Rechtliche Ansätze an den Missbrauch von Datenmacht: Datenwirtschaftsvölker(straf)rechtliche Grundlegungen

Caroline Böck & Matthias C. Kettemann

I. Einleitung

Das Völkerstrafrecht ist grundsätzlich ein sehr eng gefasster Rechtsbereich. In materieller Hinsicht umfasst er die Tatbestände der Art. 5 Abs. 1 lit. a-d bzw. 6-8*bis* des Römischen Statuts des Internationalen Strafgerichtshofs (IStGH Statut). Die dort genannten Tatbestände beschränken sich auf die Verbrechen des Völkermordes (Art. 6), Verbrechen gegen die Menschlichkeit (Art. 7), Kriegsverbrechen (Art. 8) und das Verbrechen der Aggression (Art. 8*bis*). Allerdings enthält Art. 10 des Römischen Statuts eine Öffnungsklausel, wie folgt:

> „Dieser Teil ist nicht so auszulegen, als beschränke oder berühre er bestehende oder sich entwickelnde Regeln des Völkerrechts für andere Zwecke als diejenigen dieses Statuts."

Insofern ist es denkbar, dass sich völkerstrafrechtliche Regelungen jenseits der genannten Verbrechenstatbestände entwickeln und somit auch erweitern. Eine solche Auslegung ist indes nicht unumstritten.[1] Aktuell fokussieren sich Diskussionen um eine Erweiterung der Straftatbestände hauptsächlich auf den Tatbestand des sogenannten Ökozides, der eine völkerrechtliche Verantwortlichkeit bei extrem schwerwiegenden Eingriffen in die Umwelt pönalisieren soll, wobei eine genaue Begriffsbestimmung nicht besteht.[2] Somit wäre auch ein Wirtschaftsvölkerstrafrecht, ebenso wie ein spezifisches Daten(wirtschafts-)völkerstrafrecht, denkbar, welches unter anderem die Verwendung von Spionagesoftwares, wie PEGASUS oder Prism, strafrechtlich sanktioniert, die Grund- und Menschenrechte in

1 Vgl. etwa: *Bock*, Ökozid – ein neues völkerstrafrechtliches Kernverbrechen?, ZRP 2021, S. 187, 188 zum Ökozid.

2 *Batura/Eschenhagen/Oidtmann*, Defining Ecocide: An Interview with Philippe Sands, Völkerrechtsblog, 24.4.2021. Im Juni 2021 hat eine unabhängiges Expert:innengremium eine Definition für Ökozid vorgeschlagen, s. www.stopecocide.earth/legal-definition.

einer nicht rechtfertigbaren Art und Weise beschränken. Dabei würde auf einen potenziellen Missbrauch staatlicher Datenmacht abgestellt.

Ein spezifisches Daten(wirtschafts-)völkerstrafrecht existiert momentan nicht. Beleuchtet man den Begriff des Datenwirtschaftsvölkerstrafrechts genauer, bemerkt man die Zusammensetzung aus verschiedenen Bezeichnungen für unterschiedliche Rechtsbereiche. Dies deutet eine potenzielle Betroffenheit mehrerer Rechtsbereiche an, die für sich genommen grundsätzlich auch eine strafrechtliche Verantwortlichkeit implizieren: das Strafrecht selbst, das Datenwirtschaftsrecht sowie im weiteren Sinne die (strafrechtliche) Verantwortlichkeit von international agierenden Unternehmen.

1. Strafrecht

Aktuell existiert als umfassendes völkerstrafrechtliches Regelungswerk im Zusammenhang mit dem Missbrauch von Daten ausschließlich die Budapest Convention on Cybercrime des Europarates.[3] Auf Ebene der Vereinten Nationen (UN) befasst sich das United Nations Office on Drugs and Crimes (UNDOC) mit Sachverhalten im Bereich des Cybercrime.[4] Die durch UN GA Res. 64/230 initiierte Open-ended Intergovernmental Expert Group on Cybercrime befasste sich zwischen 2011 und 2021 ausschließlich mit dieser Thematik. Diese Arbeitsgruppe erstellte eine umfassende Studie zu Cyberkriminalität. Darin enthalten waren Untersuchungen zu den Reaktionen der Vertragsstaaten, der internationalen Gemeinschaft und des Privatsektors auf solche Sachverhalte. Daneben wurde der Informationsaustausch sowie weitere Rechtshilfemaßnahmen zwischen den Akteuren im Einklang mit nationalen Rechtsvorschriften untersucht, sowie bewährte Praktiken und die technische Unterstützung dieser Zusammenarbeit. Ziel war es, Optionen zur Stärkung bestehender und zum Vorschlagen neuer nationaler und internationaler rechtlicher oder sonstiger Reaktionen auf Cyberkriminalität zu erarbeiten.[5]

3 Council of Europe, Convention on Cybercrime, 23.11.2001, www.refworld.org/docid/47fdfb202.html.

4 Cybercrime: www.unodc.org/unodc/en/cybercrime/index.html.

5 Open-ended Intergovernmental Expert Group Meeting on Cybercrime, www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html.

Zudem gibt es im Völkerrecht kein strafrechtliches Verbot der Spionage, also der angriffsmäßigen, verdeckten Beschaffung von „geheimen" Daten[6], welche nicht unbedingt auf die wirtschaftliche Nutzung gerichtet ist, aber zumindest einige Gemeinsamkeiten mit dem Begriff des Datenwirtschaftsstrafrechts aufweist. Allerdings ist rechtlich auch keine allgemeine Zulässigkeit von Spionage anerkannt, da hierüber keine Erlaubnisnorm existiert. Daher besteht zumindest die Möglichkeit, dass einige Arten von Spionage gegen allgemeine völkerrechtliche Normen verstoßen. Gleiches gilt für Teile der Datenwirtschaft, die in Zusammenhang mit „geheimen Daten" stehen.[7]

2. Datenwirtschaftsrecht

Der Begriff sowie der Rechtsbereich des Datenwirtschaftsrechts sind relativ neu. Datenwirtschaftsrecht rekurriert vorwiegend auf Vorschriften aus dem EU-Recht, wobei – auch mangels unionaler Gesetzgebungskompetenz – kein konkreter Diskurs zu einem unionalen Datenwirtschaftsstrafrecht besteht. Verstanden wird unter dem Begriff jene Rechtsmaterie, welche sich mit Daten und deren Stellung als Wirtschaftsgut beschäftigt.[8] Untersucht und reguliert werden sollen in diesem Rechtsbereich die Nutzbarkeit, der Zugang, die Marktfähigkeit, aber auch mögliche Grenzen einer (nicht-) kommerziellen, allgemeinwohlorientierten Verwendung von Daten.[9]

Zu den existierenden und zukünftigen Rechtsgrundlagen zählen die E-Commerce Richtline (2000/31/EG), (die „Richtlinie über audiovisuelle Mediendienste"), Abl. 1989 Nr. L 331/51; geändert durch Richtlinie 2007/65 EG, Abl. 2007 Nr. L 332/27 (ehemals Fernseh-RL) und der Digital Services Act (DSA). Darüber hinaus zählen zum Datenwirtschaftrecht Regelungen im Bereich des Immaterialgüterrechts (Internet of Things; insbesondere

6 Zum Begriff etwa: *Wagener*, Begriff Spionage, in Görres-Gesellschaft, Staatslexikon.

7 So etwa: *Ewer/Thienel*, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, S. 30, 31.

8 *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, Die Datentreuhand, MMR-Beil. 2021, S. 25, 25; *Louven*, Datenmacht und Zugang zu Daten, NZKart 2018, S. 217, 217 mit Verweis auf das Arbeitspapier der Kommission „BUILDING A EUROPEAN DATA ECONOMY", die den Aufbau einer europäischen Datenwirtschaft zum Ziel hat.

9 Genauer zur Begriffsbestimmung und -einordnung: *Steinrötter*, Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RDi 2021, S. 480, 481 f.

Reform der Warenkauf-RL (RL 2019/771, „embedded software") und solche im Bereich der Künstlichen Intelligenz (Artificial Intelligence Act), ebenso Gesetzesänderungen im Bereich des Kartellrechts durch den Digital Markets Act (DMA), Verordnung über bestreitbare und faire Märkte (Gesetz über digitale Märkte). Das Datenschutzrecht kann aufgrund zahlreicher Schnittstellen ebenso als Teil angesehen werden.[10] Daher bilden auch die DSGVO und der jüngst verabschiedete Data Governance Act einen Teil dieses Rechtsgebiets.

