

Cambridge Analytica als Beispiel für eine politische Datenwirtschaftsstraftat

Tobias Reinbacher

I. Einleitung

Die Furcht vor dem gläsernen Menschen ist eine Science-Fiction-Urangst. Inzwischen sind wir davon aber gar nicht mehr so weit entfernt, insbesondere weil Unternehmen wie Alphabet oder Meta auf eine Vielzahl an persönlichen Informationen zugreifen, damit operieren und Handel treiben, ja sogar ihr Geschäftsmodell darauf ausrichten,¹ und diese Informationen mit anderen kombinieren, sodass ein sehr deutliches Bild von unserem Leben entsteht. Und das betrifft sehr viele Menschen, die vermeintlich nur von den Errungenschaften der modernen Technik profitieren. Im Fall Cambridge Analytica² hat das gleichnamige Unternehmen über eine App Daten von Millionen Nutzerinnen und Nutzern von Facebook gesammelt, um diese u.a. im US-amerikanischen Wahlkampf zum Targeting, also zur politischen Einflussnahme, zu benutzen. Der Fall war in verschiedener Hinsicht ein Weckruf.

Erstens lassen sich die Augen nun kaum noch davor verschließen, was mit unseren Daten geschehen kann, wenn wir uns in sozialen Netzwerken wie Facebook, Instagram, X etc. einloggen, v.a. wenn wir über diese Netzwerke auf andere Apps zugreifen bzw. den Zugriff erlauben. Wir können uns nicht mehr sicher sein, wer was über uns weiß, während wir wenig bis nichts über die Personen oder Institutionen wissen, die dieses Wissen im Geheimen akkumulieren.

Zweitens dürfte spätestens dadurch klar geworden sein, welchen bedeutenden Wert Daten in der Informationsgesellschaft für Tech-Unternehmen haben. Dieser Wert ist gerade auch wirtschaftlicher Natur, was es rechtfertigt, Überlegungen zur wirtschaftsstrafrechtlichen Seite des Vorgangs anzustellen.

1 Vgl. *Kubiciel*, Regulierung digitaler Plattformen und Sanktionierung von Unternehmen, FS Dannecker, 2022, S. 53, 57.

2 S. dazu noch ausführlich unter II.

Drittens hatte der Fall aber auch eine besondere politische Dimension, weil die Daten der Nutzerinnen und Nutzer zur Beeinflussung einer Wahl benutzt wurden. Insofern ist er auch im Zusammenhang mit anderen Phänomenen zu sehen, die neuerdings in sozialen Netzwerken zu beobachten sind: Desinformationskampagnen, Fake News, Social Bots, Trolling und Hate Speech, die jeweils auch auf die Einflussnahme auf Wahlen abzielen.

Die Grundbedingungen unserer Demokratie sind in Gefahr, weil der gläserne Mensch, über den eine Organisation, sei sie nun unmittelbar staatlich oder rein an wirtschaftlichen Interessen ausgerichtet, alles weiß.³ *Shoshana Zuboff* empfindet dies als „Sturz der Volkssouveränität“.⁴ Dieser gläserne Mensch ist zudem leicht durch gezielte Propaganda zu manipulieren. Die Unternehmen haben die Bedeutung der Daten erkannt, der Strafgesetzgeber u.U. noch nicht so ganz. Die Informationsgesellschaft stellt uns vor die Frage, wie die Gesellschaft aussehen soll, in der wir leben wollen, oder auch: Wo bleibt bei Big Data der (dahinterstehende) Mensch?

Mir kommt nun die Aufgabe zu, den Blick auf einen konkreten Anwendungsfall zu richten, den Fall Cambridge Analytica, und meine Gedanken zu der Frage zu äußern, welche Schlüsse daraus zu ziehen sind, insbesondere der Frage nachzugehen, inwieweit es sich dabei um den Fall einer politischen Datenwirtschaftsstrafat⁵ handelt und welche Konsequenzen sich daraus ergeben. Ich werde den Fall im Folgenden zunächst rekapitulieren (II.), dann eine Einordnung vornehmen (III.), kurz das geltende deutsche Strafrecht in dieser Hinsicht beleuchten (IV.) und schließlich Überlegungen zu einer zukünftigen Behandlung anstellen (V.).

II. Der Fall Cambridge Analytica

In den Worten von *Jimenez* und *Oleson* war der Fall Cambridge Analytica⁶ „a case that forever changed politics, media, populism, and of course, data

3 Vgl. *Zuboff*, Das Zeitalter des Überwachungskapitalismus, 2018, S. 7.

4 *Zuboff* (Fn. 3), S. 7.

