

# „Daten(wirtschafts)völkerstrafrecht“. Eine begriffliche Annäherung

*Andreas Werkmeister & Julia Geneuss*

## *I. Einleitung*

„Brauchen wir ein Daten(wirtschafts)völkerstrafrecht?“ ist der Titel dieses Bandes. Aber was meinen wir eigentlich mit Datenvölkerstrafrecht bzw. Datenwirtschaftsvölkerstrafrecht?

Der Begriff des „Daten(wirtschafts)völkerstrafrechts“ greift offensichtlich recht unterschiedliche Begriffselemente auf. Man bezieht sich bzgl. der „Völkerstrafrechtskomponente“ zunächst auf das etablierte Völkerstrafrecht. Bezüglich der „Wirtschaftskomponente“ knüpft man an die insbesondere von *Florian Jeßberger* initiierte Diskussion um ein sog. Wirtschaftsvölkerstrafrecht<sup>1</sup> an, welche wiederum eng verbunden ist mit der Diskussion um den von *Wolfgang Naucke* geprägten weiter gefassten Begriff der „politischen Wirtschaftsstraftat“,<sup>2</sup> der später sogar über die Wirtschaft hinaus zu einem „machtverneinenden Strafrecht“<sup>3</sup> ausgebaut worden ist. Mit der Komponente der „Daten“ wird schließlich die Frontstellung der datenschützenden Menschenrechte gegen systematische (digitale) Überwachung einerseits sowie das nationale Datenschutzstrafrecht andererseits aufgegriffen.

Mit dem Begriff des Daten(wirtschafts)völkerstrafrecht sollen die erwähnten Komponenten nun in gewisser Weise alle verknüpft werden. An dieser Stelle ist indes zunächst eine Systematisierung von Nöten, um von den vorläufig nur lose zusammenhängenden Aspekten zu einem immerhin einigermaßen konturierten Begriff zu gelangen. Im Folgenden sollen zu diesem Zweck zwei begriffliche Dimension unterschieden werden: eine engere, sich in den (wirtschafts-)völkerstrafrechtlichen Bahnen bewegende

---

1 Zuerst *Jeßberger*, Die I.G. Farben vor Gericht: Von den Ursprüngen eines „Wirtschaftsvölkerstrafrechts“, JZ 2009, S. 924, 930 ff.; ausführlich sodann der Band von *Jeßberger/Kaleck/Singelnstein* (Hrsg.), Wirtschaftsvölkerstrafrecht, 2015; in der Folge monographisch u.a. bearbeitet von *Ambos*, Wirtschaftsvölkerstrafrecht, 2018.

2 *Naucke*, Der Begriff der politischen Wirtschaftsstraftat, 2012.

3 *Naucke*, Negatives Strafrecht, 2015, S. 119.

(dazu II.) und eine weitere den von *Naucke* geprägten machtverneinenden Aspekt betonende (dazu III.). In einem Ausblick (dazu IV.) werden ausgehend davon die offenen Fragen, die für den vorliegenden Bandes prägend waren, skizziert.

## II. Daten(wirtschafts)völkerstrafrecht und die Systematik des Völkerstrafrechts

In einer ersten und strengen Dimension handelt es sich beim „Daten(wirtschafts)völkerstrafrecht“ um einen eng geführten Begriff, bei dem das *geltende Völkerstrafrecht* die begriffliche Klammer bildet. Das geltende Völkerstrafrecht erfasst – sei es nun auf internationaler Ebene, das heißt wie es von internationalen Strafgerichten praktiziert wird, oder auch auf nationaler Ebene, wie bspw. in Deutschland mit dem Völkerstrafgesetzbuch – über die vier sog. Kernverbrechen (also Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen und das Verbrechen der Aggression) primär massenhaft und systematisch ausgeübte Gewaltkriminalität. Die Pönalisierung der Gewalthandlungen erfolgt unmittelbar durch die Völkerrechtsordnung.

