Warum Datenschutz? Warum (Völker-)Strafrecht? Verfassungs-, europa- und völkerrechtliche Begründungsansätze

Antje von Ungern-Sternberg

I. Einleitung

Warum „Datenverbrechen" bestimmen, warum ein „Daten(wirtschafts)völkerstrafrecht" ausrufen? Diese Frage verweist auf mögliche Rechtsgüter, die dem Datenschutz zugrunde liegen und die das scharfe Schwert des Strafrechts rechtfertigen. Einer solchen Rechtfertigung bedarf es erst recht für eine völkerrechtliche Sanktionierung. Denn das Grundanliegen dieses Bandes bezieht sich ja nicht nur auf die grenzüberschreitende Sanktionierung von Straftaten im Sinne eines „internationalen Strafrechts" (§§ 3-7 StGB), sondern auf die Etablierung von Völkerstrafrecht, also die Sanktionierung auf völkerrechtlicher Grundlage. Datenverbrechen würden dann die bisherigen vier Völkerrechtsverbrechen – Genozid, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen, Aggression (Angriffskrieg) – ergänzen.

Die beiden Beiträge von *Brodowski* und *Golla* zum nationalen Datenstrafrecht betonen beide zu Recht Grenzen für einen strafrechtlichen Ansatz. *Brodowski* zeigt zunächst, dass die bestehenden Normen des Datenstrafrechts nicht das erfassen, was in diesem Band mit Daten(wirtschafts)völkerstrafrecht bezeichnet wird. Sodann führt er mögliche strafrechtliche Regelungsmodelle auf, die an Stufen der Verarbeitung, unterschiedliche Schutzobjekte, die fehlende Berechtigung zur Datenverarbeitung oder die prozessuale Zweckmäßigkeit anknüpfen. Dabei weist er kritisch auf die besondere Offenheit und mangelnde Fokussierung des derzeitigen Rechts hin (§ 42 BDSG, § 27 SaarlDSG, Art. 83 Abs. 4 und 5 DSGVO als „Quasi-Strafrecht"). *Golla* stellt mögliche Schutzgüter in den Mittelpunkt seiner Überlegungen. Er kritisiert die Akzessorietät des geltenden Datenschutzstrafrechts zum Datenrecht, da dessen offenes Schutzgut – das Recht auf informationelle Selbstbestimmung – nicht zum strafrechtlichen Schutz geeignet sei. Stattdessen schlägt er den Schutz von Persönlichkeitsprofilen und von Datenökosystemen vor.

Im Folgenden sei an diese Überlegungen angeknüpft, um schutzfähige Rechtsgüter aus öffentlich-rechtlicher Sicht zu benennen. Dabei soll es nicht nur um das nationale Recht, sondern gerade auch um das überstaatliche Europa- und Völkerrecht gehen. Hierbei lassen sich Individualgüter (II.) und Gemeinschaftsgüter (III.) unterscheiden. Im Anschluss sei nach der *völkerrechtlichen* Strafwürdigkeit von Datenschutzverstößen gefragt (IV.). Nach diesen Überlegungen ist – so meine These – für völkerrechtliche Datenverbrechen wenig Raum.

II. Individualgüter

Datenschutz dient zunächst den Rechten und Interessen der betroffenen Datensubjekte. Allerdings ist es gar nicht so einfach, die Schutzrichtung des Datenschutzes zu präzisieren. Die Datenschutzgrundverordnung (DSGVO) etwa erfasst die Verarbeitung personenbezogener Daten (nicht aber beispielsweise statistischer oder technischer Daten) in automatisierter Form oder zur Speicherung in einem Dateisystem (Art. 2 Abs. 1 DSGVO). Relevant sind also allein der Personenbezug und die Verarbeitungsmodalität, nicht aber etwa eine besondere Nähe zur Privat- oder Intimsphäre des Datensubjekts oder die mangelnde Öffentlichkeit des Datums. Ein derart umfänglicher Schutz bedarf der Begründung. Die Debatte um die Schutzgüter des Datenschutzes wird inzwischen auch auf europäischer Ebene mit Blick auf den sekundärrechtlichen Datenschutz und Art. 8 EU-Grundrechtecharta geführt. Sie erhält ferner Impulse von der völkerrechtlichen Ebene mit Blick insbesondere auf den menschenrechtlichen Schutz des Privatlebens, namentlich nach Art. 8 EMRK und Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte. Insgesamt ist festzustellen, dass Datenschutz zum einen die Privatsphäre schützt und zum anderen einen Vorfeldschutz zur Sicherung menschlicher Freiheit und Gleichheit beinhaltet.