Sowohl die DSGVO als auch DMA und DSA enthalten umfassende Bestimmungen mit Sanktionscharakter. Beispielhaft sei hier auf Art. 84 DSGVO iVm. § 42 Abs. 2 BDSG verwiesen, wonach das Erschleichen von personenbezogenen Daten – sogar – strafrechtlich sanktioniert wird.[11] Zu erwähnen sind auch die potenziell hohen Zwangsgelder, welche nach Art. 76 DSA erlassen werden können. Diese können sich auf bis zu 5 % des weltweiten Jahresumsatzes eines Unternehmens erstrecken, wenn dieses etwa den einschlägigen Bestimmungen der Verordnung sowie den weitreichenden Auskunftsansprüchen nicht Folge leistet, vgl. Art 76 Abs. 1 lit. e DSA.

Auf regional völkerrechtlicher Ebene finden sich erste grobe Datenschutzregelungen in der Convention 108 des Europarates aus dem Jahr 1981.[12] Diese enthalten keine Sanktionen und stellen nur grobe Richtlinien für (un)-zulässige Datenverarbeitung dar, aber sie lassen eine Richtung dahingehend erkennen, dass die wirtschaftliche Nutzung von Daten aus Sicht der Unternehmen nicht uneingeschränkt erfolgen kann.

Es handelt sich somit nicht um eine abgeschlossene Rechtsmaterie. Vielmehr findet das Datenwirtschaftsrecht in verschiedenen Gesetzes- sowie Rechtsbereichen seinen Niederschlag, wenn es um die wirtschaftliche Nutzung der Daten geht.

10 Im Ergebnis auch: *Steinrötter* (Fn. 9), S. 481 f., sieht das Datenschutzrecht zwar als einzelnes Rechtsgebiet an, aber er verweist selbst auf wesentliche Schnittmengen und dass die Fragestellungen nicht isoliert betrachtet werden können.

11 Vgl. genauer zum Straftatbestand etwa: Gola/Heckmann/*Gola*, 3. Aufl. 2022, DS-GVO Art. 84 Rn. 10 ff.

12 Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28.1.1981, ETS 108, www.refworld.org/docid/3dde1005a.html.

3. Unternehmensverantwortung

In Deutschland hat sich die Diskussion über mehr strafrechtliche Verantwortlichkeit von Unternehmen in dem – nunmehr vorerst gescheiterten – Entwurf über ein sog. Verbandssanktionengesetz kanalisiert. Damit sollten Unternehmen unter Androhung von teils hohen Geldstrafen wegen im Unternehmen begangener Straftaten zu mehr Compliance-Anstrengungen angeregt werden. Ziel sollte es sein, strafrechtliche Handlungen von Mitarbeitenden im Unternehmen von vorneherein zu unterbinden.[13] Dennoch werden Unternehmen in Zukunft aufgrund des beschlossenen Lieferkettensorgfaltspflichtengesetzes zumindest zu mehr Verantwortlichkeit im Umgang mit Menschenrechtsverletzungen und Umweltverstößen genommen.[14] Zudem wird in Deutschland zumindest im Zivilrecht eine neue Form von Sammelklagen gegen Konzerne auf den Weg gebracht, wodurch Verbraucher*innen in (zivilrechtlichen) Verfahren schnelle, kollektive Entschädigungen erhalten können sollen, ohne selbst ein Gerichtsverfahren anstrengen zu müssen. Der Entwurf wurde Ende März 2023 vom Bundeskabinett gebilligt und muss nun noch durch Bundestag sowie Bundesrat bewilligt werden.[15]

Auch in anderen europäischen Ländern, wie Frankreich und Schweden, wird die Frage von internationaler strafrechtlicher Verantwortlichkeit von Unternehmen thematisiert. Diese Initiativen beschränken sich anders als das deutsche Vorbringen auf Gerichtsverfahren und deren konkrete Parteien. Das französische Verfahren, gegen das Zementunternehmen *Lafarge*, ist das weltweit erste Gerichtsverfahren, in welchem ein Unternehmen als juristische Person und nicht nur dessen Führungskräfte wegen Beihilfe zu Verbrechen gegen die Menschlichkeit bezichtigt wurden. Es soll in den

13 *Rotsch/Mutschler/Grobe*, Der Regierungsentwurf zum Verbandssanktionengesetz – kritische Analyse und Ausblick, CCZ 2020, S. 169, 169 f.

14 Vgl. hierzu etwa: *Bomsdorf/Blatecki-Burgert*, Lieferketten-Richtlinie und Lieferkettensorgfaltspflichtengesetz, ZRP 2022, S. 141; auch: *Berg/Kramme,* LkSG (im Erscheinen).

15 Vgl. hierzu etwa: Kabinett bringt neue Form von Sammelklagen gegen Konzerne auf den Weg, 29.3.2023, www.zeit.de/wirtschaft/2023-03/abhilfeklage-verbraucher-sammelklagen-konzerne-kabinett-marco-buschmann?utm_referrer=https%3A%2F%2Fwww.google.com%2F.

Jahren 2013 und 2014 Schutzgeld an den IS in Syrien gezahlt zu haben, um die eigene Fabrik weiterbetreiben zu können.[16]

Darüber hinaus gibt es aktuell Diskussionen zur internationalen strafrechtlichen Verantwortlichkeit von Unternehmen auf globaler Ebene, insbesondere von Transnationalen Corporations (TNCs). Diskutiert wird die Frage, wie Unternehmen für ethisch oder sogar rechtlich vorwerfbares Verhalten zur Verantwortung gezogen werden sollen resp. gezogen werden können. Die Meinungen hierbei sind vielfältig. Einerseits wird progressiv gefordert, eine direkte Unternehmensverantwortlichkeit ohne Umweg über leitende Angestellte international zu etablieren, um die kollektive Macht und Dynamik eines Unternehmens ausreichend rechtlich zu würdigen.[17] Andererseits wird darauf abgestellt, zunächst eine Verantwortlichkeit von leitenden Angestellten zu fordern und erst in einem zweiten Schritt eine daran anschließende, zusätzliche Verantwortlichkeit von Unternehmen.[18] Zudem solle dies nur ein Teil eines Maßnahmenbündels darstellen, welches insbesondere völker- sowie menschenrechtliche Mindeststandards festlegt.[19] Deutlich wird indes der internationale Trend hin zu mehr unternehmerischer Verantwortlichkeit in straf- sowie zivilrechtlichen Verfahren, welche auch den Einsatz von Sanktionen vorsehen soll.

16 *Fock*, War Lafarge an IS-Verbrechen beteiligt?, 24.5.2022, www.lto.de/recht/hintergruende/h/lafarge-syrien-buergerkrieg-beihilfe-unternehmen-verbrechen-gegen-menschlichkeit; *Riello/Furtwengler*, Corporate Criminal Liability for International Crimes: France and Sweden Are Poised To Take Historic Steps Forward, 6.9.2021, www.justsecurity.org/78097/corporate-criminal-liability-for-human-rights-violations-france-and-sweden-are-poised-to-take-historic-steps-forward.

17 *Lambridis*, Corporate Accountability: Prosecuting Corporations for the Commission of International Crimes of Atrocity, 24.5.2021, www.nyujilp.org/corporate-accountability-prosecuting-corporations-for-the-commission-of-international-crimes-of-atrocity.

18 *Ambos*, International Economic Criminal Law: The Foundations of Companies' Criminal Responsibility Under International Law, Criminal Law Forum 29 (2018), S. 499, 565.

19 *Ambos* (Fn. 18), S. 565.; vgl. wohl auch *Engelhart*, International Criminal Responsibility of Corporations, in Burchard/Triffterer/Vogel (Hrsg.), The Review Conference and the Future of the International Criminal Court, 2010, S. 187 ff.; *Burchard*, Regulating Business with Bad Actors: Aiding and Abetting and Beyond, Texas International Law Journal: The Forum 50 (2015), S. 2; *Buzanich-Sommeregger*, Menschenrechte und Berichtspflicht, ÖstAnwbl 2016, S. 580, 580 f.

4. Zwischenergebnis

Ein spezifisches Daten(wirtschafts-)völkerstrafrecht existiert weltweit aktuell nicht. Das liegt mitunter daran, dass der Begriff des Datenwirtschaftsrechtes als solcher vornehmlich innerhalb der Europäischen Union und im Rahmen der entstehenden Digitalstrategie verwendet wird.