5 Meine Überlegungen knüpfen insofern an den Beitrag von *Werkmeister*, Erste Überlegungen zur politischen Datenwirtschaftsstrafat, GA 2021, S. 570, an.

6 Zum Sachverhalt: U.S. Federal Trade Commission, Docket No. 9383, In the Matter of Cambridge Analytica, LLC, Opinion of the Commission; vgl. auch *Confessore*, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, New York Times v. 4.4.2018, abrufbar unter www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html; vgl. ferner *Maschewski/Nosthoff*, Der plattformökonomische

and privacy”.⁷ Das Unternehmen, das seinen Sitz in den USA hatte, machte sich ein Programm zur Persönlichkeitsanalyse zu Nutze, das ursprünglich an der Universität Cambridge, UK, entwickelt worden war. Dieses sollte es möglich machen, mittels eines Algorithmus‘ aus den Vorlieben einer Person auf Facebook anhand eines psychometrischen Modells ihre Persönlichkeit zu ermitteln. So sollten etwa *Likes* bestimmter Serien, Lieder oder Politiker wie *George W. Bush* auf ein konservatives Weltbild hindeuten. Die Entwickler meinten, ihr Algorithmus habe das Potential, die Persönlichkeit besser vorherzusagen als Arbeitskollegen, Freunde oder gar Familienmitglieder. Das Unternehmen Cambridge Analytica interessierte sich sehr für dieses Tool, da es selbst für politische Parteien Dienste wie das Erstellen von Wählerprofilen und Wahlwerbung inklusive Micro-Targeting, also das gezielte Ansprechen von potenziellen Wählerinnen und Wählern, anbot. Tatsächlich gelang es Cambridge Analytica, einen der beteiligten Wissenschaftler für eine kommerzielle Zusammenarbeit zu gewinnen. Er hatte die App *Thisisyourdigitallife* entwickelt, die auf Facebook installiert werden und dadurch auf die Daten der Nutzerinnen und Nutzer zugreifen konnte. Facebook selbst erlaubte seinerzeit Drittanbietern, deren Apps über Facebook benutzt wurden, nicht nur auf die Daten derjenigen zuzugreifen, die das Programm installiert hatten, sondern auch auf die Daten von deren Facebook-Freundinnen und -Freunden.

Die App *Thisisyourdigitallife* enthielt vordergründig eine Umfrage, bei der die Teilnehmenden gegen eine geringe Geldsumme freiwillig an einem Persönlichkeitstest mitwirken und Fragen beantworten konnten. Sie wurden gefragt, ob die App auf einige ihrer Daten auf Facebook zugreifen dürfe, wobei ihnen jedoch versichert wurde, dass keine Informationen gesammelt würden, die eine Identifizierung ermöglichen, wie etwa Name oder User ID. Tatsächlich sammelte die App von den Teilnehmenden aber Facebook User ID, Geschlecht, Geburtstag, Wohnort, ihre gesamte Freundesliste sowie ihre *Likes* von Facebook-Seiten. Auch von ihren Freundinnen und Freunden, die selbst an der Umfrage gar nicht teilgenommen hatten, sammelte die App Facebook User ID, Namen, Geschlecht, Geburtstag, Wohnort und *Likes*. Dabei waren ca. 250.000-270.000 Nutzerinnen und Nutzer der App sowie ca. 50-65 Millionen Freundinnen und Freunde be-

Infrastrukturwandel der Öffentlichkeit: Facebook und Cambridge Analytica revisited, Leviathan, Sonderband 37/2021, S. 320; *Werkmeister* (Fn. 5), S. 576.

7 *Jimenez/Oleson*, The Crimes of Digital Capitalism, *Mitchell Hamline Law Review* 48 (2022), S. 971, 1000.

troffen,⁸ es ist sogar die Rede von bis zu 87 Millionen Profilen,⁹ darunter ca. 30 Millionen identifizierbare US-Bürgerinnen und Bürger.¹⁰

Die so entstandene Datenbank und das Analyse-Tool ermöglichten es, Wählerprofile zu erstellen und im Sinne der Kampagne von *Ted Cruz* bzw. später auch von *Donald Trump*, für die Cambridge Analytica arbeitete, auf die Betroffenen mittels Micro-Targeting durch private Nachrichten und Inhalte, die ihnen angezeigt wurden, gezielt Einfluss zu nehmen. Ob und inwieweit die Wahl dadurch tatsächlich entschieden wurde, wie es die Inhaber des Unternehmens selbst behaupteten,¹¹ lässt sich im Nachhinein nicht genau sagen.¹² Dies gilt auch für einen möglichen Einfluss auf die *Leave*-Kampagne im Rahmen des *Brexit*-Referendums,¹³ für die es ebenfalls arbeitete. Der politische Schaden einerseits sowie der Vertrauensbruch und die Verletzung der Persönlichkeitsrechte der Betroffenen andererseits waren jedoch enorm.