1. Individuelle Verfügungsbefugnis zum Schutz der Privatsphäre

Datenschutz kann man zunächst als individuelle Verfügungsbefugnis über die eigenen personenbezogenen Daten begreifen. Das Bundesverfassungsgericht formuliert in seinem Volkszählungsurteil, das Grundrecht auf in-

formationelle Selbstbestimmung „gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[1] Es verfolgt hierbei aber keineswegs ein naives, eigentumsgleiches Verständnis von Datenschutz, was angesichts der unterschiedlichen Charakteristika von körperlichen Gegenständen und Daten auch nicht naheliegt.[2] Stattdessen kann man die Rechtsprechung so verstehen, dass sie das Individuum in die Lage versetzt, selbst über die Grenze zwischen Privat und Öffentlich zu entscheiden und somit die eigene Privatsphäre zu schützen.[3] Dieses Recht ist gerade im Verhältnis zu Privaten von Bedeutung, da diese ihrerseits grundsätzlich die Freiheit besitzen, Daten für ihre Zwecke zu erheben und zu verarbeiten. Dieser Aspekt des Datenschutzes ist aber auch im Verhältnis zum Staat nicht irrelevant: Zwar muss dieser sein Handeln stets rechtfertigen. Die Anforderungen hierfür sind aber umso strenger, je privater ein Datum ist. Die Breite des Datenschutzes ist somit dem Umstand geschuldet, dass die subjektiven Vorstellungen von schützenswerter Privatsphäre differieren. Es ist daher nur folgerichtig, wenn Datenschutz durch das Bundesverfassungsgericht aus dem Allgemeinen Persönlichkeitsrecht[4] oder durch den Europäischen Gerichtshof für Menschenrechte[5] und den UN-Menschenrechtsausschuss[6] aus dem Recht auf Privatleben abgeleitet bzw. in der Rechtsprechung des Europäischen Gerichtshofs in der Regel zusammen mit dem Recht auf Privatleben geprüft wird[7].

1 BVerfGE 65, 1, 43 (1983).
2 Daten zeichnen sich aus durch Nicht-Rivalität, Nicht-Exklusivität und Nicht-Abnutzbarkeit; zur aktuellen Debatte s. etwa *Kühling/Sackmann*, Irrweg „Dateneigentum", ZD 2020, S. 24 ff.
3 So etwa *Masing*, Herausforderungen des Datenschutzes, NJW 2012, S. 2305, 2308.
4 BVerfGE 65, 1, 41 ff. (1983).
5 S. etwa EGMR (GK) *S. und Marper/UK*, Nr. 30562/04, 30566/04, 4.12.2008, Rn. 66 ff.
6 S. etwa UN-Menschenrechtsausschuss, General Comment No. 16, Rn. 10.
7 S. etwa EuGH, Urt. v. 24.11.2011, C-486/10 *ASNEF*, Rn. 42; EuGH, Urt. v. 8.4.2014, C-293/12 u. C-294/12 *Digital Rights*, Rn. 38 ff.; EuGH, Urt. v. 13.5.2014, C-131/12 *Google Spain*, Rn. 80.

2. Vorfeldschutz zugunsten von Freiheit und Gleichheit

Datenschutz ist aber auch Vorfeldschutz und bezweckt, die Verletzung von Rechtsgütern mithilfe personenbezogener Daten zu verhindern.[8] Die Erhebung und Nutzung personenbezogener Daten können hierbei alle denkbaren Rechtsgüter gefährden oder beeinträchtigen: Sie beschränken Freiheit und Autonomie, wenn das Datensubjekt mithilfe seiner Schwächen, Vorlieben oder anderer Eigenschaften manipuliert und fremdgesteuert wird oder wenn sich ein Mensch in überwachten Räumen (Arbeitsplatz, öffentlicher Raum, digitaler Raum) in seiner Freiheitsbetätigung aus Furcht vor Sanktionen zurückhält.[9] Daten ermöglichen Diskriminierungen, wenn umfängliche Profile von Bewerbern, Arbeitnehmern, Kunden oder Bürgern erstellt und als Grundlage für nachteilige Entscheidungen genutzt werden.[10] Schließlich bilden Daten auch die Grundlage für Straftaten, die sich gegen eine ganze Bandbreite von Rechtsgütern richten können (Diebstahl, Betrug, Erpressung, Sexualdelikte…).[11] Den Vorfeldcharakter des Datenschutzes bringen auch zahlreiche Bestimmungen der DSGVO zum Ausdruck, etwa zur Beschränkung des Profiling und automatisierter Entscheidungen[12], zum Jugendschutz[13] oder zum Umgang mit besonders sensiblen Daten wie Gesundheit, Vorstrafen, sexuelle Orientierung oder politische Einstellung[14]. Stets geht es darum, die Datenverarbeitung als potentielle Grundlage für andere nachteilige Handlungen zu beschränken, beispielsweise das Hervorrufen und Steigern von Vorlieben bis hin zur Sucht oder das Ausnutzen von Schwächen für vertragliche Zwecke. Auch für den Menschenrechtsschutz durch Europäischen Gerichtshof für Menschenrechte oder den Zivilpakt

