Überwachungsunrecht und Völkerstrafrecht

Till Zimmermann

I. Einleitung

Der Diktator Big Brother aus *George Orwells* „1984" hat keinen sonderlich guten Ruf. Zu Recht. Staaten, die alles über ihre Bürger wissen (wollen), verhalten sich aus Sicht des normativen Individualismus[1] illegitim.[2] Die ins Werk gesetzte Sättigung monströsen Datenhungers wird entsprechend als (schweres) Unrecht wahrgenommen.

Historische Exempel sind das elaborierte Spitzelsystem der nationalsozialistischen Geheimpolizei[3] und der mit einem „flächendeckenden Spitzelsystem" operierende „Überwachungsstaat" der Deutschen Demokratischen Republik.[4] Ein Beispiel der Gegenwart ist das kontinental-chinesische Sozialkredit-System.[5] Dieses setzt die Bürger einer radikalen (gegenseitigen) Beobachtung aus und teilt die Menschen entsprechend ihrer Verhaltensqualität in moralische Klassen ein (von „AAA" bis zu „D-"); die Sanktionen für

1 Zum Begriff *v.d. Pfordten*, Normativer Individualismus, ZphilF 58 (2004), S. 321; *ders.*, Normativer Individualismus und das Recht, JZ 2005, S. 1069 ff.

2 Dasselbe gilt im Grundsatz auch für datensammelwütige Privatunternehmen. Die damit verbundenen Spezialprobleme bleiben in diesem Beitrag ausgeklammert.

3 Vgl. *Weyrauch*, Gestapo V-Leute – Tatsachen und Theorie des Geheimdienstes, 1992.

4 *Zimmermann/Dörr*, Gesichter des Bösen, 2015, S. 105; vgl. auch *Lichter/Löffler/Siegloch*, The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany, JEEA 19 (2021), S. 741 ff.; *Schaar*, Lehren aus der Stasi-Überwachung, bpb.de v. 17.1.2017, www.bpb.de/themen/deutsche-teilung/stasi/222810/lehren-aus-der-stasi-ueberwachung.

5 *Staatsrat der Republik China*, Planning Outline for the Construction of a Social Credit System (2014–2020), veröff. am 14.6.2014, inoffizielle Übersetzung; abrufbar über China Copyright and Media: https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020. Dazu etwa *Lee*, Die AAA-Bürger, Zeit-Online v. 30.11.2017, www.zeit.de/digital/datenschutz/2017-11/china-social-credit-system-buergerbewertung/komplettansicht; *Dorloff*, Guter Bürger, schlechter Bürger, Deutschlandfunk.de v. 19.4.2018, www.deutschlandfunk.de/china-guter-buerger-schlechter-buerger-102.html; *Noesselt*, Chinas Sozialkreditsysteme. Technokratie-Experimente im Schatten des digitalen Staatskapitalismus, GWP 2/2022, S. 205 ff.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

deviantes Verhalten im chinesischen System beschreibt *Markus Abraham* wie folgt:

> „So kann die Nutzung von Nachtzügen und Reisen erster Klasse, Sternelokalen und -hotels, der Zugang zu Privatschulen, der Erwerb von Versicherungs-Produkten mit Kapitalwert, sowie Hausbau und Renovierung untersagt werden."[6]

Das chinesische Sozialsteuerungsinstrument mag sich zwar noch in einer Experimentalphase befinden[7] und in seinen Auswirkungen auf die betroffenen Individuen einigermaßen weit entfernt sein von seiner fiktiven dystopischen Ausbuchstabierung in Literatur und Film.[8] Aber schon 2019 bemerkte *Kostka*, dass

> „[f]ast jeder fünfte Chinese bereits andere Dinge im Internet verbreitet [hat], als er oder sie es in einer unbewerteten Situation getan hätten, um einen negativen Einfluss auf die eigene Sozialkreditbewertung zu vermeiden."[9]

6 *Abraham*, Gesellschaftssteuerung durch Reputationssysteme, in Fritsche et al. (Hrsg.), Unsicherheiten des Rechts. ARSP-Beiheft 162, 2020, S. 155, 159.