III. Einordnung

Der Vorgang hat ein großes mediales Echo ausgelöst. *Mark Zuckerberg* wurde zu mehreren Anhörungen geladen.¹⁴ Für das Meta-Unternehmen war es nicht der einzige Daten-Skandal,¹⁵ aber auch andere Tech-Konzerne

8 U.S. Federal Trade Commission, Docket No. 9383, In the Matter of Cambridge Analytica, LLC, Opinion of the Commission, S. 7.

9 *Confessore*, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, *New York Times* v. 4.4.2018, abrufbar unter www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html; *Jimenez/Oleson* (Fn. 7), S. 1001; *Maschewski/Nosthoff* (Fn. 6), S. 322.

10 U.S. Federal Trade Commission, Docket No. 9383, In the Matter of Cambridge Analytica, LLC, Opinion of the Commission, S. 7.

11 Vgl. *Nix*, www.youtube.com/watch?v=n8Dd5aVXLCc.

12 *K.-S. Trump*, Four and a half reasons not to worry that Cambridge Analytica skewed the 2016 election, *Washington Post* v. 23.3.2018, www.washingtonpost.com/news/mon-key-cage/wp/2018/03/23/four-and-a-half-reasons-not-to-worry-that-cambridge-analytica-skewed-the-2016-election.

13 BBC News v. 7.10.2020, www.bbc.com/news/uk-politics-54457407.

14 *Confessore*, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, *New York Times* v. 4.4.2018, abrufbar unter www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

15 Vgl. *Jimenez/Oleson* (Fn. 7), S. 997 ff.

der sog. *Big Five*¹⁶ sind in dieser Hinsicht nicht unbescholten.¹⁷ Denken wir nur an die NSA-Affäre, über die hier schon berichtet wurde.¹⁸ Nun zur Einordnung als politische Wirtschaftsstraftat.

1. Warum Wirtschaftsstraftat?

Die meisten der gängigen Kriterien zur Einordnung als Wirtschaftsstraftat¹⁹ passen beim Datenskandal um Cambridge Analytica. Zwar finden sich Datenstraftaten (noch) nicht in § 74c GVG. Wir können jedoch von *White Collar* und *Corporate Crimes*²⁰ sprechen und einen hohen Schaden bei den betroffenen Nutzerinnen und Nutzern konstatieren, wobei es weniger um materielle Schäden, sondern um besonders hohe immaterielle Schäden geht, nämlich um eine systematische Verletzung von Grund- und Menschenrechten durch die Unternehmen.²¹ Das Wirtschaftsstrafrecht zielt auf den Schutz überindividueller Rechtsgüter.²² Es muss auch für eine Wirtschaft gelten, deren Handelsgut persönliche Informationen sind. Auf diese Informationen gerichtete Straftaten können ein kollektives Rechtsgut angreifen, nämlich den Datenschutz insgesamt bzw. die Persönlichkeitsrechte der Betroffenen, im Falle der systematischen Erstellung umfassender Persönlichkeitsprofile sogar die Menschenwürde der Marktteilnehmerinnen und Marktteilnehmer,²³ und damit die (mensenrechtlichen) Grundbedingungen der digitalen Marktwirtschaft. Zwar zielt diese gerade auf den

16 Gemeint sind Amazon, Apple, Google, Meta und Microsoft; s. zu Unterschieden in ihrer Einordnung als „überwachungskapitalistische“ Unternehmen i.H.a. Geschäftspraktiken sowie Ausrichtung des Unternehmens aber auch *Zuboff* (Fn. 3), S. 38 ff., die sich letztlich auf Google, Facebook (Meta) und Microsoft konzentriert.

17 Vgl. *Jimenez/Oleson* (Fn. 7), S. 1013 ff.

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

19 Vgl. dazu etwa *Kudlich/Oğlakcioğlu*, Wirtschaftsstrafrecht, 3. Aufl. 2020, Rn. 1 ff.; *Tiedemann*, Wirtschaftsstrafrecht, 5. Aufl. 2017, § 1 Rn. 72 ff.; *Wittig*, Wirtschaftsstrafrecht, 6. Aufl. 2023, § 2 Rn. 5 ff.

20 So etwa *Jimenez/Oleson* (Fn. 7), S. 1013 ff.

21 *Jimenez/Oleson* (Fn. 7), S. 1014 f.