Allerdings ist insgesamt eine Tendenz zu mehr Verantwortlichkeit von Unternehmen als solchen erkennbar. Zwar besteht kein konkretes Gesetzesvorhaben oder die Erstellung eines völkerrechtlichen Vertrages zur internationalen (strafrechtlichen) Verantwortlichkeit von Unternehmen, aber die gerichtlichen Sachverhalte sowie das Lieferkettensorgfaltsgesetz zeigen einen Trend hin zu einer stärkeren Verantwortlichkeit. Dies wird selbst von weniger progressiven Stimmen in der internationalen rechtswissenschaftlichen Literatur gefordert.

Die Entstehung eines Datenwirtschaftsvölkerstrafrechts auf internationaler Ebene würde sich in diese Diskussion einbetten, ist somit denkbar und liegt im Interesse einiger rechtlicher Interessengruppen. Dies gilt umso mehr, als unionale Gesetzesinitiativen meist breite globale Ausstrahlungswirkung entfalten.

II. Mögliche Anwendungsfelder: Missbrauch staatlicher Datenmacht

Mit technologischem und digitalem Fortschritt haben sich die Möglichkeiten und Bedingungen der Informationsbeschaffung und -aufarbeitung erheblich verändert. Insbesondere gilt dies für die verdeckte Informationsbeschaffung. Nicht nur Unternehmen und große Konzerne müssen daher in den Fokus der (strafrechtlichen) Verantwortlichkeit von missbräuchlicher Datennutzung gerückt werden. Auch Staaten nutzen häufig Unternehmen, um ihr Informationsinteresse über die eigene Bevölkerung, aber auch global, zu befriedigen. Dabei verändert sich das Verhältnis von Staaten zu Individuen, da diese und rechtlich relevante Tatbestandsmerkmale vermehrt über Datenpunkte konstruiert, im Wege automatisierter Verfahren verarbeitet und letztlich gesteuert werden.[20] Individuen verlieren so ein Stück weit die Kontrolle über preisgegebene Daten.

20 Detailiert: *Johns*, Governance by Data, Annual Review of Law and Social Science, 17 (2021), S. 53 ff.

Dies führt dazu, dass zahlreiche private Akteure eine Vermittlungsrolle zwischen staatlicher Dienstleistung und staatlicher Gewaltanwendung geworden sind.[21] So hat das US-amerikanische Unternehmen *Palantir* bei der Entwicklung von Plattformen zur „effektiven" Polizeiarbeit einen maßgeblichen Beitrag geleistet. Dieses kritisch beäugte Data-Mining Programm wird von einigen Polizeibehörden in den Vereinigten Staaten von Amerika, aber auch deutschen Polizeibehörden,[22] verwendet, um zukünftige Verbrechen durch Auswertung von Verbrechens- und Verhaftungsberichten vorherzusagen. *Palantirs* Programme stehen in der Kritik, rassistische Ergebnisse zu produzieren.[23]

Die staatlich beauftragte Datenbeschaffung und -auswertung mittels privater Unternehmen oder von diesen entwickelten Software-Programmen gehtnoch viel weiter.[24] Europäische Nachrichtendienste verarbeiten in großem Ausmaß kommerziell erworbene Daten aus teils sehr fragwürdigen Quellen. Ein Erwerb findet häufig bei Datenmarklern, aber auch im Darknet statt. Woher diese Daten stammen, aber auch ob die Daten verifiziert oder illegal erworben sind, wird dabei nicht geprüft. Die Exekutive verarbeitet so eine immense, zugleich auch sensible Datenmenge in Zusammenarbeit mit Privaten und erhält ein Werkzeug, um die Bevölkerung in Bezug auf potenzielle Straftaten besser einschätzen zu können. Dies ist nicht nur aus dem eben erwähnten Argument missbrauchsanfällig. Vielmehr ist zusätzlich fragwürdig, wie und ob die privaten Akteure die erlangten Daten weiter nutzen, wenngleich dies nicht rechtmäßig wäre.

Daneben werden Daten auch in großem Umfang von internationalen Organisationen, wie der Global Working Group on Big Data for Official Statistics erhoben und verwertet, die 2015 von der Statistischen Kommission der Vereinten Nationen ins Leben gerufen wurde.[25] Diese erhebt Daten in zahlreichen Lebensbereichen, wie etwa anonymisierte Mobiltelefondaten

21 *Johns* (Fn. 20), S. 57 f.

22 *Harlan/Kartheuser/Schöffl*, Schafft die Polizei den gläsernen Bürger?, 3.6.2022, www.tagesschau.de/investigativ/br-recherche/polizei-analyse-software-palantir-101.html.

23 Vgl. etwa: *Hvistendahl*, How the LAPD and PALANTIR use data to justify racist policing, 30.1.2021, https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing.

24 *Wetzling/Dietrich*, Disproportionate Use of Commercially and Publicly Available Data: Europe's Next Frontier for Intelligence Reform?, 2022, www.stiftung-nv.de/de/publikation/disproportionate-use-commercially-and-publicly-available-data.

25 *Johns* (Fn. 20), S. 62 f.

zur Erstellung von Migrations- und Tourismusstatistiken oder Supermarkt-Scannerdaten zur Erstellung von Inflationsstatistiken. Auch diese Datenerhebungen bergen erhebliches Missbrauchspotenzial.[26]

Anders als bei klassischen Statistiken sind solche Datenerhebungen umfangreicher, und aufgrund der Anonymität der Daten werden die betroffenen Personen nicht über die Datenerhebung informiert. Durch wen und wie diese Daten anonymisiert werden, ist weitgehend unbekannt. Staatliche Akteure können so einen stärkeren sowie schnelleren Einfluss auf das Verhalten der einzelnen Bürger nehmen, als es noch vor einigen Jahrzehnten der Fall war, als klassische Statistiken die Mehrheit der erworbenen Daten darstellten.

Diese großen Sicherheitsrisiken und Missbrauchspotenziale sollten von regulatorischer Seite in den Blick genommen werden, um sich aus Sicht des Gesetzgebers selbst eindeutige Grenzen zu setzen und einen menschenrechtsfreundlichen Umgang mit Datenerwirtschaftung zu ermöglichen. Insbesondere sollte die Tätigkeit der Nachrichtendienste beim kommerziellen Erwerb von – aus ihrer Sicht öffentlich zugänglichen - Daten reguliert werden, denn fehlende rechtliche Beschränkungen und unzureichende Aufsicht können das Risiko eines unverhältnismäßigen Zugangs zu personenbezogenen Daten ohne ausreichende Rechenschaftspflicht erhöhen.[27] Dies gilt umso mehr, als die bestehenden datenschutzrechtlichen und die Privatsphäre regelnden Normen vorwiegend nicht auf nachrichtendienstliche Tätigkeit anwendbar sind.

Anstatt sich auf „einzelne missbräuchliche Datenverarbeitungsvorgänge zu fokussieren, sollte zudem die Gefahr systematisch datenbezogenen Machtmissbrauchs adressiert werden".[28] Um effektive Governance-Regelungen zu schaffen, ist es zudem wichtig, verschiedene Interessensgruppen in den Gesetzgebungsprozess miteinzubeziehen. Aus Sicht demokratischer Staaten sollte eine Regelung dabei immer auf einen potenziellen Missbrauch untersucht und ggfs. angepasst werden, da diese sonst von autoritären Regimen missbraucht werden könnte (sog. Dictator-proof rules). Gleichzeitig muss eine Überregulierung vermieden werden. Hier ist es notwendig, einen Mittelweg zu finden und stets die geschützten Interessen der Individuen im Blick zu behalten, die Ausgangspunkt einer Regulierung sein sollten.

26 *Johns* (Fn. 20), S. 62 f.
27 *Wetzling/Dietrich* (Fn. 24), S. 4.
28 *Wetzling/Dietrich* (Fn. 24), S. 53.

Diskutiert werden sollte daher eine Nachbesserung der DSGVO; insbesondere die Zuständigkeitsbereiche des Europäischen Datenschutzbeauftragten sollten überdacht werden.[29] Zudem sollten die Mitglieder des Europarats das Übereinkommen 108+[30] ratifizieren.