Von seinen historischen Ursprüngen her betrachtet, soll Völkerstrafrecht in erster Linie staatsverstärkte Kriminalität<sup>4</sup> erfassen. Von diesem traditionellen Verständnis des Völkerstrafrechts ausgehend, könnte man von *Datenvölkerstrafrecht* insoweit nur sprechen, wenn auf datengestützte Mittel zurückgegriffen wird, um solche staatsverstärkten Gewaltdelikte zu verwirklichen. An Beispielen für eine derartige Fallkonstellationen mangelt es jedoch nicht; genannt werden kann etwa die Lieferung von Überwachungstechnik an einen kriminellen Unrechtsstaat oder auch die Befeuerung der Hassspirale, die den Völkermord an den Rohingya in Myanmar trieb, durch Algorithmen, was Facebook vorgeworfen wird. Da diese Vereinfachung oder Unterstützung völkerstrafrechtsrelevanter Gewaltverbrechen regelmäßig von privaten Unternehmen, also Akteuren aus der Wirtschaft ausgeht, handelt es sich zudem um einen Aspekt des „*Wirtschaftsvölkerstrafrechts*“.

---

4 Dazu auch wieder wichtig: *Naucke*, Die strafjuristische Privelegierung staatsverstärkter Kriminalität, 1996.

### III. Daten(wirtschafts)völkerstrafrecht als datenmachtverneinendes politisches Strafrecht

#### 1. Begrifflicher Ausgangspunkt

Wir wollen jedoch über diese engere Dimension des „Daten(wirtschafts)völkerstrafrechts“ hinausgehen. *Werkmeister* hatte mit einem Fokus auf die Wirtschaft bereits vorgeschlagen in Anknüpfung an *Naucke* eine weiter gefasste „politische Datenwirtschaftsstraftat“ zu konzeptionalisieren.<sup>5</sup> Diskutieren wollen wir in diesem Sinne – auch jenseits der Wirtschaft – ein datenmachtverneinendes „politisches“ Strafrecht. Gemeint sind damit systematische Datenschutzverletzungen, die von den Inhabern staatlicher oder wirtschaftlicher Macht ausgehen, und die sich – wie *Naucke* es formuliert hat – dadurch auszeichnen, dass sie „durch ihre Stärke Freiheit überwältigen“.<sup>6</sup> Im Kern geht es insoweit um Sachverhalte wie den NSA-Skandal oder den Facebook-Cambridge-Analytica-Fall. Der damit angedeutete Begriff eines Datenvölkerstrafrechts bzw. Datenwirtschaftsvölkerstrafrecht ist zunächst deshalb *weiter*, weil er über die Kernverbrechen – und damit auch über die diesen überwiegend zu Grunde liegende Gewaltkomponente: Völkerrechtsverbrechen als „atrocity crimes“ – hinausweist. Er ist aber zugleich in einem bestimmten Sinne *enger*, wenn man nämlich speziell auf die *Datenkomponente* fokussiert. Denn insoweit geht es nun auch um die Strafbarkeit und Strafwürdigkeit von datenbezogenen Akten *an sich*, also ohne Bezug zu Gewaltstraftaten wie den Kernverbrechen oder sonstigen Menschenrechtsverletzungen. Hier kann man also die Frage stellen, inwieweit „elektronische Überwachung“ als *eigene Macht* strafrechtlich in den Blick genommen werden kann und muss.

#### 2. Zwischen nationalem Datenschutzstrafrecht und Völkerstrafrecht

##### a. Völkerstrafrechtsähnliches Rechtsgut?

Das geltende, *nationale* Strafrecht macht eine Ahndung von Datenschutzverletzungen über verschiedene Tatbestände auch des Nebenstrafrechts na-

---

5 *Werkmeister*, Erste Überlegungen zum Begriff der „politischen Datenwirtschaftsstraftat“, GA 2021, S. 570 ff.

6 *Naucke* (Fn. 2), S. 4.

türlich vom Prinzip her bereits möglich. Es fokussiert sich aber – so die Hypothese<sup>7</sup> – auf einzelne missbräuchliche Datenverarbeitungsvorgänge, nicht „völkerstrafrechtsähnlich“ auf die *systematischen* Regelbrüche, um die es uns im Kern geht.