22 *Otto*, Konzeption und Grundsätze des Wirtschaftsstrafrechts, ZStW 96 (1984), S. 339, 342; *Tiedemann*, Wirtschaftsstrafrecht, 5. Aufl. 2017, § 1 Rn. 81.

23 BVerfGE 27, 1, 6: Mit der Menschenwürde nicht zu vereinbaren, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“; BVerfGE 65, 1, 53: umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlich-

Handel mit Daten ab. Wenn aber auch die letzte Information nicht mehr sicher ist, dann werden diese Grundbedingungen einer menschenrechtskonformen Marktwirtschaft beseitigt. Zumindest diese gilt es im Zeitalter des sog. „Überwachungskapitalismus“²⁴, oder auch: des Informationskapitalismus, dessen Kapital die Information ist, zu sichern.

Die Verletzung des allgemeinen Vertrauens in die Wirtschaftsordnung macht das Wesen der Wirtschaftskriminalität aus.²⁵ In unserem Fall geht es um eine Verletzung des Vertrauens in eine grund- und menschenrechtskonforme Marktwirtschaft. Der Einzelne muss zumindest darauf vertrauen können, dass gewisse Grundbedingungen im Markt eingehalten werden. Nun mag man einwenden, ein solches Vertrauen in die Sicherheit der Daten sei ohnehin nicht schützenswert, weil es gar kein entsprechendes Interesse der Nutzerinnen und Nutzer sozialer Medien gebe, weil sie doch heutzutage ihre Daten ganz bereitwillig hergäben. Datenschutz sei, so könnte man meinen, den jüngeren Generationen gar nicht so wichtig. Der Fall Cambridge Analytica hat aber doch etwas anderes gezeigt: Es mag den Betroffenen schlicht am Bewusstsein fehlen, was gerade mit ihren Daten geschieht.

2. Warum politisch?

Kann man auch von einer politischen Wirtschaftsstraftat sprechen? Im Fall Cambridge Analytica wurden zwar keine staatlich gesteuerten Taten begangen. Es bestand jedoch ein recht klarer Bezug zur Politik, da die Daten an Institutionen, die für Parteien bzw. politische Kampagnen arbeiteten, weitergegeben und im Wahl- und Meinungskampf verwendet wurden. Die jeweils unterstützten Kampagnen sollten auf diese Weise einen Vorsprung erlangen. Unabhängig von diesem Fall liegt das politische Problem bei den sozialen Medien insbesondere in der Kontrolle des *free flow of information*, weil mittels Algorithmen nicht nur Werbung gezielt eingesetzt wird, sondern auch Informationen in demokratiegefährdender Weise selektiert

keitsprofilen der Bürger unzulässig; BVerfGE 109, 279, 323: Menschenwürde durch Persönlichkeitsprofil verletzt.

24 Zuboff (Fn. 3).

25 Otto (Fn. 22), S. 342.

werden.²⁶ Gerade dies hat das Potenzial für einen enormen politischen Einfluss, der in der Hand der Betreiber dieser Netzwerke liegt.

Vorgänge, in denen großflächige Datenschutzverstöße vorliegen, müssen aber nicht unbedingt einen unmittelbaren Politikbezug aufweisen, um sie als politische Wirtschaftsstraftaten zu bezeichnen. Auch bei der kommerziellen Nutzung der Daten kann mit *Naucke* eine politische Dimension des Vorgangs anzunehmen sein, staatlich veranlasst oder auch in Form staatlich nicht beherrschter (oder beherrschbarer) Macht.²⁷ Er hat in seiner Analyse der politischen Wirtschaftsstraftat zunächst das wirtschaftliche Wirken in Unrechtsstaaten im Blick gehabt, diesen danach aber auf staatliches Handeln in der Wirtschaftskrise, sodann auf die „schwarzen Kassen“ einer Partei als „politische Untreue“ sowie schließlich auf das Mannesmann-Verfahren als Politikum erweitert.²⁸ Der Charakter als politische Wirtschaftsstraftat entstehe gerade durch die weitreichenden Folgen für viele Bürgerinnen und Bürger.²⁹ Wer so viel wirtschaftliche Macht habe, „dass er dem Wirtschaftssystem und damit dem Einzelnen, der von diesem System abhängig ist, schweren Schaden zufügen kann“, der begehe „politische Untreue“.³⁰ Gleiches lässt sich aber auch bei systematischen Verstößen gegen den Datenschutz sagen,³¹ untechnisch gesprochen bei einem „Veruntreuen von Daten“ im großen Stil.