III. Konkret: NSA-Skandal, Pegasus und Co. – Völker(straf-)rechtliche Bewertung

1. Sachverhalt(e): NSA (Prism); Pegasus (NSO Israel); ECHELON (5 Eyes); HackingTeam

In der letzten Dekade des 21. Jahrhunderts hat sich die digitale Technik so rasant wie noch nie entwickelt. Allerdings bringt diese Technik auch einige Schattenseiten mit sich, gerade wenn es um die Überwachung anderer Personen sowie staatlicher Akteure geht, wie soeben beschrieben. Mittlerweile sind zahlreiche Sachverhalte in der Weltgemeinschaft bekannt, in denen staatlicher Akteure selbst oder unter Zuhilfenahme von privaten Unternehmen systematisch Gruppen von Individuen oder anderen Staaten teils über mehrere Jahre hinweg überwacht sowie die erhobenen Daten gespeichert haben.

Wir erinnern uns: Im Jahr 2011 entwickelte das israelische Unternehmen NSO Group Technologies (NSO) die Spionagesoftware Pegasus (*zero-touch exploit*). Obwohl die Software ursprünglich zur Bekämpfung von Terrorismus und Kriminalität entwickelt wurde, wurde die Technologie von autoritären Staaten zur Überwachung und Spionage weltweit genutzt. Dazu zählt, neben autoritären Staaten, auch eine lange Liste von EU-Mitgliedstaaten.[31] Auch der deutsche Bundesnachrichtendienst sowie das Bundeskriminalamt haben jüngst den Einsatz einer modifizierten Software „Pegasus" zugegeben.[32] Es folgte eine öffentliche sowie politische Verurteilung dieser Aktivitäten durch eine Vielzahl von anderen EU-Institutionen.[33] Ähnliche Soft-

29 *Wetzling/Dietrich* (Fn. 24), S. 53.
30 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.1.1981, https://rm.coe.int/1680078b38.
31 *Marzocchi/Mazzini*, Pegasus and Surveillance Spyware, In-Depth Analysis, 2022, www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf.
32 *Marzocchi/Mazzini* (Fn. 31), S. 11.
33 *Marzocchi/Mazzini* (Fn. 31), S. 15 ff.

ware wurde bzw. wird durch das italienische Unternehmen HackingTeam, das mittlerweile den Geschäftsbetrieb eingestellt hat und unter dem neuen Namen MementoLabs agiert, entwickelt und an Dritte verkauft, die diese unbeschränkt nutzen können.[34]

Daneben sei mit Bedacht auf die Vereinigten Staaten von Amerika und Großbritannien auf die internationale Geheimdienstallianz Five Eyes (AUS/CAN/NZ/UK/US) und mittlerweile auch Nine Eyes (+DEN, FR, NL, NOR) sowie 14 Eyes (+DE, S, BE, ES, IT) verwiesen. Zu dieser Geheimdienstallianz gehört im erweiterten Kreis nun auch Deutschland, wobei bei Weitem nicht alle Informationen wie im engen Kreis der 5 Eyes-Staaten ausgetauscht werden.

Zu Zeiten des Kalten Krieges entwickelten die 5-Eyes-Staaten das Überwachungsnetzwerk ECHELON, welches sämtliche staatliche Kommunikation erfassen, sammeln und analysieren können sollte. Mit dem Zusammenbruch der Sowjetunion fokussierte das Überwachungsnetzwerk auch auf private sowie kommerzielle Kommunikation weltweit. Dies mündete unter anderem im NSA-Skandal.[35]

Der NSA-Skandal wurde 2013 nach den Enthüllungen von geheimen Dokumenten durch den Whistleblower Edward Snowden publik. Demnach hatten die US-Regierung und das Vereinte Königreich unter Mitwirkung von Internetkonzernen im großen Umfang global und dazu noch verdachtsunabhängig Kommunikation überwacht. Dazu nutzten die Staaten Software wie Prism sowie deren Weiterentwicklung von ECHELON. Prism ermöglichte die massenhafte Speicherung und Auswertung von Internetkommunikation. In diesem Zusammenhang wurde durch Edward Snowden auch das ähnlich funktionierende britische Programm TEMPORA des britischen Geheimdienstes Government Communications Headquarters (GCHQ) offengelegt. Nach Offenlegung fiel die Rechtfertigung des Einsatzes solcher umfassender Überwachungsmechanismen recht knapp aus. Als Rechtfertigung wurde lediglich die Terrorismusbekämpfung im Allgemeinen angeführt.[36] Dies scheint vor dem Hintergrund der umfassenden Überwachung eine juristisch schwache Argumentation dazustellen.

---

34 *Brien,* HackingTeam: Mitgründer erklärt Spionagesoftwarefirma für tot, 30.5.2020, https://t3n.de/news/hacking-team-mitgruender-fuer-1284946.

35 Vgl. zu der genauen Geschichte: *Shim,* Diese Augen sind überall: So agieren Geheimdienste im Internet, 27.7.2021, www.computerbild.de/artikel/cb-Tests-Software-Tipps-Five-Eyes-14-Eyes-VPN-erklaert-27863421.html.

36 Vgl. zur Geschichte etwa: *Ewer/Thienel* (Fn. 7), S. 30 f.

Diese Sachverhalte haben medial große Wellen geschlagen und für viel Unmut sowie Sorgen betreffend die Wahrung von Menschenrechten, wie der Meinungsfreiheit sowie Privatsphäre, gesorgt. Der Unmut ist sogar so weit gegangen, dass das Europäische Parlament die Einsetzung eines Untersuchungsausschusses beschlossen hat, um die Nutzung von Staatstrojanern, wie PEGASUS, innerhalb der EU zu untersuchen.

Aufgabe des Ausschusses ist es, etwaige Verstöße oder Missstände bei der Anwendung des EU-Rechts im Zusammenhang mit der Verwendung von PEGASUS und gleichwertiger Spionage-Software zu untersuchen. Im Fokus der Untersuchung steht dabei die Frage, inwiefern die Mitgliedsstaaten (oder Drittländer) durch Überwachungsmaßnahmen gegen die Grundrechte-Charta der EU verstoßen.

Im Verfahren des PEGASUS-Untersuchungsausschusses ging *David Kaye*, der ehemalige Sonderberichterstatter für Meinungsäußerungsfreiheit, am 27. Oktober 2022 in Bezug auf die PEGASUS Software von einer Rechtswidrigkeit der Anwendung ex ante vor:[37]

> „In Anbetracht all dessen, was ich festgestellt habe, habe ich ernsthafte Zweifel daran, dass Überwachungstechnologien mit ähnlichen Merkmalen wie PEGASUS jemals den Anforderungen der internationalen Menschenrechtsvorschriften genügen können. Ihr Einsatz sollte daher als rechtswidrig angesehen werden."

Darüber hinaus forderte *Kaye* im Moratorium für die „Entwicklung, die Vermarktung, der Verkauf, die Weitergabe und der Einsatz von Instrumenten wie PEGASUS", um Schutzmaßnahmen zu ermöglichen:

> „Strenge, international vereinbarte Exportkontrollen, echte Transparenz und Aufsicht, eine radikale rechtliche Reform der Überwachungspraktiken und -gesetze, die Beseitigung von Hindernissen für die Immunität von Staaten".

Insofern scheint es naheliegend, die Gefährlichkeit von solchen eingesetzten Softwares umfassend rechtlich und insbesondere strafrechtlich zu untersuchen.

37 *Kaye*, Testimony to the PEGA Committee of the European Parliament vom 27.10.2022; abrufbar unter https://cpb-us-e2.wpmucdn.com/sites.uci.edu/dist/2/4290/files/2022/10/Testimony-before-the-European-Parliament-PEGA-Committee-KAYE-27-Oct-2022.pdf.

2. Rechtliche Würdigung

Wie solche Sachverhalte rechtlich zu bewerten sind und anhand welcher Normen sie rechtlich fixiert werden können, wird im nachfolgenden Abschnitt genauer analysiert. Dabei werden zunächst die möglichen bestehenden völkerstrafrechtlichen Tatbestände dargestellt, in einem zweiten Schritt eingeordnet sowie subsumiert, und schließlich werden ausgewählte Problemfragen beleuchtet, die mit einer solchen Strafbarkeit einhergehen.

a. Völkerstrafrechtliche Tatbestände de lege lata

Wie bereits beschrieben, existiert kein klar konturiertes Datenwirtschaftsvölkerstrafrecht. Allerdings existieren allgemeine völkerrechtliche Normen, welche einschlägig sein können. Diese finden sich hauptsächlich im Römischen Statut des Internationalen Strafgerichtshofs wieder.