7 Für eine Entdramatisierung der Entwicklung plädieren etwa *Brussee*, China's social credit score – untangling myth from reality, Merics.org v. 11.2.2022, https://merics.org/de/kommentar/chinas-social-credit-score-untangling-myth-reality und – sehr apologetisch – *Hernig*, Errichtet China eine Big-Data-Diktatur? Nein., Die Republik v. 4.10.2018, www.republik.ch/2018/10/04/errichtet-china-die-erste-big-data-diktatur-des-21-jahrhunderts-nein. Überlegungen zu einem rechtsstaatlich vertretbaren Reputationssystem finden sich bei Abraham (Fn. 6).

8 Der satirische Roman QualityLand von *Marc-Uwe Kling* (2007) beschreibt eine mithilfe eines zentralen Sozialkreditsystems organisierte Gesellschaft, in der jedem Bürger ein veränderliches „Level" zwischen 1 und 100 zugewiesen ist; Menschen mit einstelligem Level gelten als „Nutzlose" und sind von der gesellschaftlichen Teilhabe weitgehend ausgeschlossen. Die Episode „Abgestürzt" der TV-Serie Black Mirror (2016; Regie: *Joe Wright*) beschreibt eine Welt, in der die Menschen durch gegenseitige Bewertung mit 1 bis 5 Punkten ihren individuellen Sozialpunktewert ermitteln; dieser entscheidet über die Möglichkeiten gesellschaftlicher Teilhabe.

9 *Kostka*, Sozialkreditsystem in China – Totale Kontrolle oder Schließung regulatorischer Lücken?, NG/FH 10/2019, S. 22, www.frankfurter-hefte.de/artikel/totale-kontrolle-oder-schliessung-regulatorischer-luecken-2817.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Zudem gibt es Anhaltspunkte dafür, dass bei der gewaltsamen Unterdrückung der uigurischen Bevölkerung in der VR China technologische Instrumente zur Sozialkontrolle eine wichtige Rolle spielen.[10]

Vor diesem Hintergrund erscheint es diskutabel, solchermaßen extreme staatliche Datensammelexzesse auch als völkerstrafrechtliches Unrecht zu brandmarken (und idealerweise zu ahnden). Im Folgenden geht es (nur) um eine Spezialfrage, die in dieser Diskussion eine Rolle spielt: Diejenige nach dem Deliktscharakter eines Tatbestands, der das Unwesen staatlicher Datenkraken pönalisiert. Dabei werden insbesondere Denkanstöße aus der deutschen verfassungsrechtlichen Debatte für die (völker-)strafrechtliche Diskussion fruchtbar zu machen versucht.

II. Dateneingriffe und Überwachungsunrecht

Die (strafrechtsethische) Frage, worin genau das Schädliche bzw. das rechtsgutsbeeinträchtigende Unrecht des massenhaften und grenzenlosen Sammelns personenbezogener Daten liegt, ist wenig geklärt. Weitgehend unstreitig ist immerhin (zumindest aus europäischer Perspektive), *dass* es ein Grund- bzw. Menschenrecht auf informationelle Selbstbestimmung gibt – verortet in Art. 2 I i.V.m. Art. 1 GG[11] und Art. 8 EMRK[12] sowie ausdrücklich normiert in Art. 16 I AEUV und Art. 8 GRC. Dieses „Grundrecht auf Datenschutz"[13], so das BVerfG, „gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[14]

Klar ist ferner, dass das Recht auf informationelle Selbstbestimmung durch staatliche Datenverarbeitung („Dateneingriffe")[15] in verfassungs-

10 *Human Rights Watch*, China's Algorithms of Repression – Reverse Engineering a Xinjiang Police Mass Surveillance App, 2019, www.hrw.org/sites/default/files/report_pdf/china0519_web5.pdf.

