberechtigte Zugriff auf die Daten das auch strafrechtlich zu bestimmende Rechtsgut der informationellen Selbstbestimmung bzw. der Datensicherheit.¹⁹ Für diese dogmatische Betrachtung streitet die verfassungsgerichtliche und europarechtliche Judikatur, wonach schon die Speicherung und nicht erst die Verwendung personenbezogener Daten einen Grundrechtseingriff darstellt,²⁰ was für die strafrechtliche Rechtsgutsbestimmung und die Angriffsintensität nutzbar gemacht werden kann. Entsprechend kann die unmittelbare Schwere der Individualrechtsgutsverletzung und damit des strafrechtlichen Unrechts an der Qualität der Daten gemessen werden. Von Bedeutung ist somit, aus welcher Sphäre die Daten stammen, auf die unberechtigt zugegriffen wird. Die Nähe zum Kernbereich privater Lebensgestaltung spielt hierbei ebenso eine Rolle wie die Frage, ob es sich um Daten handelt, die Art. 9 DSGVO unterfallen.²¹ Auch die Form des Zugriffs, also etwa ob Sicherheitsvorkehrungen überwunden werden oder ob in ein Computersystem eingedrungen wird, ist beachtlich. Ebenso bestimmt der Grad fehlender Berechtigung die Schwere des Individualunrechts. Die Unrechtstiefe bemisst sich etwa danach, ob auf die Daten ohne Einwilligung zugegriffen, der Zugriff durch Täuschung erschlichen wird oder ob eine Einwilligung lediglich (formal) fehlerbehaftet ist.

Nicht zu übersehen ist allerdings, dass der im Recht der informationellen Selbstbestimmung enthaltene, abstrakt wirkende Schutz auch bei der

18 Buchheim, in Barczak (Hrsg.), BKA-Gesetz, 2023, § 9 Rn. 14; Poscher, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in Gander/Perron/Poscher et al. (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 ff.; s. auch von Ungern-Sternberg, in diesem Band, S. 89 f. mit Beispielen und Nachweisen.

19 Hierzu Zimmermann, in diesem Band, S. 141 ff.

20 EuGH, Urt. v. 8.4.2014, C-293/12, C-594/12; EuGH, Urt. v. 21.12.2016, C-203/15; C-698/15; EuGH, Urt. v. 20.9.2022, C-793/19, C-794/19 u.a.; BVerfGE 125, 260, 311; zu einer entsprechenden Rechtsgutskonzeption auch Puschke, Legitimation, Grenzen und Dogmatik von Vorbereitungstatbeständen, 2017, S. 96 ff.

21 Hierzu auch Reinbacher, in diesem Band, S. 162 f.; Zimmermann, in diesem Band, S. 151 f.

Beurteilung der Schwere des Individualrechtsgutsangriffs zu beachten ist. Insofern sind insbesondere auch die (geplanten) Verwendungszusammenhänge mit Rückwirkungen auf das Individuum zu berücksichtigen. Die massenhafte Verletzung von Individualinteressen durch die Betroffenheit einer Vielzahl von Personen²² erhält insofern auch bzgl. der Verwendungszusammenhänge Bedeutung. Können somit das Recht auf informationelle Selbstbestimmung als Rechtsgut im Strafrecht nutzbar gemacht und unterschiedliche Unrechtsdimensionen abgebildet werden, bleiben aktuelle strafrechtliche Regelungen nicht frei von Widersprüchlichkeiten und Kritik.²³ Während das Datenschutzrecht Risiken, die durch die Verarbeitung von personenbezogenen Daten entstehen, in großer Breite adressiert, bedarf es für das Strafrecht einer Fokussierung auf spezifisches Unrecht.²⁴ Ein weitgehend akzessorisches Datenschutzstrafrecht kann diese rechtsstaatlich notwendige Beschränkung nur bedingt leisten. Wann die Schwelle zur Strafwürdigkeit überschritten ist, bleibt jenseits der auch hier abstrakt vorgenommenen Gewichtungen undeutlich.