In Betracht kommt de lege lata lediglich eine Strafbarkeit nach Art. 7 des Römischen Statuts. Dieses ist an strenge Voraussetzungen geknüpft und erfüllt den Tatbestand, wenn es sich bei dem zu untersuchenden Sachverhalt um einen solchen handelt, der ein Verbrechen gegen die Menschlichkeit darstellt. Nach Art. 7 Abs. 1 IStGH Statut ist ein solches anzunehmen, wenn es sich um eine der dort aufgezählten Handlungen handelt und diese „im Rahmen eines ausgedehnten oder systematischen Angriffs gegen die Zivilbevölkerung und in Kenntnis des Angriffs begangen wird". Zu den aufgezählten Handlungen gehört etwa nach lit. a die vorsätzliche Tötung, lit. b die Ausrottung oder nach lit. c die Versklavung. Internationale Strafgerichte prüften diese Strafbarkeit etwa in Verfahren der ad-hoc Tribunale für das ehemalige Jugoslawien sowie Ruanda.[38] Dies sowie die aufgezählten Straftaten zeigen, dass es sich bei der begangenen staatlichen Handlung um eine schwerwiegende Straftat als solche handeln muss.

Art. 7 des Römischen Statuts sieht in lit. h allerdings auch dann ein Verbrechen gegen die Menschlichkeit, wenn es sich bei der Tathandlung um eine „Verfolgung einer identifizierbaren Gruppe oder Gemeinschaft aus politischen, rassischen, nationalen, ethnischen, kulturellen oder religiösen Gründen, Gründen des Geschlechts im Sinne des Absatzes 3 oder aus

38 Vgl. näher der Thematik etwa: *Barthe*, Der Straftatbestand der Verbrechen gegen die Menschlichkeit in § 7 VStGB, NStZ 2012, S. 247, 247 f. m.V.a. die internationalen ad hoc Tribunale JStGH und RStGH, die 1993 respektive 1994 jeweils durch Resolutionen des UN-Sicherheitsrats errichtet wurden.

anderen nach dem Völkerrecht universell als unzulässig anerkannten Gründen im Zusammenhang mit einer in diesem Absatz genannten Handlung oder einem der Gerichtsbarkeit des Gerichtshofs unterliegenden Verbrechen" handelt. Daneben besteht der Auffangtatbestand, wonach „andere unmenschliche Handlungen ähnlicher Art, mit denen vorsätzlich große Leiden oder eine schwere Beeinträchtigung der körperlichen Unversehrtheit oder der geistigen oder körperlichen Gesundheit verursacht werden", ebenso ausreichend seien, um den Tatbestand zu erfüllen, vgl. Art. 7 lit. k IStGH Statut. Beide Tathandlungen sind bei der eben geschilderten massenhaften sowie systematischen Überwachung der Gesamtbevölkerung sowie einzelner Gruppen prima facie einschlägig.

Einige der genannten Tatbestandsmerkmale sind in Art. 7 Abs. 2 IStGH Statut genauer definiert. So wird unter dem Begriff der „Verfolgung" nach Art. 7 Abs. 2 lit. g ein „völkerrechtswidriger, vorsätzlicher und schwerwiegender Entzug von Grundrechten wegen der Identität einer Gruppe oder Gemeinschaft" verstanden.

Die handelnden Staaten (in Verbindung mit den privaten Akteuren) müssten zusätzlich auch in den persönlichen Verantwortlichkeitsbereich des Statuts fallen. Innerhalb des Römischen Statuts ist die persönliche Verantwortlichkeit vor dem Internationalen Strafgerichtshofs auf Grundlage des Statuts geregelt. Diese findet sich in Art. 25 Abs. 3 des Römischen Statuts, wonach eine strafrechtliche Verantwortlichkeit auch dann anzunehmen ist, wenn eine Person nach lit. c „zur Erleichterung eines solchen Verbrechens Beihilfe oder sonstige Unterstützung bei seiner Begehung oder versuchten Begehung leistet, einschließlich der Bereitstellung der Mittel für die Begehung". Ebenso ist strafrechtlich verantwortlich nach Art. 25 Abs. 3 lit. d IStGH Statut, wer „auf sonstige Weise zur Begehung oder versuchten Begehung eines solchen Verbrechens durch eine mit einem gemeinsamen Ziel handelnde Gruppe von Personen beiträgt." Natürliche Personen, die für einen Staat oder dessen Organe, alleine oder mittels beauftragten privaten Unternehmen die oben beschriebenen Sachverhalte vornehmen, können somit grundsätzlich im Sinne des Römischen Statuts strafrechtlich verantwortlich sein, wenn die sachlichen Tatbestandvoraussetzungen erfüllt sind.

Schließlich müsste auch – ähnlich wie im nationalen deutschen Recht – der subjektive Tatbestand erfüllt sein, es dürften keine rechtfertigenden sowie schuldausschließenden Gründe vorliegen.

b. Einordnung und Subsumtion

Fraglich ist nun, ob diese potenziell mögliche Strafbarkeit im Einzelnen auch alle Tatbestandvoraussetzungen und die weiteren Voraussetzungen erfüllt, um im Ergebnis eine Strafbarkeit anzunehmen. In Betracht kommt jedenfalls ein Verbrechen gegen die Menschlichkeit nach Art. 7 Abs. 1 lit. h oder k IStGH Statut wegen einer systematischen, massenhaften sowie umfassenden staatlichen Überwachung durch „Cyber Surveillance Instrumente" der Weltbevölkerung sowie besonders überwachter, einzelner Gruppen durch die genutzten Programme.

aa. Rechts- und Deliktsnatur im Allgemeinen

Dazu ist zunächst die Rechts- und Deliktsnatur des Straftatbestands im Allgemeinen zu beleuchten. Verbrechen gegen die Menschlichkeit meinen solche Verbrechen, die als Massenverbrechen anzusehen sind. Die Verbrechen müssen daher systematisch gegen eine bestimmte Bevölkerung begangen werden. Historisch gesehen werden Verbrechen wie die gezielte Ausrottung und die Tötung von Bevölkerungsgruppen, aber auch die Verpflichtung zur Zwangsarbeit, die Deportation von Menschen aus ihren eingesessenen Siedlungsgebieten, das Foltern von politischen Gegnern sowie die massenhafte Vergewaltigung von Frauen und Männern, die systematische Verbringung von Menschen oder die Verfolgung von Bevölkerungsgruppen aufgrund diskriminierender Gesetze erfasst.[39]

Daher stellen gerade die Interessen der Völkergemeinschaft als Ganzes, also deren grundlegende Menschenrechte sowie der Mindeststandard der Regeln mitmenschlicher Existenz, das geschützte Rechtsgut dar.[40] Aus historischer Perspektive sind noch keine Sachverhalte mit digitalem Bezug erörtert worden, was jedoch auch an der mangelnden technischen Entwicklung liegt. Betrachtet man die zuvor beschriebenen Fälle, dann kommt man zu dem Ergebnis, dass die staatlichen Überwachungsmaßnahmen zu schwerwiegenden Bedrohungen der Meinungsfreiheit, der Privatsphäre,

39 MüKoStGB/*Werle/Jeßberger* VStGB § 7 Rn. 2 f. (Kommentierung zum deutschen Völkerstrafgesetzbuch (VStGB), das sich als deutsche Implementierung des Römischen Statuts des Internationalen Strafgerichtshofs sieht und die Ziele sowie Werte der Mutternorm erfüllen soll, wenngleich geringe textliche Abweichungen bestehen.)

40 MüKoStGB/*Werle/Jeßberger* VStGB § 7 Rn. 1.

der Vereinigungsfreiheit und anderer Grundrechte führen (können), was einen Rückzug der Menschen aus dem demokratischen Diskurs mit verheerenden Folgen bedingen kann.[41] Die Maßnahmen haben somit das Potenzial, schwerwiegende Eingriffe in zahlreiche Menschenrechte darzustellen.