Bemerkenswert ist, dass die betreffenden Tech-Unternehmen ganz offensichtlich eigene Maßstäbe befolgen, auch im Hinblick auf Grund- und Menschenrechte. Dies erklärt sich daraus, dass ihr Business Modell darin besteht, einen „kostenlosen“ Service gegen Daten anzubieten, sodass sie sich durch das Sammeln von und den Handel mit Daten finanzieren.³²

26 Vgl. etwa *Reinbacher/Welzel*, Das Veröffentlichen politischer Fake News in sozialen Medien aus strafrechtlicher Sicht, in Bendheim/Pavlik (Hrsg.), „Fake News“ in Literatur und Medien, 2022, S. 55, 59 ff.; zum Einsatz von Social Bots s. *Reinbacher*, Social Bots aus strafrechtlicher Sicht, in Beck/Kusche/Valerius (Hrsg.), Digitalisierung, Automatisierung und Recht, FG zum 10jährigen Bestehen der Forschungsstelle RobotRecht, 2020, S. 457.

27 *Naucke*, Der Begriff der politischen Wirtschaftsstraftat, 2012, S. 4.

28 *Naucke* (Fn. 27), S. 13 ff., 39 ff., 48 f., 49 ff.

29 *Naucke* (Fn. 27), S. 57.

30 *Naucke* (Fn. 27), S. 36.

31 Für eine Einordnung des Falls Cambridge Analytica als politische Wirtschaftsstraftat bereits *Werkmeister* (Fn. 5), S. 576, zumal hier die Taten nicht nur wegen ihrer freiheitsüberwältigenden Macht als politisch anzusehen seien, sondern auch in ihren Auswirkungen unmittelbare auf das politische System bezogen gewesen seien.

32 Vgl. auch *Kubiciel* (Fn. 1), S. 57.

Ist ihre auf die Daten bezogene Überlegenheit an Wissen aber staatlich kaum noch kontrollierbar, so lässt sich eine Ohnmacht der Bürgerinnen und Bürger, letztlich sogar des Staates befürchten, die eine politische Dimension erreicht hat. *Jimenez* und *Oleson* sprechen hier von einer „Erosion der Staatsmacht“.³³ Nach *Naucke* ist eine Wirtschaftsstraftat auch dann politisch, „wenn sie als staatlich unkontrollierbare Macht auftritt und durch ihre Stärke Freiheit überwältigen kann“.³⁴

3. Warum Strafrecht?

Die in Rede stehenden Verstöße sind keine Bagatelle, da eine systematische Verletzung von Grund- und Menschenrechten in Rede steht. Im deutschen Rechtsverständnis geht es um das Recht auf informationelle Selbstbestimmung als Teil des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, bei umfassenden Persönlichkeitsprofilen sogar um den Kernbereich. In Art. 8 Abs. 1 der Charta der Grundrechte der EU und in Art. 16 Abs. 1 AEUV heißt es gleichlautend: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten“. Es gibt auf Unionsebene inzwischen diverse Regelungen, die den Datenschutz betreffen, insbesondere die DS-GVO.

Mit einfachen Ge- und Verboten ist es angesichts der Dimension des Unrechts aber nicht getan, da es um die Ahndung schwerwiegender Rechtsverstöße geht, die das Grundvertrauen in die digitale Marktordnung sowie die Menschenrechte, wenn nicht gar die Menschenwürde, verletzen, und wegen der Überlegenheit des Wissens der Täter das Potenzial besitzen, die Demokratie zu bedrohen. Dies gilt insbesondere dann, wenn durch die Addition von Informationen Persönlichkeitsprofile erstellt werden können oder jedenfalls besondere personenbezogene Daten im Raume stehen, wie sie in Art. 9 Abs. 1 DS-GVO aufgezählt sind und deren Verarbeitung grundsätzlich untersagt ist, nämlich personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Gerade solche Daten wurden im Cambridge Analytica-Fall verarbeitet. Auf dieses spezifische Unrecht muss auch das Strafrecht eine spezifische Antwort geben, auch wenn es dabei natürlich nicht den Anfang bilden sollte.

33 *Jimenez/Oleson* (Fn. 7), S. 989.

34 *Naucke* (Fn. 27), S. 4.