Vor diesem Hintergrund erscheint der individuelle Datenschutz auch als Materie des Völkerstrafrechts problematisch. Trotz der offenkundig grenzüberschreitenden Dimension eines solchen Datenmissbrauchs in einer vernetzten Welt könnte ein Völkerstrafrecht allenfalls in absoluten Grenzbereichen zum Einsatz kommen. Um einen universellen Geltungsanspruch eines Strafrechts, das nur bei gravierenden Grund- und Menschenrechtsverletzungen von systemischem Ausmaß greift, behaupten und für einen diskursiven Prozess in Anschlag bringen zu können, bedarf es einer Beschränkung auf schwerste Systemverbrechen und Beteiligung hieran. De lege lata dürfte ein systematischer Datenmissbrauch allenfalls dann als Materie des Völkerstrafrechts in Betracht kommen, wenn es um die hierin liegende Beteiligung an Kernverbrechen des Völkerstrafrechts geht. Hinsichtlich der Unrechtsbestimmung steht in diesen Fällen allerdings nicht das spezifisch missbräuchliche an der Datenerhebung- und -verarbeitung im Zentrum, sondern die Förderung von Völkerstraftaten, die durch andere Begehungsformen verwirklicht werden. Ob bestimmte Formen eines systematischen, menschenrechtsverletzenden Datenmissbrauchs auch als eigenständiges Delikt, insbesondere als Verbrechen gegen die Menschlichkeit i.S.d. Art. 7 Römisches Statut, gewertet werden können, erscheint demge-

22 Vgl. § 42 Abs. 1 BDSG.

23 Eingehend *Brodowski*, in diesem Band, S. 61 ff., 67 f.

24 S. auch *Golla*, in diesem Band, S. 78 f.

genüber fraglich.²⁵ Steht die Schaffung neuer Regelungen im Raum, gilt es völkerstrafrechtlich relevantes Datenmissbrauchsverhalten von sonstigen (strafrechtlich relevanten) Missbräuchen auf einer abstrakten Ebene abzugrenzen. Dies ist eine konzeptionelle Aufgabe, die durchaus herausfordernd sein kann und die sich nicht ausschließlich an Missbrauchsformen der Vergangenheit²⁶ orientieren darf. Sie muss neben der Tiefe der unmittelbaren Verletzung des Individualrechtsgutes bzw. der Individualrechtsgüter auch die (abstrakte) systemische Komponente berücksichtigen und somit einerseits wirtschaftlichen²⁷ oder staatlichen Machtmissbrauch,²⁸ andererseits aber auch potenzielle Rückwirkungen durch die Verwendung der Daten berücksichtigen. Dabei wird man auch damit konfrontiert sein, dass sich gerade die staatliche Überwachung und damit verbundene Verletzungen des Rechts auf informationelle Selbstbestimmung im oben beschriebenen Sinne legitimatorisch auf die Notwendigkeit zur Gefahrenabwehr, Strafverfolgung sowie die äußere Sicherheit stützen. Die Akzeptanz von Überwachung vor diesen Hintergründen dürfte innerhalb einer Gesellschaft und zwischen unterschiedlichen Gesellschaften erheblich divergieren. Die Übergänge von der Vorratsdatenspeicherung, den sog. Chatkontrollen, der Infiltrierung von Encrochat, der Nutzung von Pegasus, dem Vorgehen der NSA bis zur flächendeckenden Überwachung für ein Social Scoring System und einem vollständigen Ausspähen und Unterdrücken der Bevölkerung können hier durchaus fließend sein. Entsprechend sind die Maßstäbe zur (verfassungs)rechtlichen Bewertung von Privatheitsschutz und dessen Grenzen nicht einheitlich.²⁹ Zwar können Ansätze zur Beschränkung auf einen hinreichend bestimmten Unrechtskern von individuell geprägten Datenmissbräuchen nutzbar gemacht werden. So verweist etwa *Sebastian Golla* auf die Notwendigkeit des Schutzes von Persönlichkeitsprofilen und das entsprechende Begrenzungspotenzial eines solchen Zuganges.³⁰ Eine

25 Hierzu abwägend *Böck/Kettemann*, in diesem Band, S. 118 ff.

26 S. zu einer entsprechenden Kritik am Datenschutzstrafrecht auch *Kubiciel/Großmann*, Doxing als Testfall für das Datenschutzstrafrecht, NJW 2019, S. 1050, 1051.

27 Grundlegend *Zuboff*, Das Zeitalter des Überwachungskapitalismus, 2018; zu möglichen Kriterien *Reinbacher*, in diesem Band, S. 159 ff.; s. auch *Wittig*, in diesem Band, S. 172 ff.