11 BVerfGE 65, 1 ff.; krit. etwa *Behrendt*, Entzauberung des Rechts auf informationelle Selbstbestimmung, 2023.

12 Calliess/Ruffert/*Kingreen*, EUV/AEUV, 6. Aufl. 2022, Art. 8 GRC Rn. 5; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, 7. Aufl. 2021, § 22 Rn. 10.

13 So BVerfG, NJW 1991, 2129, 2132.

14 BVerfGE 65, 1 Ls. 1.

15 Näher Lisken/Denninger/*Schwabenbauer*, Handbuch des Polizeirechts, 7. Aufl. 2021, Kap. G. Rn. 20 ff.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

rechtlich-technischer Hinsicht *verletzt* werden kann.[16] Allerdings ist ein grundrechts*verletzender Eingriff* nicht dasselbe wie eine Rechtsguts- bzw. Interessen*verletzung*[17] im strafrechtsdogmatischen Sinne; so kann nämlich auch eine bloße Lebens*gefährdung* (im strafrechtlichen Sinne) nach der grundrechtlichen Terminologie eine „Verletzung" des Lebensgrundrechts i.S.v. § 90 I BVerfGG sein.[18] Sowohl aus strafrechtsdogmatischer als auch aus kriminalpolitischer Perspektive spielt es allerdings eine bedeutende Rolle, ob ein tatbestandlich beschriebenes Verhalten eine bloße (abstrakte oder konkrete) Rechtsgutsgefährdung oder eine tatsächliche Verletzung desselben darstellt.[19] Wie man sich die Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung in Bezug auf die strafrechtsdogmatische Kategorie des Deliktstypus (Verletzungsdelikt vs. Gefährdungsdelikt)[20] vorzustellen hat, ist aber gänzlich unklar.

Soweit das deutsche Strafrecht Tatbestände zum Schutz personenbezogener Daten vorsieht (exemplarisch: § 42 BDSG), wird die Frage praktisch nicht diskutiert.[21] Die Ursache für diesen Zustand der Unklarheit dürfte vor allem darin zu suchen sein, dass bereits auf grund- bzw. menschenrechtlicher Ebene Unsicherheit über die Natur der mit dem Recht auf informationelle Selbstbestimmung geschützten Interessen herrscht. *Golla* spricht vom Datenschutz als einem „diffusen Interesse"; es habe sich „als überaus schwierig erwiesen, die Gefahrenlage, der das Datenschutzrecht begegnen soll, präzise zu beschreiben."[22] Auffallend häufig finden sich im verfassungsrechtlichen Kontext (wohl) deshalb unentschlossene Formulierungen dergestalt, das Recht auf informationelle Selbstbestimmung diene

16 Vgl. *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze, 2015, S. 112 („Verletzung" des RiS).

17 Zum Verhältnis von Interessen zu Rechtsgütern *Zimmermann*, Unrecht der Korruption, 2018, S. 354.

18 Vgl. Dürig/Herzog/Scholz/*Di Fabio*, Art. 2 Abs. 2 S. 1, 43. Lfg. (2/2004), Rn. 49.

19 Kurzgesagt: Bloße Gefährdungsdelikte erfassen lediglich „verdünntes" Unrecht. Die Kriminalisierung von Verletzungsunrecht ist daher eher legitim als diejenige von Gefährdungsunrecht (grdl. *Hassemer*, Kennzeichen und Krisen des modernen Strafrechts, ZRP 1992, S. 378 ff.); zudem müssen bei Gefährdungsdelikten Abstriche im Strafmaß vorgenommen werden.

20 Dazu *Kindhäuser/Zimmermann*, Strafrecht AT, 11. Aufl. 2024, § 8 Rn. 21 ff.

21 BeckOK Datenschutzrecht/*Brodowski/Nowak*, 47. Ed. (2/2024), § 42 BDSG Rn. 4, 20, 45, die der Frage noch am intensivsten nachgehen, sprechen zwar von „Taterfolgen" bzw. einer „Verletzung" der Vertraulichkeit von Daten, lassen es i.E. aber offen, ob es sich in materieller Hinsicht um eine Verletzung oder lediglich um eine Gefährdung der geschützten Interessen handelt.