IV. Das geltende deutsche Datenstrafrecht

Fälle wie Cambridge Analytica können bereits nach geltendem deutschem Strafrecht geahndet werden. Hier steht zuvorderst § 42 BDSG im Fokus.³⁵ Nach § 42 Abs. 2 BDSG ist es strafbar, nicht allgemein zugängliche personenbezogene Daten ohne Berechtigung zu verarbeiten oder durch unrichtige Abgaben zu erschleichen. Beides war hier der Fall, da selbst die Nutzerinnen und Nutzer, die freiwillig an der Umfrage teilnahmen, zuvor darüber getäuscht wurden, dass Daten erhoben wurden, die Rückschlüsse auf ihre Person erlaubten, und zudem Daten ihrer Freundinnen und Freunde gesammelt wurden, die ohnehin gar keine Zustimmung gegeben hatten.

Der Tatbestand ist in verschiedener Hinsicht sehr problematisch und möglicherweise nicht geeignet, die Dimension des in Frage stehenden Unrechts abzubilden, auch wenn er in seinem Abs. 1 immerhin eine qualifizierte Strafe für Fälle enthält, in denen Daten einer großen Anzahl von Menschen ohne Berechtigung übermittelt oder zugänglich gemacht werden. Da ist zum einen seine Weite im Tatobjekt, das personenbezogene Daten jeder Art umfasst und nicht auf sensible Daten im Sinne des Art. 9 Abs. 1 DS-GVO beschränkt ist.³⁶ Zum anderen birgt das Merkmal „ohne Berechtigung“ ein hohes Unsicherheitspotenzial im Hinblick auf das Einsammeln von Daten durch Tech-Konzerne. Es zielt insbesondere auf eine datenschutzrechtliche Interessenabwägung sowie auf die datenschutzrechtliche Einwilligung i.S.d. Art. 6 DS-GVO ab.³⁷ Neben diesem Tatbestandsausschluss³⁸ dürfte zudem Raum für die allgemeine strafrechtliche Einwilligung sein, da ein nach europäischem Datenschutzrecht unzulässiger Vorgang nicht nach deutschem Recht strafbar sein muss. Hier ist nicht der Platz, ausführliche Überlegungen dazu anzustellen.³⁹ Einige kurze Anmerkungen seien jedoch gestattet.

So mag man die Frage aufwerfen, ob es dem Einzelnen möglich sein darf, so weitreichende Eingriffe in sein Persönlichkeitsrecht zu gestatten,

35 S. dazu ausführlich den Beitrag von *Dominik Brodowski* in diesem Band.

36 *Ehmann*, in: Gola/Heckmann, DS-GVO, BDSG, § 42 BDSG Rn. 9; *Werkmeister* (Fn. 5), S. 581.

37 *Brodowski/Nowak*, in: BeckOK Datenschutzrecht, § 42 BDSG, 43. Edition, Stand: 1.2.2023, Rn. 38 ff.

38 *Brodowski/Nowak*, in: BeckOK Datenschutzrecht, § 42 BDSG, 43. Edition, Stand: 1.2.2023, Rn. 35.1.

39 Insofern verweise ich wiederum auf den Beitrag von *Dominik Brodowski* in diesem Band.

dass er zum gläsernen Menschen wird und der Kern seiner Persönlichkeit, seine Menschenwürde, betroffen ist.⁴⁰ Meines Erachtens müssen wir das hier aber nicht vertiefen, denn das Problem der Datensammlung in den sozialen Netzwerken liegt insbesondere darin, dass eine solche Einwilligung eine vollständige Aufklärung über den Umfang der Datenerhebung und -verarbeitung voraussetzen würde und sich auf alle datenverarbeitenden Akteure beziehen müsste. Der Fall Cambridge Analytica hat zudem ein Licht darauf geworfen, dass Personen betroffen sein können, die gar nicht eingewilligt haben. Die Person, die in die Erhebung und Verarbeitung ihrer Daten einwilligen soll, muss vollständig darüber aufgeklärt sein, welche Daten erhoben werden sollen und was mit diesen Daten geschehen soll. Viele Menschen stimmen der Datenerhebung scheinbar zu, wissen sie aber überhaupt, worin sie einwilligen? Wenn das wahre Ziel der Unternehmen nicht in der Ermöglichung bestimmter Dienste, sondern im Sammeln und Verwerten von Daten liegt, so mag es häufig an der notwendigen Transparenz fehlen. Gar nicht wirksam ist die Einwilligung, wenn sie, wie im Fall Cambridge Analytica, durch eine Täuschung erlangt wurde. Zu überlegen ist auch, ob ein ausreichendes Wahlrecht der Kundinnen und Kunden angenommen werden kann, wenn ohne Einwilligung ein notwendiger Service gar nicht genutzt werden kann. Auch in solchen Fällen kann eine Einwilligung mit Willensmängeln behaftet sein.⁴¹

V. Auf dem Weg zu einer neuen Datenwirtschaftsstrafat?

Wenden wir uns zum Abschluss nun aber der Frage zu, wie ein Straftatbestand, der das spezifische Unrecht einer solchen politischen Datenwirtschaftsstrafat zum Ausdruck bringt, aussehen könnte, der Frage also, die den Background der heutigen Tagung bildet.⁴²

40 An einem dispositiven Rechtsgut würde es dann fehlen, wenn dem durch eine entsprechende Strafnorm zu schützenden Rechtsgut ein kollektiver Charakter beigemessen wird.