28 S. auch *von Ungern-Sternberg*, in diesem Band, S. 92 ff.

29 Hierzu eingehend unter Analyse der Maßstäbe des Bundesverfassungsgerichts, des Europäischen Gerichtshofs und des U.S. Supreme Court *Wischmeyer*, in diesem Band, S. 133 ff.

30 *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 235; *ders.*, in diesem Band, S. 79 ff. m.w.N.; vgl. hierzu bereits *Wittig*, Die datenschutzrechtliche

derartige Konturierung eines datenschutzstrafrechtlichen Individualrechtsgutes kann sich auf national³¹ sowie international³² anerkannte Maßstäbe besonders gravierender Datenschutzverletzungen berufen. Um die Schwelle für den Einsatz des Völkerstrafrechts zu erreichen, gilt es freilich auch hier eine systemische Unrechtskomponente zu ergänzen.

Bei allen Widersprüchlichkeiten und ungeklärten Fragen eines Individualrechtsgüter schützenden Datenschutzstrafrechts erscheinen Anknüpfungspunkte für eine völkerstrafrechtliche Adressierung am Horizont. Die Herausforderung besteht darin, die Unrechtsschwere auf Basis systemischen Unrechts abstrakt, aber dennoch hinreichend konkret zu fassen.

2. Schutz von Autonomie und Freiheit als gesellschaftliche Güter

Allerdings bleibt die Frage im Raum, ob ein derartig zu beschränkendes Datenschutzstrafrecht den von *Sabine Müller-Mall* aufgezeigten besonderen (internationalen) Zukunftsherausforderungen hinreichend Rechnung tragen kann.³³ Denn gesamtgesellschaftliche Veränderungen, die sich durch Digitalisierung und Algorithmisierung ergeben können, werden von einem im Ursprung Individualrechtsgüter schützenden Strafrecht nur unzureichend erfasst. Sollen Schutzziele wie Autonomie-, Freiheits-, Teilhabe- und Gleichheitssicherung auf einer grundlegenden gesellschaftlichen Ebene strafrechtlich adressiert werden, müssten Gefahren hierfür auch im Zentrum entsprechender Normierungen stehen, wodurch Legitimationszusammenhänge und die Normenausgestaltung beeinflusst werden. Im Vordergrund stehen dann abstrakte Gefährdungen grundlegender Werte des Zusammenlebens durch Techniken der Datenverarbeitung. Dass auch eine solche Perspektive mit dem Konzept eines klassischen Datenschutzstrafrechts in unmittelbarer Verbindung steht, ist offensichtlich und wurde bereits zuvor thematisiert. Gerade die Nutzung personenbezogener Daten ermöglicht ein Mikrotargeting zur Wahlbeeinflussung, führt zur Informationsreduktion in sog. sozialen Blasen oder lässt Möglichkeiten individuel-

Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, S. 59; s. auch *Werkmeister*, Erste Überlegungen zum Begriff der „politischen Datenwirtschaftsstrafat“, GA 2021, S. 570, 582 ff.

31 BVerfGE 65, 1, 53 f.; 115, 320, 351; 120, 378, 407; 125, 260, 319 f.; 141, 220, 267; s. auch BVerfG, Urt. v. 16.2.2023, 1 BvR 1547/19, 1 BvR 2634/20.

32 Vgl. Erwägungsgrund 71 der DSGVO.

33 Ähnliche Zweifel auch bei *Golla*, in diesem Band, S. 76 ff.

ler sozialer und wirtschaftlicher Teilhabe schwinden. Entsprechend wurde festgestellt, dass die Intensität der Betroffenheit des Rechts auf informationelle Selbstbestimmung auch von den Nutzungsinteressen der Missbrauchenden und potenziellen Auswirkungen des Missbrauchs abhängt.³⁴