22 *Golla* (Fn. 16), S. 226.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

der Verhinderung von „Gefährdungen *und* Verletzungen" der Persönlichkeit.[23] Diese latente Unklarheit schlägt – wenig überraschend – auf die strafrechtliche Rechtsgutsbestimmung durch. Entsprechend ist unklar, ob das als Eingriff in das Recht auf informationelle Selbstbestimmung betrachtete unbefugte Sammeln (und Weiterverarbeiten)[24] personenbezogener Daten tatsächlich bereits als Verletzungsunrecht zu betrachten ist oder eher als bloßes Unrecht der Gefährdung von (weiteren bzw. anderen) Interessen.

III. Datensammeln als Gefährdungsunrecht

Betrachtet man die Fragestellung unter dem theoretischen Blickwinkel des *harm principles*,[25] fällt auf, dass das Erheben von personenbezogenen Daten als solches niemandem, auch nicht der betroffenen Person, unmittelbar weh tut bzw. dieses „keine spürbaren Auswirkungen" hat.[26] Dies spricht prima facie dafür, dass hierbei eine Verletzung individueller Interessen (noch) nicht stattfindet.[27]

23 Exemplarisch BVerfGE 118, 168, 184; 130, 151, 183; vgl. auch 120, 274, 303 („Die moderne Informationstechnik […] begründet neuartige Gefährdungen der Persönlichkeit").

24 Vgl. Lisken/Denninger/*Schwabenbauer* (Fn. 15), Kap. G Rn. 20: „grundsätzlich [stellt] jeder Verarbeitungsschritt im gesamten ‚Lebenszyklus' einer Information einen Eingriff dar".

25 Das sog. Schädigungsprinzip übernimmt im anglo-amerikanischen Rechtsraum weitgehend dieselbe straflegitimationskritische Funktion, wie sie in Deutschland dem systemtranszendenten Rechtsgutsbegriff zugeschrieben wird. Die Grundaussage des Schädigungsprinzips liegt darin, dass die Kriminalisierung eines Verhaltens nur unter der Bedingung zulässig sei, dass jenes Verhalten bei anderen Personen zu einer Schädigung (*harm*) führt (bzw. führen kann). Schlüsselbegriff dieses Prinzips ist der Terminus des Schadens bzw. der Schädigung, worunter wiederum eine Verletzung von Interessen verstanden wird. Im Kern geht es damit bei der Anwendung des Schädigungsprinzips um die Frage nach dem Vorliegen einer Interessenverletzung. Ausf. dazu *Zimmermann* (Fn. 17), S. 353-359 m.w.N.

26 *Golla* (Fn. 16), S. 93.

27 Zur sog. Erfahrbarkeitsbedingung als (logisch-analytische) Voraussetzung der Annahme einer Verletzung von Individualinteressen *Merkel*, Forschungsobjekt Embryo, 2002, S. 134 ff.; dazu auch *Zimmermann*, Vom Leid und Eigeninteresse künstlicher Rechtsträger: Juristische Personen als moralische Subjekte?, FS Merkel, 2020, S. 295, 297 ff.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

1. Dateneingriffe und Folgeeingriffe

Häufig wird entsprechend angenommen, dass die Gefährlichkeit des Datensammelns vor allem in den drohenden Konsequenzen einer späteren Nutzung dieser Daten zum Nachteil der überwachten Person liege.[28] So betont das BVerfG, das Recht auf informationelle Selbstbestimmung erweitere den grundrechtlichen Schutz des allgemeinen Persönlichkeitsrechts, indem es vor „Gefährdungslagen" schützt, die

> „bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, so insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden, die der Betroffene weder überschauen noch beherrschen kann."[29]