8 *Solove*, A Taxonomy of Privacy, University of Pennsylvania Law Review 154 (2006), S. 477 ff.; *Poscher*, Artificial Intelligence and the Right to Data Protection, in Voeneky/Kellmeyer/Mueller/Burgard (Hrsg.), The Cambridge Handbook of Responsible Artificial Intelligence, 2022, S. 281 ff.

9 S. hierzu BVerfGE 65, 1, 43; aus rechtsphilosophischer Sicht eindrücklich auch *Kœnig*, La fin de l'individu, 2019.

10 S. etwa *von Ungern-Sternberg*, Diskriminierungsschutz bei algorithmenbasierten Entscheidungen, in: Mangold/Payandeh (Hrsg.), Handbuch Antidiskriminierungsrecht – Strukturen, Rechtsfiguren und Konzepte, 2022, S. 1131 ff.

11 *Solove* (Fn. 8), 479 ff.

12 Art. 22 DSGVO.

13 Art. 6 Abs. 1 S. 1 lit. f, Art. 8 DSGVO.

14 Art. 9 und 10 DSGVO.

spielen die potentiell schädlichen Folgen der Datenverarbeitung eine Rolle.[15]

3. Datenverkehrsfreiheit im Binnenmarkt?

Der unionsrechtliche Datenschutz ist schließlich nicht nur dem Schutz der Datensubjekte, sondern auch dem freien Datenverkehr im Binnenmarkt verpflichtet, wie der Titel der Datenschutzgrundverordnung[16], die Kompetenzgrundlage[17] und die Zweckbestimmung der DSGVO[18] bezeugen. Die Vollharmonisierung weiter Bereiche des Datenschutzes[19] kommt insoweit auch Personen und Unternehmen zugute, die im Binnenmarkt personenbezogene Daten verarbeiten wollen. Allerdings wäre es missverständlich, die Datenverkehrsfreiheit als Schutzgut des Datenschutzes zu bezeichnen. Denn sie steht üblicherweise im Spannungsverhältnis zum Anliegen des Datenschutzes im engeren Sinne, die Verarbeitung personenbezogener Daten zu begrenzen. Außerdem fügt die „Datenverkehrsfreiheit" den klassischen Verkehrsfreiheiten des Binnenmarktes nichts hinzu, sondern umschreibt lediglich den einheitlichen Rechtsrahmen, auf den sich die datenverarbeitende Wirtschaft berufen kann.[20]

15 Der EGMR thematisiert etwa die negativen Auswirkungen staatlicher und privater Überwachung (Willkür, Missbrauch), s. z.B. EGMR (GK) *Zakharov/Russland*, Nr. 47143/06, 4.12.2015, Rn. 227 ff.; EGMR (GK) *Bărbalescu/Rumänien*, Nr. 61496/08, 5.9.2017, Rn. 121; zum UN-Menschenrecht etwa *Seibert-Fohr*, Digital Surveillance, Meta Data and Foreign Intelligence Cooperation: Unpacking the International Right to Privacy, in David/Ronen/Shany/Weiler (Hrsg.), Strengthening Human Rights Protections in Geneva, Israel, the West Bank and Beyond, 2021, S. 40 ff.; *United Nations High Commissioner for Human Rights*, Report, The Right to Privacy in the Digital Age, 3.8.2018, A/HRC/39/29, Rn. 12 ff.

16 Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

17 Art. 16 Abs. 2 AEUV.

18 Art. 1 Abs. 1 DSGVO.

19 S. bereits EuGH, Urt. v. 24.11.2011, C-486/10 *ASNEF*, Rn. 24 ff.

20 So wohl auch *Botta*, Die Datenverkehrsfreiheit – Ein Beitrag zur Schutzgutdebatte im Datenschutzrecht, DVBl. 2021, S. 290 ff.; ferner *Klement*, Öffentliches Interesse an Privatheit, JZ 2017, S. 161, 163 ff.