Die Ähnlichkeit systematischer Datenschutzverletzungen zu den etablierten völkerrechtlichen Kernverbrechen ist hier freilich noch zu konkretisieren und kritisch zu diskutieren – wozu die Beiträge in diesem Band Ansatzpunkte liefern sollen. Neben der rein internationalen Dimension, die derartigen systematischen Datenverbrechen schon rein faktisch immanent ist und jedenfalls eine inter- bzw. transnationalstrafrechtliche Reaktion zu erfordern scheint, lässt sich – auch das eine Hypothese – der Gedanke der „Völkerstrafrechtsähnlichkeit“ systematischer Regelbrüche über das betroffene Rechtsgut und die Eingriffsbreite und -tiefe rechtfertigen.

## b. Überwachung und Freiheit

Für die Rechtsgutsstruktur eines solchen Datenvölkerstrafrechts zentral ist der enge Zusammenhang von Überwachung und Freiheit; es geht um Taten die durch ihre Stärke Freiheit überwältigen. Wenn auch durch Überwachung niemand zu Tode kommt, und sich daher eigentlich die Analogie zu den Kernverbrechen verbietet, ist dennoch zu beachten: ein freies Leben ist unter Bedingungen einer vollständigen Überwachung unmöglich. Das prägte auch die grund- und menschenrechtliche Entwicklung. Bereits als das Bundesverfassungsgericht im Volkszählungsurteil 1983 die Grundlagen für das Grundrecht auf informationelle Selbstbestimmung legte, hob es genau das hervor: Freiheit im Sinne von Entfaltungsfreiheit braucht Freiheit von Überwachung. Das Bundesverfassungsgericht hat das so formuliert:

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“<sup>8</sup>

---

7 Dazu bereits die Überlegungen bei *Werkmeister* (Fn. 5), S. 581 ff.

8 BVerfGE 65, 1, 43.

Hier denkt man vielleicht gar nicht mal primär an die heutige Internetgesellschaft, sondern an Überwachungsdictaturen der Vergangenheit und Gegenwart, in denen eine drohende Zwangsgewalt für Anpassung an die „erwarteten Verhaltensmuster“ sorgte. Genannt werden kann das Beispiel der Stasi, die zum Symbol des Unrechtscharakters der DDR geworden ist; nebenbei: ist aber das Stasi-Überwachungsunrecht als systematisches Unrecht erfasst und strafrechtlich aufgearbeitet worden? Nein. Eine Anklage an die führenden Urheber der „ausgedehnten und systematischen ‚Datenangriffe‘ gegen die Zivilbevölkerung“ – wie es sich in Anlehnung an die Gesamttat der Verbrechen gegen die Menschlichkeit formulieren ließe – gab es nicht.

### c. Instrumentäre Macht (Zuboff)

Vor dem Hintergrund der Digitalisierung und Verdatung der Welt erhält nun der Zusammenhang von Überwachung und Freiheit eine weitere Facette. Glaubt man nämlich der auch für unsere Fragestellung durchaus impulsgebende Theoretikerin des sog. Überwachungskapitalismus *Shoshana Zuboff* dann sind quasi-allwissende digitale Großkonzerne die zentralen Player des 21. Jahrhunderts. Als vermeintliches Nebenprodukt aus Diensten wie Suchmaschinen oder Freundesnetzwerken haben sie alles über uns erfahren, und veräußern dies nun gewinnbringend an andere Unternehmen – oder auch den Staat? –, damit auch diese wissen bzw. dieser weiß, was uns gefällt. Nach *Zuboffs* Narrativ ist auf diese Weise schleichend eine nach Allwissenheit strebende sog. „instrumentäre Macht“ zum Vorschein gekommen, die nicht nur alles weiß, sondern auch dazu neigt, uns mit „Verhaltensmodifikationsmitteln“ wie einen Menschenschwarm zu lenken. *Zuboff* zieht hier im Hinblick auf die freiheitsaufhebende Dimensionen explizit einen Vergleich mit totalitären Unrechtsstaaten: „Operiert der Totalitarismus durch Gewaltmittel, operiert instrumentäre Macht durch Mittel zur Verhaltensmodifikation“.<sup>9</sup> Ihr zufolge geht es heute also nicht mehr nur um einen Chilling-Effect für die Entfaltungsfreiheit, sondern es steht schon die Entscheidungsfreiheit selbst auf dem Spiel. Nicht wir entscheiden über unser Leben, so ihre These, sondern diejenigen, die sich das Wissen über uns aneignen, und unser Verhalten durch dieses Wissen per Verhaltensmodifikationsmittel lenken können.