Anknüpfend an diese Erwägung wird in der verfassungsrechtlichen Diskussion um die Intensität informationeller Eingriffe argumentiert, diese sei stets einzelfallabhängig zu beurteilen und hänge maßgeblich von der Intensität der konkret drohenden Folgeeingriffe ab.[30] Daraus wird etwa abgeleitet, dass beim Abhören mittels einer Wanze sich die Schwere des damit verbundenen Grundrechtseingriffs danach bemisst, *wer* den Betroffenen belauscht: Tut dies eine Polizei- oder Strafverfolgungsbehörde (von der dem Betroffenen anschließend eine Razzia, seine Festnahme und ggf. ein Strafprozess droht), wiegt der Eingriff schwer; lauscht hingegen „nur" der nicht über Exekutivbefugnisse verfügende Inlandsnachrichtendienst, handele es sich bloß um einen geringfügigen (und damit viel einfacher legitimierbaren) Eingriff;[31] lauscht gar eine *ausländische* Behörde, vor deren exekutivem Arm der Abgehörte im Inland überhaupt nichts zu fürchten braucht, sei der Eingriff ganz besonders leichtgewichtig.[32]

Dieses Argumentationsmuster betrachtet Datenschutz als „strukturellen Vorfeldschutz",[33] dessen Sinn und Zweck vor allem darin besteht, vor der

28 *Golla* (Fn. 16), S. 93.
29 BVerfGE 118, 168, 184.
30 I.d.S. BeckOK Polizei- und SicherheitsR Bayern/*Linder/Unterreitmeier*, BayVSG, 23. Ed. (10/2023), Syst. Vorbemerkungen Rn. 41 ff.; *Gärditz*, Sicherheitsverfassungsrecht und technische Aufklärung durch Nachrichtendienste, EuGRZ 2018, S. 6, 9 ff.
31 So *Unterreitmeier*, Überwachung durch Polizei oder Nachrichtendienst – kein Unterschied?, GSZ 2018, S. 1, 5; a.A. Dietrich/Fahrner/Gazeas/v. Heintschel-Heinegg/*Zimmermann*, HdB Sicherheits- und StaatsschutzR, 2022, § 27 Rn. 45 f.
32 I.d.S. BVerfG, NJW 2020, 2235, 2248 Rn. 149 (BND-Überwachung im Ausland).
33 Vgl. *Golla* (Fn. 16), S. 229; *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 78 ff.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Verletzung konkreter anderer Rechtsgüter durch Folgeeingriffe unter (missbräuchlicher) Verwendung der gesammelten Daten zu schützen. In der Datenerhebung als solcher liegt hingegen keine (signifikante) eigenständige Interessenverletzung. Überträgt man diesen Gedanken auf die strafrechtliche Rechtsgutsbeeinträchtigungsdogmatik, dann sind unbefugte Eingriffe in Datenschutz(grund)rechte als strafwürdiges Unrecht anzusehen, wenn und weil es sich dabei um eine (abstrakte) Gefährdung anderer, „handfester" Interessen handelt. Ganz in diesem Sinne wird in Bezug auf die strafrechtlichen Datenschutzdelikte der §§ 201, 201a StGB vielfach die Ansicht vertreten, dass die darin enthaltenen Verbote, andere Personen ohne Einverständnis akustisch oder visuell aufzuzeichnen, bloß als abstrakte Gefährdungsdelikte einzustufen seien, deren Zweck letztlich in der Verhinderung nachgelagerter missbräuchlicher *Verwendung* der heimlich aufgezeichneten Informationen liege.[34]

2. Völkerstrafrechtsdogmatische Konsequenz

Bezogen auf die Makro-Dimension des Datenkraken-Phänomens ist diese Deutung nicht unplausibel – man erinnere den Hinweis auf die mithilfe der massenhaften Datensammlung bewerkstelligte Verfolgung der Uiguren in der VR China. Hinsichtlich der Frage, ob ein völkerstrafrechtliches Delikt des unbefugten massenhaften Datensammelns geschaffen werden sollte bzw. wie ein solches aussehen könnte, ist dieses Deutungsmodell in folgender Hinsicht aufschlussreich: So ließen sich massenhaft-systematische Verletzungen des Rechts auf informationelle Selbstbestimmung ggf. als Teilnahme an den (bereits heute normierten) Verbrechen gegen die Menschlichkeit erfassen, etwa als Beihilfehandlung im Vorfeld von Verfolgungshandlungen i.S.v. § 7 I Nr. 10 VStGB.