III. Gemeinschaftsgüter

Da personenbezogene Daten zu ganz unterschiedlichen (schädlichen) Zwecken eingesetzt werden können, lässt sich Datenschutz auch als Vorfeldschutz zugunsten kollektiver Schutzgüter verstehen.[21] Aus der Fülle potentieller Schutzgüter seien Demokratie und Rechtsstaatlichkeit (1.) sowie die nationale Souveränität (2.) herausgegriffen.

1. Demokratie und Rechtsstaatlichkeit

Die großen Datenschutzskandale der jüngeren Zeit belegen, dass Verletzungen des Datenschutzes auch Demokratie und Rechtsstaatlichkeit untergraben können. Der Skandal um *Cambridge Analytica* zeigt, wie personenbezogene Daten für gezielte Wahlkampfmaßnahmen genutzt werden. Das rechtswidrige Ausspähen von Vorlieben und Schwächen potentieller Wählerinnen und Wähler und das Ausnutzen eines derartigen Wissensvorsprungs durch eine Seite im Wahlkampf – ggf. mittels Desinformation und Manipulationen – gefährden den demokratischen Wahlkampf, die Freiheit der Wahlentscheidung und die Chancengleichheit der Parteien.[22] Zugleich können entsprechende gezielte und ggf. verzerrende und manipulative Informationen auch den Zweck verfolgen, verfeindete Bevölkerungsgruppen gegeneinander aufzuhetzen, seien es die „Black Lives Matter"-Bewegung und ihre Gegner in den USA, seien es verfeindete Ethnien in Ländern, die ohnehin mit Spannungen und Bürgerkriegen zu kämpfen haben.[23] Dies hat gravierende Folgen für die Geltung des Rechts und das staatliche Gewaltmonopol. Die Enthüllungen zu behördlichen Überwachungen von *Edward Snowden* bis *Pegasus* verdeutlichen ebenfalls, dass die Verfügbarkeit von Überwachungstechniken Staaten und ihren Behörden eine Umgehung

21 Zur autonomen (Selbstzweck) und funktionalen (Mittel als Zweck) Konzeption von Grundrechten im Allgemeinen *von Ungern-Sternberg*, Autonome und funktionale Grundrechtskonzeptionen unter besonderer Berücksichtigung der Rechtsprechung des EGMR, EuGRZ 2011, S. 199 ff.

22 S. bereits *von Ungern-Sternberg*, Demokratische Meinungsbildung und künstliche Intelligenz, in Unger/dies., (Hrsg.), Demokratie und künstliche Intelligenz, 2019, S. 3 ff.

23 S. etwa die vielfältigen Beispiele in *Woolley/Howard*, Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media, 2018.

rechtsstaatlicher Verfahren ermöglicht – ggf. auch, um Regimekritiker und Journalisten einzuschüchtern und zu bekämpfen.[24]

2. Schutz staatlicher Souveränität?

Das Völkerrecht beruht auf dem Recht eines jeden Staates auf Souveränität. Auch diesem völkerrechtlichen Gut könnte der Datenschutz dienen. Diese Überlegung mag auf den ersten Blick überraschen, da das klassische Völkerrecht vor physischen Übergriffen in die staatliche Souveränität schützt, aber die reine Informationsbeschaffung und -verarbeitung kaum regelt (also etwa Spionage nicht per se verbietet[25]). Außerdem betrifft der klassische Datenschutz die Daten natürlicher Personen, nicht aber die des Staates. Allerdings können die gerade genannten Gefahren von Datenschutzverstößen für Demokratie und Rechtsstaatlichkeit auch eine völkerrechtliche Dimension erlangen. Gerade die Nutzung personenbezogener Daten für grenzüberschreitende Eingriffe in einen Wahlkampf, für das Anheizen von gesellschaftlichen Konflikten oder das Vorgehen gegen unerwünschte Personen, jeweils verantwortet durch einen Staat und gerichtet auf das Gebiet eines anderen Staates, berühren dessen Souveränität. Das Völkerrecht tut sich noch schwer damit, diese nichtkörperlichen Einwirkungen einzuordnen. Eine mögliche Option wäre es beispielsweise, das Interventionsverbot – das bislang ein Element des Zwangs voraussetzt[26] – auch bei vergleichbar gravierenden informationellen Einwirkungen (etwa auf demokratische Wahlen) für einschlägig zu erachten.[27] Die Beispiele zeigen jedenfalls, dass personenbezogene Daten eben auch für grenzüberschreitendes Einwirken

24 *European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs*, Pegasus and Surveillance Spyware, PE 732.268, Mai 2022.