Ob diese betroffenen Menschenrechte ausreichen, um den Tatbestand zu erfüllen, kann zum jetzigen Zeitpunkt nicht abschließend bewertet werden. Gerichtliche Entscheidungen des Internationalen Strafgerichtshofs fehlen. Zwar ist bei Schaffung des Art. 7 Römischen Statuts nicht an eine massive „Cyber Surveillance" gedacht worden, da im Wesentlichen andere Schutzgüter, insbesondere die persönliche Freiheit und die körperliche Unversehrtheit, umfasst sein sollen, wie die bisherigen Fälle zeigen. Allerdings hat die Norm offene Elemente, wie nachfolgend genauer dargelegt wird, sodass eine Beeinträchtigung des Schutzbereichs der Norm denkbar ist.

bb. Subjektive und objektive Tatbestandsmerkmale

Demnach müssen sowohl die objektiven als auch die subjektiven Tatbestandsvoraussetzungen vorliegen. Auf objektiver Seite sind „Handlungen [..] im Rahmen eines ausgedehnten oder systematischen [vorsätzlichen] Angriffs gegen die Zivilbevölkerung" nach Art. 7 Abs. 1 Hs. 1 IStGH Statut notwendig.

Das Merkmal der „Ausgedehntheit sowie Systematik" sollte vorliegend anzunehmen sein. Überwachungsmaßnahmen – insbesondere solche, die der Cyber Surveillance zuzurechnen sind – dürften grundsätzlich als ausgedehnt und systematisch eingestuft werden, da sie durch bestimmte staatliche Programme, wie PEGASUS, über einen unbegrenzten Zeitraum sämtliche Online-Kommunikation filtern und auswerten können. Nationalstaatliche Grenzen stellen ebenso wie die Anzahl der überwachten Personen kein Hindernis dar.

Zur Voraussetzung des „Angriffs" lässt sich folgendes festhalten: Fest steht, dass eine militärische Aggression sowie jegliche körperlich wirkende Gewalt gegen die Zivilbevölkerung nicht als notwendig erachtet werden, wenngleich vergangene Fälle eine solche Komponente beinhaltet haben. Daher ist die massive Ausübung von Druck auf eine Zivilbevölkerung ausreichend, wenn sie ausgeübt wird, um sie zu einem bestimmten Verhalten

41 Vgl. *Kaye* (Fn. 37).

zu zwingen. Bereits dann kann von einem Angriff gesprochen werden.[42] Durch eine umfassende sowie dauerhafte Überwachung von nationalen sowie internationalen Bevölkerungsgruppen durch einen staatlichen Akteur kann ein immenser Druck auf die betroffenen Personengruppen ausgeübt werden. Dadurch kann es zu einer Beeinflussung der Verhaltensweisen, etwa einer Vermeidung der Nutzung von online Kommunikation, kommen oder zu anderen Verhaltensweisen, die einen Rückzug aus der öffentlichen Gesellschaft mit sich bringen. Welche besonderen Auswirkungen umfassende Überwachungsmaßnahmen für die Gesellschaft und den einzelnen mit sich bringen, lässt sich an zahlreichen Sachverhalten aus Zeiten der DDR zeigen. Dies ist indes nicht zwingend der Fall, sodass hier nicht eindeutig von einem Angriff gesprochen werden kann. Hier wird eine Auslegung durch die Judikatur maßgeblich sein.

Auf subjektiver Seite ist ein Vorsatz und somit das Wissen und Wollen aller als Tatbestandsvoraussetzung notwendig. Dass die umfassende Nutzung von Spionagesoftware und deren systematische Auswertung eine besonders schwerwiegende Beeinträchtigung von Menschenrechten darstellt, müssen die anwendenden Behörden – auch aufgrund des breiten medialen Diskurses darüber – notwendigerweise wissen, und da solche Software fortwährend eingesetzt wird, nehmen sie diese billigend in Kauf. Der Vorsatz kann insofern angenommen werden.

Daneben müssten die Voraussetzungen nach Art. 7 Abs. 1 lit. h oder k IStGH Statut erfüllt sein. Die Formulierung, wie oben beschrieben, ist recht offengehalten, sodass eine Subsumtion dem Wortlaut nach denkbar wäre:

In Bezug auf Art. 7 Abs. 1 lit. h IStGH Statut geht es um eine Handlung, die auf die Verfolgung einer identifizierbaren Gruppe aus politischen, rassischen, nationalen, ethnischen, kulturellen, religiösen Gründen oder Gründen des Geschlechts gerichtet ist. Es muss sich insofern um eine abgrenzbare Gruppe und nicht die Gesamtbevölkerung handeln. Sofern die umfassende Überwachung die gesamte Bevölkerung eines Landes betreffen würde, wird das Merkmal mangels Bestimmtheit nicht erfüllt sein, da in einem solchen Fall alle Personen betroffen sind, wenngleich auch die Gesamtbevölkerung eine Gruppe darstellt. Allerdings werden Softwares, wie etwa die polizeiliche Software *Palantir,* als rassistisch eingestuft, da

42 MüKoStGB/*Werle/Jeßberger* VStGB § 7 Rn. 23 f. m.V.a. RStGH, Urt. v. 2.9.1998 (Akayesu, TC), para. 581. Vgl. auch RStGH, Urt. v. 6.12.1999 (Rutaganda, TC), para. 68 und RStGH, Urt. v. 27.1.2000 (Musema, TC), para. 205.

sie ethnischen Gruppen besondere Straffälligkeit unterstellen und diese daher häufiger kontrollieren oder es leichter zu einer Festnahme kommt. In solchen Fällen könnte eine Bestimmbarkeit der Gruppe denkbar sein. Allerdings werden hierbei Probleme der Nachweisbarkeit bestehen. Es müsste aufgezeigt werden, dass die Software gerade zur Verfolgung dieser identifizierbaren Gruppe geschaffen wurde, und dies wird in der Praxis nur schwer möglich sein. Zusätzliches Hindernis im Rahmen von Art. 7 Abs. 1 lit. h IStGH Statut ist die Akzessorietät, die der Tatbestand – laut dem Statut des Internationalen Strafgerichtshofs – mit sich bringt. Das bedeutet, dass nur solche Verbrechen umfasst sind, die neben diesem Tatbestandsmerkmal ein weiteres Verbrechen gegen die Menschlichkeit oder einen anderen Tatbestand des Römischen Statuts darstellen.[43] Ziel ist es, die Weite des Tatbestands einzudämmen.[44]

In Bezug auf den Auffangtatbestand des Art. 7 Abs. 1 lit. k IStGH Statut, welcher die Strafbarkeit von „anderen unmenschlichen Handlungen ähnlicher Art, mit denen vorsätzlich große Leiden oder eine schwere Beeinträchtigung der körperlichen Unversehrtheit oder der geistigen oder körperlichen Gesundheit verursacht werden", normiert, lässt sich folgendes festhalten: Obwohl es denkbar und abhängig von der Qualität der Überwachungsmaßnahmen sogar naheliegend sein mag, dass auch Überwachungsmaßnahmen negative Auswirkungen auf die körperliche Integrität haben können, wäre eine solche jedenfalls mittelbar und daher nicht vom Tatbestand des Art. 7 Abs. 1 lit. k IStGH Statut umfasst. Überwachung an sich wird als nicht ausreichend für die Erfüllung des genannten Tatbestandes angesehen, zumal die anderen Einzeltaten gemäß dem Wortlaut der Norm einen unmittelbaren Zwang und eine Beeinträchtigung der körperlichen Unversehrtheit erfordern. Das gilt umso mehr, wenn man die Systematik und den Charakter der Norm betrachtet. Diese kann als Ausnahmetatbestand angesehen werden. Solche werden grundsätzlich eng ausgelegt, sodass mittelbare Eingriffe in die körperliche Unversehrtheit nicht umfasst sein werden.

43 MüKoStGB/*Werle/Jeßberger* VStGB § 7 Rn. 115. Beachtlich ist in diesem Zusammenhang, dass dieses Akzessorietätserfordernis im deutschen Umsetzungsgesetz nicht zu finden ist. Dies ist zutreffend, da dem Tatbestand sonst kein eigener Raum zukommt, zumal eine anderweitige Strafbarkeit jedenfalls immer vorliegen muss. Dieser läuft somit ins Leere. Der deutschen Umsetzungsregelung kommt somit ein strafbarkeitserweitender Anwendungsspielraum zu.