Die eigenständige Normierung eines Verbrechens des massenhaften Datensammelns – etwa als neuer § 7 I Nr. 10a VStGB (und damit als Verlagerung der Strafbarkeit bereits ins Vorfeld der eigentlichen Rechtsgutsbe-

34 I.d.S. MüKo-StGB/*Graf*, 4. Aufl. 2021, § 201 Rn. 5; § 201a Rn. 15; vgl. auch BT-Drs. 15/2466, S. 4 (§ 201a StGB sei ein „abstraktes Gefährdungsdelikt" im „Vorfeld der eigentlichen Rechtsverletzung"); Matt/Renzikowski/*Altenhain*, StGB, 2. Aufl. 2020, § 201a Rn. 20; *Hoyer*, Die Verletzung des höchstpersönlichen Lebensbereichs bei § 201a StGB, ZIS 2006, S. 1, 4 (§ 201a StGB als abstraktes Gefährdungsdelikt, das vor „sozialen Geltungsschäden" infolge der Weitergabe des hergestellten Bildmaterials schützen soll); vert. NK-StGB/*Kargl*, 6. Aufl. 2023, § 201a Rn. 7 f.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

einträchtigungen) – wäre nach diesem Modell hingegen nicht angeraten. Dagegen wäre insbesondere einzuwenden, dass bloße Gefährdungsdelikte im Bereich des Völkerstrafrechts prinzipiell Fremdkörper darstellen und diese das Gesamtgefüge des Völkerstrafrechts mit schwerwiegenden Wertungswidersprüchen zu belasten drohen.[35]

IV. Datensammeln als Verletzungsunrecht

Allerdings ist zweifelhaft, ob das Gefährdungsmodell das Überwachungsunrecht angemessen beschreibt. Es ist sehr wohl möglich, bereits die Erhebung von personenbezogenen Daten als eigenständige Interessenverletzung zu begreifen. Der Umstand, dass das hierbei beeinträchtigte Interesse weniger „greifbar" ist als bei der Verletzung klassischer körperlicher Individualrechtsgüter wie Leib, Leben und Sachbesitz, darf nicht zu dem Fehlschluss verleiten, es läge (noch) gar keine Interessenverletzung vor.

1. Interessenverletzung trotz fehlender „Greifbarkeit"

Für die Annahme einer materiellen Interessenverletzung kann es ausreichen, dass das Opfer eine lediglich *gefühlsmäßige* Freiheitseinbuße erleidet: Wer fest vorhat, den ganzen Tag am Schreibtisch zu verbringen, ist auch dann Opfer einer Freiheitsberaubung (§ 239 StGB), wenn jemand gegen seinen ausdrücklichen Willen bis zum Abend die Bürotür von außen verriegelt (und damit dem Eingesperrten „nur" das mulmige Gefühl des Gefangenseins beschert wird).[36] Und selbst wer aus dem lügnerischen Verhalten eines anderen bloß *irrigerweise* schließt, von diesem künftig unbotmäßig drangsaliert zu werden (obwohl in Wahrheit keine solche Gefahr besteht), wird als gegenwärtig in seinem individuellen Rechtsfrieden gestört betrachtet (vgl. § 241 III StGB, der das „Freisein von Angst und Schrecken"[37] strafrechtlich absichert).

35 Vgl. *Bock*, Ökozid – ein neues völkerstrafrechtliches Kernverbrechen?, ZRP 2021, S. 187, 188; *dies.*, Umweltschutz durch Völkerstrafrecht?, BRJ 1/2022, S. 32, 35 (in Bezug auf den Ökozid).