---

<sup>9</sup> *Zuboff*, Das Zeitalter des Überwachungskapitalismus, 2018, S. 420 f.

Die Idee eines Daten(wirtschafts)völkerstrafrechts – verstanden im weiteren Sinne – zehrt von diesem Narrativ,<sup>10</sup> nähert sich den sehr zugespitzten Thesen aber doch nur teilweise an. Es geht hier ja nicht zuerst um die gesellschaftstheoretische Diagnose, das heißt um die Deutung von „*konformen*“ Verhaltensweisen als totalitär, sondern um eine strafrechtstheoretische These, die noch einmal bestimmte Verhaltensweisen identifiziert, die selbst von den weitgehend praktizierten, von Zuboff kritisierten, sozialen Normen noch einmal deutlich abweichen. Im Zentrum stehen, wie gesagt, pointierte Geschehnisse, die, wie bei NSA – also von staatlicher Seite – oder Cambridge Analytica – also von wirtschaftlicher Seite, ein Überwachungsinstrumentarium zum Vorschein kommen lassen, das aus menschenrechtlicher Sicht kritikwürdig ist, das aber strafrechtlich kaum geahndet wird.

Was also tun? NSA, Facebook und Google verbieten? Nein, es geht darum eine kluge und menschenrechtlich fundierte Spielregel zu finden und zwar für Datenstaat und Datenwirtschaft. Die Essenz dieser Spielregel und eines im Entstehen begriffenen, möglicherweise universalisierbaren Unrechtsbewusstseins könnte sich aus einer Kombination von Eingriffsbreite und Eingriffstiefe ergeben:<sup>11</sup> die *systematische* Erstellung und Nutzung von Persönlichkeitsprofilen von uns allen, die auch vor unserem innersten Selbst, insbesondere vor unserer politischen oder sexuellen Orientierung, keinen Halt machen, darf es nicht geben und zwar weder um damit Geld zu verdienen, noch um uns als Staatsbürger zu verwalten. Hält man dies nicht ein, machen sich auch und gerade die Mächtigen strafbar. Ist das eine tragfähige theoretische und strafrechtliche These?

#### IV. Ausblick

Dieser Band kann freilich nur der Auftakt sein, um das zweidimensionale Feld des „Daten(wirtschafts)völkerstrafrechts“ näher zu vermessen. Anschließend an diese Begriffsbestimmung haben sich für uns vorläufig insbesondere drei Fragen aufgedrängt:

Zum einen, in einem ersten Schritt, die verschiedenen Facetten und Dimensionen, die mit dem Begriff und Konzept eines „Daten(wirtschafts)völkerstrafrechts“ verbunden sind, präzise herausarbeiten; die Gefährdungs-

---

10 Dies im Zusammenhang der „politischen Datenwirtschaftsstrafat“ aufgreifend *Werkmeister* (Fn. 5), S. 572 ff.

11 S. dazu die Ansätze bei *Werkmeister* (Fn. 5), S. 582 ff.

gen systematisieren; und vor allem auch das bzw. die von „Datenverbrechen“ betroffenen Schutzgüter fassen.

Zweitens zu überlegen, ob das Strafrecht zum Schutz dieser Güter überhaupt etwas leisten kann und sollte.

Und schließlich: sofern das Strafrecht einen Beitrag leisten kann, ob es dann nicht zwangsläufig internationaler, das heißt völkerstrafrechtlicher oder zumindest transnationalstrafrechtlicher Regelungen bedarf, um die globale Dimension des Phänomens oder gar das über die Systematik der Rechtsverletzungen bestehende „völkerstrafrechtsähnliche“ Globalunrecht zu erfassen. Konkreter geht es hier darum, die „internationale“ Dimension von Datenverbrechen zu erfassen und zu beschreiben, um auch daraus Folgen für mögliche Regelungstechniken abzuleiten.