25 *Aust*, Spionage im Zeitalter von Big Data – Globale Überwachung und der Schutz der Privatsphäre im Völkerrecht, AVR 52 (2014), S. 375 ff.

26 IGH *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua. v. U.S.)*, 1986 I.C.J. 14, Rn. 205: „Intervention is wrongful when it uses methods of coercion […]. The element of coercion… defines, and indeed forms the very essence of prohibited intervention […]".

27 Hierzu *Watts*, Low-Intensity Cyber Operations and the Principle of Non-Intervention, in Ohlin/Govern/Finkelstein (Hrsg.), Cyber War: Law and Ethics for Virtual Conflicts, 2015, S. 249 ff.; *Ohlin*, Did Russian Cyber Interference in the 2016 Election Violate International Law? Texas Law Review 95 (2017), S. 1579 ff.; *Kilovaty*, Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information, Harvard National Security Journal 9 (2018), S. 146 ff.; *Tsagourias*, Electoral Cyber Interference, Self-Determination and the Prin-

auf andere Staaten, etwa für die Integrität der dortigen Wahlen und das friedliche Zusammenleben der dortigen Bevölkerungsgruppen genutzt werden können. Somit kann Datenschutz auch der völkerrechtlich geschützten Souveränität der Staaten zugutekommen.

IV. Strafwürdigkeit nach Völkerstrafrecht?

Anknüpfend an diese potentiellen Schutzgüter des Datenschutzes lässt sich nun nach der Strafwürdigkeit von Datenschutzverstößen fragen. *Brodowski* und vor allem *Golla* haben hier zu Recht eine gewisse Zurückhaltung angemahnt; stattdessen hat *Golla* eine Strafbarkeit nur bei spezifischen Unrechtstatbeständen vorgeschlagen. Diese Überlegungen gelten umso mehr für das Völkerstrafrecht, das sich bislang auf vier Kernverbrechen beschränkt. Soweit sich Datenschutz auf die Privatsphäre des einzelnen Individuums bezieht oder weiteren Individualrechtsgütern dient, erscheint es zweckmäßiger, auf völkerrechtlicher Ebene an einem gemeinsamen Verständnis und einer effektiven Beachtung der Menschenrechte zu arbeiten, als diese Menschenrechte gleich schon völkerstrafrechtlich sanktionieren zu wollen. Ein Datenschutzverbrechen, das einem Verbrechen gegen die Menschlichkeit[28] oder dem Kriegsverbrechen der Würdeverletzung[29] gleichkommt, kann man wohl nur in besonders krassen Ausnahmefällen, etwa bei der Totalüberwachung einer bestimmten Bevölkerungsgruppe, annehmen.

Eine ähnliche Zurückhaltung ist auch für den völkerstrafrechtlichen Schutz von Kollektivgütern wie der staatlichen Souveränität geboten, die nach bestehendem Völkerstrafrecht im Wesentlichen vor einem Angriffskrieg geschützt wird.[30] Auch hier müsste das Völkerrecht zunächst Normen für zulässige und unzulässige Formen des informationellen Handelns entwickeln, wie man es mit dem Tallinn Manual ja bereits versucht, bevor man das Völkerstrafrecht in Stellung bringt. Diese Weiterentwicklung des Völkerrechts ist eine drängende Aufgabe, denn das Beschaffen, Vermitteln und Nutzen bzw. Manipulieren von Informationen wirkt sich im Informationszeitalter ganz reell aus, etwa auf Wahlen, den gesellschaftlichen Frieden

ciple of Non-intervention in Cyberspace, in Broeders/van den Berg (Hrsg.), Governing Cyberspace: Behavior, Power, and Diplomacy, 2020, S. 45 ff.

28 Art. 7 IStGH Statut.

29 Art. 8 Abs. 2 lit. b) xxi) IStGH Statut.

30 Art. 8*bis* IStGH Statut.

oder die Funktionsfähigkeit der Infrastruktur. In einem zweiten Schritt könnten dann Überlegungen zur Strafwürdigkeit besonders schädlicher Handlungen (Cyberoperationen, Information Warfare) anschließen.