Jedoch sind der Personenbezug und das Handeln gegen oder ohne den Willen der Dateninhaber*innen nicht oder jedenfalls nicht allein zentral für die angesprochenen grundlegenden Gefährdungen. Von besonderer Relevanz ist vielmehr die algorithmenbasierte statistische Auswertung, die bspw. Rückschlüsse auf mutmaßliches Verhalten von Angehörigen bestimmter Personengruppen zulässt oder in Verbindung mit Anwendungen in der analogen Welt bestimmte Verhaltensweisen von Anfang an verunmöglicht. Werden zwecks Auswertung oder späterer Rückanwendung personenbezogene Daten benötigt, können diese auch mit der (formalen) Einwilligung der Dateninhaber*innen erlangt und zur Anwendung gebracht werden, ohne dass die Gefahren für Autonomie und Freiheit entfallen müssten. Gerade die Selbstbeschränkungen, mit der auch Fremdbeschränkungen einhergehen, sind ein grundlegendes Problem,³⁵ worauf auch *Delphine Reinhardt* etwa mit dem Blick auf die „Privatheitsmüdigkeit“ hingewiesen hat.³⁶ Entsprechend zeichnen sich die von *Sabine Müller-Mall* aufgezeigten Techniken der smartness gerade dadurch aus, dass ihnen Versprechungen von Nachhaltigkeit und Sicherheit unterlegt und sie damit häufig positiv konnotiert sind.³⁷ Soll vor diesem Hintergrund die Einwilligung in die Datenpreisgabe, ggf. auch im Sinne eines broad consent unter Verzicht auf umfassende Informiertheit, nicht aus einem übergeordneten Interesse heraus einschränkt werden, ist eine ausschließliche Konzeptionalisierung eines Datenstrafrechts über die Individualrechtsgüter nicht zielgenau. Auch die von *Andreas Werkmeister* vorgeschlagene Rückbeziehung auf die Menschenwürde mit kollektiver Dimension und ein diesbezügliches Vertrauen der Nutzergemeinschaft in den Datenumgang³⁸ erscheint für diese Konstellationen noch nicht vollständig ausbuchstabiert. So wird auch hier der Unrechtskern primär individuell hergeleitet, was für viele Fälle jedoch konstruiert erscheint und insoweit eine paternalistische Komponente aufweist. Selbst bei eindeutigen Verletzungen von Individualrechten aufgrund

34 S. hierzu noch einmal *Buchheim* (Fn. 18), § 9 Rn. 13 ff.; vgl. bereits unter III.1.

35 Hierzu auch *Burchard* (Fn. 13), S. 557 f.

36 *Reinhardt*, in diesem Band, S. 43.

37 S. auch *Werkmeister* (Fn. 30), S. 575 f.

38 *Werkmeister* (Fn. 30), S. 582 ff.; hierzu auch *Reinbacher*, in diesem Band, S. 165.

fehlender Einwilligung und vielzähligen Betroffenen werden die hierbei entstehenden Summationseffekte³⁹ von einem individuell abgeleiteten Unrechtsgehalt nicht vollständig abgebildet. Das Vorgehen von Cambridge Analytica⁴⁰ war nicht, jedenfalls nicht nur deswegen besonders einschneidend, weil die personenbezogenen Daten vieler Nutzer*innen täuschungsbedingt unberechtigt erlangt wurden. Entscheidend war ebenfalls die Nutzung der Daten mit dem Ziel der Wahlbeeinflussung, die auch unabhängig von einer potenziellen individuellen Betroffenheit der Dateninhaber*innen Unrechtsrelevanz haben kann.

Strafrechtliche Regelungen, die diese Unrechtskomponente abbilden sollen, müssten daher unabhängig von den Bedingungen der individuellen Datenpreisgabe ansetzen⁴¹ und die erlangten Datenbestände, ihre Verknüpfung und bereichsbezogene Nutzung erfassen. Sollen entsprechende Beeinträchtigungsmodalitäten der Schutzinteressen konkret beschrieben werden, lässt sich jedoch schnell feststellen, dass Autonomie, politische Freiheit oder Chancen sozialer Teilhabe wegen ihrer Vielschichtigkeit kaum als strafrechtliche Rechtsgüter nutzbar gemacht werden können. Zudem wird die Anwendung der in Rede stehenden Techniken und Nutzungsmodalitäten weit im Vorfeld einer unmittelbaren Beeinträchtigung dieser Schutzinteressen stattfinden, eine reale Verletzung in vielen Fälle daher nicht auszumachen sein. Insofern kommt es auf konkret zu benennendes Missbrauchsverhalten an. Was missbrauchende oder aber gewollte bzw. hinzunehmende Techniken und Vorgehensweisen sind, muss allerdings zunächst klar definiert werden. Dieser Prozess ist durchaus kleinteilig und unter Einbeziehung unterschiedlicher Interessen durchzuführen.⁴² Für den Bereich des Strafrechts müsste zudem extrahiert werden, welche Missbräuche als strafrechtliches Unrecht markiert werden können, und dies konzeptionell