41 S. nur Art. 7 Abs. 4 DS-GVO, worin ein allgemeines Koppelungsverbot normiert ist, falls die Datenverarbeitung zur Vertragserfüllung nicht erforderlich ist; vgl. dazu Stemmer, in: BeckOK Datenschutzrecht, Art. 7 DS-GVO Rn. 42 ff.; ferner bereits Werkmeister (Fn. 5), S. 580.

42 S. bereits Werkmeister (Fn. 5), S. 576 ff.

1. Welchen Inhalt müsste eine Straftat nach deutschem Recht haben, die das gesteigerte Unrecht abbildet?

Die Informationswirtschaft muss rechtlich eingehegt werden, denn auch bei dieser darf es sich nicht um rechtlich ungebundene Macht handeln. Und dies kann ultimativ eben auch bedeuten, das Strafrecht als Mechanismus der rechtlichen Zählung eines informationsgierigen Unternehmens einzusetzen. Anders als dies in § 42 BDSG der Fall ist, bietet es sich an, einen qualitativen Blick auf die Daten zu richten, die es zu schützen gilt. Hier kann einerseits der bereits genannte Art. 9 Abs. 1 DS-GVO einen Anhaltspunkt bieten, der, wie ausgeführt, die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, generell verbietet. Andererseits stellt die systematische Kumulation von Informationen zu einem Persönlichkeitsprofil einen bestimmten Unwert dar, was auf dieser Tagung ja auch schon thematisiert wurde.⁴³ In einem solchen Fall ist die Menschenwürde tangiert.⁴⁴ Also ließen sich immerhin die Verwendung besonders sensibler Daten sowie die Kumulation zu einem Persönlichkeitsprofil als gravierende und spezielle Datenstraftaten ansehen. Im Vergleich dazu ist § 42 BDSG viel zu weit und unspezifisch. Aus der Sicht des Wirtschaftsstrafrechts könnte eine solche Norm dann nicht nur dem Schutz des Einzelnen dienen, sondern darauf gerichtet sein, das Vertrauen der Nutzergemeinschaft in die Einhaltung menschenrechtlicher Minimalstandards im Markt zu sichern.⁴⁵ Diese Forderung würde nicht unbedingt eine Erweiterung des Strafrechts beinhalten, sondern vielmehr auf eine Fokussierung auf den wesentlichen Unrechtskern abzielen, was mit einer Neuausrichtung des meines Erachtens zu weit gehenden und wenig überzeugenden Datenstrafrechts insgesamt einhergehen könnte.⁴⁶

In diesem Sinne ist interessant, dass auch Art. 1 Abs. 1 der VO über digitale Dienste⁴⁷ es als Ziel aus gibt, „durch die Festlegung harmonisier-

43 S. den Beitrag von *Sebastian Golla* in diesem Band.

44 Vgl. auch BVerfGE 27, 1, 6; 65, 1, 53.

45 Zur kollektiven Unrechtsdimension *Werkmeister* (Fn. 5), S. 577 f.

46 Vgl. zur Kritik etwa an der Datenhehlerei *Reinbacher*, Daten- oder Informationshehlerei, GA 2018, S. 311.

47 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates v. 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. EU L 277/1 v. 27.10.2022.

ter Vorschriften für ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld, in dem Innovationen gefördert und die in der Charta verankerten Grundrechte [...] wirksam geschützt werden, einen Beitrag zum reibungslosen Funktionieren des Binnenmarkts für Vermittlungsdienste zu leisten“. Im Hintergrund steht dabei aber auch der Schutz der Demokratie, wie der Fall Cambridge Analytica eindrucksvoll beleuchtet.

2. Sanktionen für Unternehmen oder persönliche Verantwortlichkeit?

Meines Erachtens ist es nicht ausreichend, Geldbußen für die Unternehmen zu verhängen, die in deren Berechnung der Gewinnspanne eingepreist werden können, denn es ist der Einzelne, der die bewusste Entscheidung trifft, in Ausübung seiner Tätigkeit für das Unternehmen bzw. unter Ausnutzung desselben, menschenrechtswidrig zu handeln.⁴⁸ Dafür muss er sich dann auch strafrechtlich verantworten. Versuche in die Richtung, Unternehmer dazu zu zwingen, menschenrechtskonform zu handeln, sehen wir gerade im Lieferkettensorgfaltspflichtengesetz,⁴⁹ das auch die internationalen Verzahnungen der Wirtschaft in Rechnung stellt. In diese Richtung geht auch das Gebot, menschenrechtliche Grundstandards in der Informationswirtschaft zu wahren, das dann auch strafbewehrt sein sollte.