44 MüKoStGB/*Werle/Jeßberger* VStGB § 7 Rn. 115, m.V.a. Ambos/*Hall/Powderly* ICC Statute Art. 7 Rn. 141.

Zusammenfassend ist somit festzuhalten, dass eine eindeutige Betroffenheit der Art. 7 Abs. 1 lit. h oder k des Römischen Statuts nicht anzunehmen ist. Je nach Ausgestaltung des Sachverhalts könnte allerdings zumindest der Art. 7 Abs. 1 lit. h IStGH Statut erfüllt sein, wobei hierbei die Nachweisbarkeit sowie das Akzessorietätserfordernis[45] problematisch sein wird. Zudem wird Überwachung bislang als Teil eines Verbrechens und systematischer Menschenrechtverletzungen angesehen und daher im strafrechtlichen System häufig im Vorbereitungsstadium angesiedelt. Dieser ist nach Art. 7 Römisches Statut nicht unter Strafe gestellt.

Eine Unterscheidung zwischen systematischer Überwachung *an sich* und als Teil und Ermöglichung anderer Tatbestandsmerkmale wäre für eine strafrechtliche Beurteilung allerdings hilfreich und notwendig. Damit gemeint ist, dass eine umfassende Überwachung, sofern sie dem staatlichen oder dem privaten Akteur für die Begehung einer weiteren Straftat dient, zumindest die Nachweisbarkeit für diese weitere Strafbarkeit erhöht. Sie weist aber gleichzeitig auch als solche bereits einen starken Unrechtgehalt auf und sollte daher selbst als strafrechtlich missbilligend eingestuft werden, da hierdurch bereits tiefgehende Eingriffe in Menschenrechte ausgeübt werden. Zudem wäre eine solche Unterscheidung sinnvoll für die Beurteilung des Art. 25 Römisches Statut im Hinblick auf Täterschaft und Teilnahme.

cc. Zwischenergebnis

Eine Betroffenheit des Art. 7 IStGH durch umfassende Überwachungstätigkeiten ist insofern de lege lata daher nicht ausgeschlossen, aber es bestehen einige Bedenken hinsichtlich einzelner Tatbestandmerkmale. Hinzukommt, dass der Artikel aus historischer Sicht nicht auf digitale Verbrechen ausgelegt war, insofern wäre eine weite Auslegung der Tatbestandsmerkmale jedenfalls erforderlich. Ob eine solche Auslegung von den Richter*innen des

45 Dieses Erfordernis wurde jedoch zumindest durch den JStGH, Urt. v. 14.1.2000 (Kupreškić u.a., TC), paras. 580 f.; auch JStGH, Urt. v. 26.2.2001 (Kordić und Čerkez, TC), para. 194 eingedämmt, da der Gerichtshof befand, dass dieses Erfordernis durch den Auffangtatbestand von Art. 7 Abs. 1 lit. h IStGH Statut umgangen werden könne und die Möglichkeit beziehungsweise der Wille des Gesetzgebers des Statuts bestehe, das Völkerrecht fortlaufend weiterzuentwickeln sowie Definitionen anzupassen. Dies wurde mit Art. 10 IStGH Statut begründet.

Internationalen Strafgerichtshofs angenommen wird, kann nicht treffsicher vorausgesagt werden.

c. Ausgewählte Problemfragen im Zusammenhang mit der Strafbarkeit

Daneben stellen sich weitere einzelne Problemfragen, die erörtert werden sollen, wenn über die Etablierung eines Datenwirtschaftsvölkerstrafrechts nachgedacht wird. Diese werden nachfolgend gesondert diskutiert.

aa. Problem 1: Spionage ist völkerrechtlich nicht verboten

Ein Problemkreis ergibt sich daraus, dass Spionage als solche völkerrechtlich nicht verboten ist. Allerdings verstoßen tatsächlich durchgeführte Spionageakte regelmäßig gegen Menschenrechte, wie das Recht auf Privatsphäre aus Art. 12 AEMR und Art 8 EMRK. Daneben sind diese Handlungen zusätzlich in den meisten nationalen Rechtsordnungen strafrechtlich sanktioniert.[46]

In diesem Zusammenhang wird insbesondere auf den Verstoß von Normen aus dem Internationalen Pakt über bürgerliche und politische Rechte (ICCPR) rekurriert, welche sich gerade auf Privatunternehmen beziehen. Spionagesoftware beeinträchtigt zahlreiche Rechte aus diesem Pakt, so etwa das Recht auf Privatsphäre (Art. 17), da der Einzelne nicht bestimmen kann, wer im Besitz von Informationen über ihn ist und wie diese Informationen genutzt werden. Daneben das Recht auf Meinungsfreiheit und freie Meinungsäußerung (Art. 19), zumal potenziell überwachte Personen und deren Umfeld abgeschreckt sind von dem potentiellen Einsatz der Softwaren. Zudem möglicherweise das Versammlungs- bzw. Vereinigungsrecht (Art. 21, 22), wenn Versammlungen durch Abhörung leichter unterbunden werden können. Mittelbar werden das Recht auf Leben (Art. 6), das Verbot von Folter (Art. 7), willkürliche Festnahmen (Art. 9) und das Recht auf Freizügigkeit (Art. 12) und ein ordnungsgemäßes Verfahren (Art. 14) beeinträchtigt, wenn man den Untersuchungen von Citizen Lab, Amnesty International, Mexico's R3D und ARTICLE 19 folgt.[47] Solche Beeinträchtigungen müssen, ähnlich wie im deutschen sowie unionalen Recht, auf-

46 *Schaller*, Spies, Oxford Public International Law, 2015, s. 2, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e295?prd=MPIL.

47 *Kaye* (Fn. 37).

grund des Pakts gerechtfertigt werden, also jedenfalls verhältnismäßig sein. Innerhalb der Verhältnismäßigkeitsprüfung ergeben sich insbesondere Bedenken hinsichtlich des relativ mildesten Mittels. Strafverfolgungs- oder Sicherheitsdienstbehörden steht meistens eine weniger restriktive, alternative Ermittlungsmethode zur Verfügung. Zudem ist es Staaten nicht bzw. begrenzt möglich, den Einsatz von Spionagesoftware nur auf verhältnismäßige Fälle zu begrenzen, da eine Verhältnismäßigkeit im Einzelfall häufig erst ex post bestimmt werden kann.

Daher stellt sich die Frage, ob solche Software generell als rechtswidrig einzustufen ist, wie dies etwa *David Kaye* in dem dazugehörigen Untersuchungsausschuss gefordert hat. Fraglich ist jedoch, ob und inwiefern ein politischer Wille zu einer solchen Einstufung besteht.

Daneben sind Verstöße gegen Art. 8 EMRK denkbar. Diese können indes nur durch die Vertragsstaaten, also im Fall von PEGASUS durch Großbritannien, begangen werden. Begründet werden könnte ein Eingriff damit, dass Personen wegen der Überwachung ihrer Kommunikation von Meinungsäußerungen abgehalten werden könnten („chilling effect"). Auch dieser Eingriff müsste durch ein Gesetz gerechtfertigt werden sowie verhältnismäßig sein. Großbritannien hat in Zusammenhang mit dem Einsatz von TEMPORA durch GCHQ ein Gesetz erlassen. Dieses hat der EGMR allerdings als rechtswidrig eingestuft, da es an Bestimmtheit fehle. Das Gesetz sah vor, dass „ein Minister anordnen durfte und wohl auch angeordnet hatte, alle Datenströme in allen Unterseekabeln, die eine britische Station haben, zu überwachen und im Hinblick auf die nationale Sicherheit und das wirtschaftliche Wohlergehen des Landes zu durchsuchen". Dies sei nach Ansicht des EGMR rechtswidrig, weil die Befugnisse zu weitreichend seien und anlasslos erscheinen. Zudem würden etwa Vorschriften zur Festlegung von Suchbegriffen fehlen.[48] Dieses Urteil zeigt, dass Spionage nach Ansicht des EGMR nur unter bestimmten sowie engen Voraussetzungen möglich sein darf, wenngleich einzelne Staaten – vielleicht auch mangels Vollstreckungskompetenz des EGMR – dem keine Folge leisten.