39 Hierzu mit Blick auf die Ausgestaltung des § 42 BDSG als absolutes Antragsdelikt Brodowski, in diesem Band, S. 63 f.

40 Hierzu Reinbacher, in diesem Band, S. 156 ff.; Abschlussbericht des Kultur- und Medienausschusses des britischen Parlaments *House of Commons – Digital, Culture, Media and Sport Committee*, Disinformation and ‘fake news’: Final Report, S. 5, 45; hierzu auch Knorre/Müller-Peters/Wagner, Die Big-Data-Debatte, 2020, S. 20 ff.; s. auch Wylie, Mindf*ck: Cambridge Analytica and the Plot to Break America, 2019; Werkmeister (Fn. 30), S. 570 m.w.N.; Oganessian/Heermann, China: Der durchleuchtete Mensch – Das chinesische Social-Credit-System, ZD-Aktuell 2018, 06124.

41 S. zu einer entsprechenden Datenschutzkonzeption auch Poscher, Artificial Intelligence and the Right to Data Protection, MPI-CSL Working Paper 2021 (3), S. 8 f., 12.

42 S. zur allgemeinen Diskussion um den Missbrauch staatlicher Datenmacht Böck/Kettemann, in diesem Band, S. 113 ff.

aufbereitet und dem Bestimmtheitsgebot entsprechend gefasst werden. Das Strafrecht oder gar das Völkerstrafrecht unabhängig von dem weitgehend noch zu führenden politischen und außerstrafrechtlichen Diskurs um sozial-technologische Fragen an die Spitze der Gefahreneindämmung zu setzen, erscheint problematisch. Eine Umgehung oder Vorwegnahme eines solchen Diskurses durch die Etablierung abstrakter Gefährdungstatbestände, die zur Bestimmung einer Gefährlichkeit, bzw. strafrechtlich gewendet eines Unrechtgehalts, auf eine Eignung zur Autonomiebeschränkung, zur Beeinträchtigung von Verfassungsgrundsätzen und Demokratie oder zur Reduzierung sozialer Teilhabe abstellen, sind ungeeignet, einen Unrechtskern hinreichend bestimmt zu umschreiben. Für die Bereiche, etwa eines Datenwirtschaftsrechts,⁴³ in denen konsentiierte Verhaltensnormen bereits ausgemacht werden können und wonach bestimmte Techniken, wie etwa der Einsatz von algorithmischer Auswertung in bestimmten Lebensbereichen, als besonders gefährlich beurteilt werden, sind (zunächst) vor allem unternehmensbezogene Regulierungen das Mittel der Wahl.⁴⁴

IV. Zeit für ein Daten(wirtschafts)völkerstrafrecht?

Die Gefahren, die sich für Einzelne und die Gesellschaft durch die Digitalisierung und hiermit im Zusammenhang stehendem Datenmissbrauch ergeben können, sind beachtlich. Sie sind zudem grenzüberschreitend und können eine Eingriffstiefe und -breite erreichen, die nach völkerstrafrechtlicher Normierung verlangt. Die Markierung von in dieser Hinsicht relevantem Missbrauchsverhalten in der Vergangenheit, wie Cambridge Analytica, oder die Beschreibung grundlegender gesellschaftlicher Veränderungen, die erhebliche Grundrechtseinschränkungen zur Folge haben können, dienen dem zu führenden Diskurs. Eine hinreichende strafrechtstheoretische Grundlage für die Etablierung eines Datenvölkerstrafrechts enthalten sie jedoch nicht. Hierfür müssen jenseits von Einzelfällen und allgemeinen Gefahren nachvollziehbare und verallgemeinerungsfähige Maßstäbe für

43 Zu einem Datenwirtschaftsrecht eingehend Böck/Kettemann in diesem Band, S. 109 f.

44 S. hierzu etwa die sog. KI-Verordnung (Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union v. 21.4.2021, 2021/0106(COD)) oder der Digital Services Act (Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates v. 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG).