3. Nationales oder internationales Strafrecht?

Dies führt mich zum letzten Punkt. Opfer der Datenverstöße der Tech-Konzerne finden sich auf der ganzen Welt, ebenso wie auch die Standorte der Täter. Die Wirtschaft wird immer globaler, immer grenzüberschreitender, immer vernetzter. Dies verlangt auch nach globalen Regelungen. Es ist folgerichtig, dass EU-Regelungen zur Einhegung des Informationskapitalismus getroffen werden. Aus ebendiesem Grunde sollte es im Interesse der Grund- und Menschenrechte der Einzelnen neben der Ahndung im nationalstaatlichen Strafrecht auch auf internationaler Ebene Regeln geben, die politische Datenwirtschaftsstrafataten adressieren. Es gibt erste Ideen,

48 Dies ist schon eine Erkenntnis der Nürnberger Prozesse der Jahre 1947/1948; vgl. *Naucke* (Fn. 27), S. 13 ff.

49 Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten, BGBl. I 2021, 2959; vgl. zu den strafbewehrten Pflichten auch *Wittig* (Fn. 19), § 3 Rn. 36.

dass es sich hierbei um Fälle handeln könnte, die ultimativ sogar als Wirtschaftsvölkerstrafrecht⁵⁰ eingestuft werden könnten, weil sie alle Staaten angehen.⁵¹

Bohlander erwägt etwa ein Verbrechen gegen die Menschlichkeit durch das Sammeln und Verwerten der Daten.⁵² Diese Überlegungen sind zwar interessant, weil systematische Angriffe auf die Menschenrechte vieler Personen im Raume stehen und eine besondere Form der Macht auftritt. Allerdings haben wir es bei Fällen wie Cambridge Analytica nicht mit der Beteiligung von Wirtschaftsunternehmen an den kriminellen Machenschaften eines Unrechtsstaates zu tun, sondern mit gezielten Angriffen auf Menschenrechte durch Einzelpersonen. Insofern besteht ein Unterschied zu Datenstrafataten, die durch staatliche Organisationen, etwa Geheimdienste, begangen oder initiiert werden.

Der erste und richtige Schritt wäre eine internationale Ächtung der genannten Praktiken durch völkerrechtliche Verträge. Da es sich um ein Problem international operierender Unternehmen in einer international verzahnten Wirtschaft handelt, müssen gemeinsame internationale Standards geschaffen werden. Die Cybercrime Convention⁵³ ist ein gutes Beispiel für einen solchen gemeinsamen Mindeststandard inklusive Pönalisierungspflicht. Diese Konvention des Europarates wurde von 68 Staaten unterzeichnet.⁵⁴ Sie bezieht sich auf Kriminelle, die von außen auf ein System und dessen Daten zugreifen, nicht aber auf ein System, das selbst auf diesen Zugriff ausgelegt ist. Insofern erscheint mir ein vergleichbares Abkommen angezeigt, das den Angriff auf Menschenrechte durch das systematische Sammeln von Daten in einem Computersystem bzw. durch den Betreiber eines Computersystems selbst zum Gegenstand hat.

50 Zum „Wirtschaftsvölkerstrafrecht“ vgl. *Ambos*, Wirtschaftsvölkerstrafrecht, 2018; *Jeßberger*, Die I.G. Farben vor Gericht, JZ 2009, S. 924, 931 f.; *Jeßberger/Kaleck/Singelstein* (Hrsg.), Wirtschaftsvölkerstrafrecht, 2015; *Wittig* (Fn. 19), § 3 Rn. 35 f.

51 *Bohlander*, „The Global Panopticon”: Mass Surveillance and Data Privacy Intrusion as a Crime against Humanity?, in *Böse/Bohlander/Klip/Lagodny* (Hrsg.), Justice Without Borders, 2018, S. 73; *Jimenez/Oleson* (Fn. 7), S. 1013 ff.

52 *Bohlander* (Fn. 51), S. 89 ff.

53 Convention on Cybercrime des Europarats v. 23.11.2001, ETS No. 185 (Budapest Convention).

54 S. www.coe.int/en/web/cybercrime/the-budapest-convention.