Insofern ist festzuhalten, dass Spionage unter gewissen Umständen aus völkerrechtlicher Sicht gegen Menschenrechte verstößt und somit zumindest mittelbar „verboten" ist, zumal es als rechtwidrig einzustufen ist. Dies

48 Vgl. EGMR, Urt. v. 1.7. 2008 – 58243/00 Rn. 43 ff., 64 ff. – Liberty u. a./Vereinigtes Königreich unter Hinweis auf EGMR, NJW 2007, 1433; untersucht bei: *Ewer/Thienel* (Fn. 7), S. 32 f.

gilt insbesondere, wenn Privatpersonen, die sonst als unauffällig im strafrechtlichen Sinne einzustufen sind, „ausspioniert" werden.

bb. Problem 2: Das Geschäftsmodell der globalen Datenwirtschaft ist auf die systematische Überwachung gerichtet

Ein weiterer Problemkreis besteht darin, dass das Geschäftsmodell der globalen Digitalunternehmen gerade auf die systematische Überwachung von Daten gerichtet ist, um diese dann möglichst lukrativ im wirtschaftlichen Sinne zu nutzen. Je mehr Daten generiert werden, desto höher sind grundsätzlich auch die damit erzielten Gewinne. Wie bereits oben beschrieben, haben auch Staaten den Nutzen der Überwachung durch umfassende Datenwirtschaft erkannt.

Als pauschale Rechtfertigung aus staatlicher sowie aus Sicht der Unternehmen wird dabei folgendes angeführt: Ein solches Werkzeug ist notwendig, um Terrorismus oder andere Bedrohungen der nationalen Sicherheit und der öffentlichen Ordnung zu filtern und in einem zweiten Schritt zu bekämpfen. Die genaue Funktionsweise der Systeme, die eine umfassende Überwachung ermöglichen – so eine Zeugenaussage des „General Counsel" der NSO Group im Rahmen des PEGASUS Komitee –, könne aufgrund von Staatsgeheimnissen sowie vertraglichen Abreden nicht erfolgen. Auch Fragen danach, wo die Software eingesetzt wird und wer weiterhin Zugriff auf die gesammelten Daten und das System hat, wurden unbeantwortet gelassen.[49]

Aufgrund der Schwere der Bedrohungen, die von einem solchen Überwachungseingriff für das private Leben des Einzelnen und die demokratische Gesellschaft ausgeht, wie oben eingehend dargelegt, ist von Seiten des Gesetzgebers und den entwickelnden Unternehmen eine Rechtfertigung dieser Rechtsbeeinträchtigung notwendig. Eine Interessenabwägung reicht insofern nicht aus, vielmehr ist eine ausführliche Rechtfertigung der Beeinträchtigung notwendig. Eine solche Rechtfertigung samt nachvollziehbaren Beweisen, warum solche Softwares zum Einsatz kommen und wie diese die positivrechtlichen Verpflichtungen zur Einhaltung der Menschenrechte erfüllen, wird – zumindest im PEGASUS Verfahren der EU – weiterhin

49 So *Hannah Neumann*, die Teil des PEGASUS-Untersuchungsausschusses ist, https://hannahneumann.eu/pegasus-untersuchungsausschuss-update-vor-der-sommerpause.

nicht gegeben.[50] Insbesondere wird nicht dargelegt, inwiefern der Einsatz einer umfassenden Spionagesoftware im Rahmen der Verhältnismäßigkeit das relativ mildeste Mittel darstellt.[51]

Die Bindung an die Grundrechte wird auch für die die Software entwickelnden Unternehmen anzunehmen sein, da eine gewisse Bindung von Unternehmen an Menschenrechte bestehen wird. Die horizontale Wirkung dieser ist in gewissem Umfang allgemein anerkannt, wie etwa die Leitprinzipien der Vereinten Nationen für Wirtschaft und Menschenrechte zeigen. Danach sollen auch Unternehmen die Menschenrechte im Rahmen ihrer Arbeitstätigkeit achten. Konkret sollen sie vermeiden, die Menschenrechte anderer zu beeinträchtigen und nachteiligen menschenrechtlichen Auswirkungen, die aufgrund ihrer Arbeit entstehen, begegnen, wenngleich dadurch ihre Geschäftstätigkeit und somit auch ihre unternehmerische Freiheit eingeschränkt wird.[52]

IV. Fazit und Ausblick

Staatliche, aber auch private Überwachungsmaßnahmen können durch die digitale Entwicklung immer präziser sowie umfassender werden. Einerseits können mehr Daten erfasst, diese besser ausgewertet, aber auch einfacher und länger gespeichert werden.

Diese Erwirtschaftung von Daten stellt das Geschäftsmodell von zahlreichen Digitalunternehmen dar. Das Potenzial dieser Technik haben mittlerweile auch Staaten erkannt. Diese nutzen die Technologie mit Hilfe privater Akteure, um eine umfassende Überwachung von (Teilen der) weltweiten Bevölkerung durchzuführen. Dies haben Sachverhalten rund um PEGASUS, Prism, Echelon oder Hacking Team gezeigt.

Im Ergebnis lässt sich aus rechtlicher Sicht aber festhalten, dass der Rechtsbereich eines Datenwirtschaftsvölkerstrafrechts de lege lata für solche Sachverhalte nicht eindeutig hergeleitet werden kann. In Betracht kommt unter gewissen Umständen eine Strafbarkeit von Einzelpersonen, die für Staaten tätig werden, wenn diese systematische, umfassende Überwachungsmaßnahmen durch Softwares wie PEGASUS gegenüber gewissen

50 Vgl. zur Argumentation: *Kaye* (Fn. 37).

51 *Kaye* (Fn. 37).

52 Vgl. etwa Berichtsrahmen für die UN-Leitprinzipien für Wirtschaft und Menschenrechte mit Umsetzungshinweisen, www.ungpreporting.org/wp-content/uploads/UNGPRF_Deutsch_Dez2017.pdf.

Bevölkerungsgruppen durchführen. Eine Verantwortlichkeit würde sich dabei gegebenenfalls aus Art. 7 Abs. 2 IStGH Statut ergeben. Aufgrund fehlender Judikatur in diesem Bereich ist das Annehmen einer solchen Strafbarkeit zum jetzigen Zeitpunkt ungewiss. Allerdings kommen beim Einsatz solch tiefgehender Spionagesoftware zahlreiche Beeinträchtigungen von Menschenrechten in Betracht, die nicht rechtfertigbar sind und somit einen Verstoß darstellen. Einschränkungen zeigen sich insoweit beim Recht auf Meinungsfreiheit und freie Meinungsäußerung sowie auch möglicherweise in Bezug auf das Versammlungs- bzw. Vereinigungsrecht; mittelbar sind im Einzelfall aber auch das Recht auf Leben, das Verbot von Folter, willkürliche Festnahmen sowie das Recht auf Freizügigkeit und das ordnungsgemäße Verfahren betroffen. Die Einschränkungen können sohin als besonders schwerwiegend eingestuft werden.

Gesetzgebungsvorhaben oder die Etablierung von völkerrechtlichen Abreden sind dennoch nicht ersichtlich. Im zivilrechtlichen Bereich zeigen sich insbesondere im unionalen Raum Tendenzen zu mehr Verantwortlichkeit von Unternehmen und zur Etablierung eines Datenwirtschaftsrechts, wonach sich zumindest zivilrechtliche Folgen, insbesondere eine hohe Besteuerung, ergeben sollen, wenn Unternehmen im erheblichen Maße Daten erwirtschaften und vermarkten, die gesellschaftlich betrachtet von geringem Wert sind. Nicht so tiefgreifend wie innerhalb der EU, aber dennoch in gewissem Maße, zeigen sich darüber hinaus Tendenzen zu mehr Verantwortlichkeit bei der Erwirtschaftung von Daten im globalen Umfeld.

Es bleibt also abzuwarten, ob sich auch die Staaten der Welt ihrer Verantwortung bewusst werden, die Möglichkeit einer umfassenden Überwachung von weiten Teilen der Bevölkerung einzuschränken und gegebenenfalls sogar strafrechtlich zu sanktionieren. Eine Untersagung solch umfassender Überwachungsmechanismen dauerhaft wäre unterdessen rechtlich geboten und darüber hinaus wünschenswert, so wie *David Kaye* dies im Rahmen seiner Anhörung innerhalb des PEGASUS-Untersuchungsausschusses geschildert hat.[53] Dass neue große Sprachmodelle mit KI-Fähigkeiten, sowie Quantencomputing, die Überwachungsfähigkeiten nur verstärken, unterstreicht die Dringlichkeit menschenrechtsbasierter Regulierung.

53 Vgl. zur Argumentation: *Kaye* (Fn. 37).