eine Normierung erarbeitet werden. Der Diskurs hierzu ist noch im Fluss und weit davon entfernt in Gesetzesform gegossen zu werden. So ist zwar der Einsatz des Strafrechts zum individuellen Datenschutz weitgehend etabliert. Neben den beschriebenen Defiziten fehlt es für eine völkerstrafrechtliche Bearbeitung jedoch an hinreichend überzeugenden Konzepten, wie eine notwendige systemische Grund- und Menschenrechtsverletzung und das sich hieraus ergebende Völkerstrafrechtsunrecht gezielt erfasst werden könnten. Demgegenüber können die grundlegenden gesellschaftlichen Gefahren eines Datenge- oder -missbrauchs für Autonomie, Freiheit, Gleichheit und Teilhabe zwar ohne Weiteres eine entsprechende Schwere aufweisen. Wo allerdings die Grenzen zwischen Missbrauch und akzeptiertem Umgang mit den Gefahren liegen, ist gesellschaftlich und außerstrafrechtlich nicht hinreichend umrissen. Zum Schließen dieser Lücken können und sollten Strafrecht und Völkerstrafrecht keine Führung beanspruchen.

An dieser Stelle ist der notwendige Diskurs um den Zuschnitt eines (völker)strafrechtlichen Unrechtskerns fortzuführen. Ansätze, welche die aufgezeigte individuelle und gesamtgesellschaftliche Perspektive zu verbinden versuchen, erscheinen dabei vielversprechend. Der strafrechtlich besser zu fassende Individualrechtsgüterschutz kann dabei als Basis eines Schutzkonzeptes fungieren. Er ist jedoch um den Schutz vor systemischen Unrechtselementen und vor gesamtgesellschaftlicher Gefährdung zu ergänzen und so auf völkerstrafrechtliches Unrecht zu beschränken. Dies mag zwar nicht alle potenziell relevanten Unrechtsdimensionen abdecken. Ein entsprechender Zugang verringert jedoch Gefahren, die von einem Pönalisierungsdiskurs für die dunklen Seiten des Strafrechts⁴⁵ ausgehen können. Denn das Strafrecht wie auch das Völkerstrafrecht sind sowohl in ihrer Anwendung als auch bzgl. der Gegenstandsauswahl hoch selektiv. Die Selektionsmechanismen basieren dabei weitgehend auf anderen Prämissen als die Beurteilung von Unrecht, Gefährlichkeit und Schädigungspotenzial. Gerade die für ein Daten(wirtschafts)völkerstrafrecht als Adressat*innen in Rede stehenden Verantwortlichen in Staaten und Unternehmen haben erheblichen Einfluss bei dem Zuschnitt der Regulierung und zudem das Potenzial, sich einem strafrechtlichen Zugriff effektiv zu entziehen.⁴⁶ Dies gilt auch für Möglichkeiten der Delegation der persönlichen strafrechtlichen

45 Kölbl (Fn. 14).

46 Ruggiero, State Crime, KrimJ 2023, S. 53 ff.

Verantwortlichkeit bzw. einer entsprechenden Verantwortungsdiffusion.⁴⁷ Angesichts der bisherigen Unschärfe datenschutzstrafrechtlicher Unrechtskonzepte gilt es zu vermeiden, dass die Diskussion um ein Daten(wirtschafts)völkerstrafrecht beim Schutz vor systematischen Datenschutz(menschenrechts)verletzungen beginnt und bei einer Intensivierung der nationalen Strafverfolgung des Hackers aus dem Kinderzimmer und der Fake News Verbreitenden politischen Extremistin endet.⁴⁸

Die wissenschaftliche Diskussion um ein Daten(wirtschafts)völkerstrafrecht hat gerade erst begonnen. Sie läuft entlang der Bestimmung adäquater Rechtsgüter, der Schwere ihrer Beeinträchtigung sowie einem dahinterstehenden systematischen Machtmissbrauch und kann so auch dazu beitragen nationales Datenschutzstrafrecht zu evaluieren. Die Zeit für eine völkerstrafrechtliche Regelung scheint aber noch nicht gekommen zu sein.

47 Vor diesem Hintergrund weist auch *Golla* auf die Vorteile eines Bußgeldmodelles hin, das sich unmittelbar an die Unternehmen richtet, in diesem Band, S. 83.

48 S. zur aktuellen Praxis der Verfolgung eher geringfügiger Verstöße aus dem Alltag *Golla*, in diesem Band, S. 75.