36 Zum Rechtsgut der Freiheitsberaubung vgl. BGH, NStZ 2022, 677 m. Anm. *Zimmermann*.

37 Näher *Zimmermann* (Fn. 17), S. 255 m.w.N.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Gegen die Annahme einer realen Interessenverletzung spricht ferner auch nicht der Umstand, dass der Verletzte von seinem konkreten Verletztwerden möglicherweise gar nichts mitbekommt. Ein klassisches Beispiel hierfür ist das (vermeintliche) Paradoxon des vollendeten Tötungsunrechts: Obwohl der Getötete von seinem Ableben niemals erfährt bzw. keine Gelegenheit hat, dieses als nachteilig zu erleben, wird die Tötung trotzdem als gravierende Verletzung *seines* individuellen Lebensinteresses betrachtet.[38] Auflösen lässt sich das Problem wie folgt: Maßgeblich ist nicht, ob *der konkret Betroffene* eine Interessenfrustration erfährt; für die intersubjektiv begründete Annahme einer Individualinteressenverletzung reicht es aus, dass das schädigende Ereignis, wenn es aus der Ich-Perspektive eines Durchschnittsmenschen auf die eigene Lebensplanung imaginiert wird, unerwünscht ist (im Beispiel: weil sich die meisten Menschen ein langes Leben wünschen, fürchten *sie* sich davor, getötet zu werden; *deshalb* wird die Tötung anderer als unrechte Verletzung von Lebensinteressen definiert).[39] Dieser Gedanke lässt sich auf verschiedenste Interessenbeeinträchtigungen übertragen. Daher ist es z.B., um i.S.v. § 242 StGB bestohlen zu werden, nicht erforderlich, dass das Opfer den Verlust jemals bemerkt. In Bezug auf informationelle Eingriffe: Der höchstpersönliche Lebensbereich kann durch Bildaufnahmen auch dann „verletzt" sein (so § 201a StGB), wenn das konkrete Opfer des Spähangriffs niemals davon erfährt (denn die meisten Menschen gruseln sich vor der Vorstellung, ohne ihre Zustimmung z.B. nackt im Badezimmer fotografiert zu werden). Ergo können auch heimliche und unbemerkte Eingriffe als aktuelle Interessenverletzung beschrieben werden.

Hält man sich beide genannten Aspekte – Freiheitsgefühlsbeeinträchtigung als Interessenverletzung und Irrelevanz der Wahrnehmung durch das konkrete Opfer – vor Augen, wird ersichtlich, dass es möglich ist, (verdeckte) informationelle Eingriffe durch Datensammeln als rechtsethisch relevante gegenwärtige *Verletzung* eines Datenschutzinteresses zu begreifen (Verletzungsthese).

---

38 Zum Problem s. *Bradley*, When Is Death Bad for the One Who Dies?, Noûs 38 (2004), S. 1 ff.; *Brueckner/Fischer*, Why Is Death Bad?, Philosophical Studies 50 (1986), S. 213 ff.; *Feldman*, Some Puzzles About the Evil of Death, Philosophical Review 2 (1991), S. 205 ff.; *McMahan*, Death and the Value of Life, Ethics 99 (1988), S. 32 ff.; *Nagel*, Death, Noûs 4 (1970), S. 73 ff.

39 Ausf. zu den Gründen *Zimmermann*, Die Rollentauschprobe im Strafrecht, in Ast et al. (Hrsg.), Gleichheit und Universalität. ARSP-Beiheft 128, 2012, S. 195, 208 ff.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

2. Verbreitung der Verletzungsthese im Recht

In der verfassungsrechtlichen Debatte finden sich Argumente für das Verletzungsmodell. So hat sich das BVerfG zuletzt insoweit vom Gedanken des Gefährdungsmodells entfernt, als es die Schwere bestimmter informationeller Grundrechtseingriffe – konkret bzgl. der akustischen und optischen Wohnraumüberwachung – *unabhängig* von der Intensität etwaig drohender Folgeeingriffe bemisst.[40] Für diese Sehweise spricht insbesondere die Erwägung, dass überwachende Kontrolle auch ohne (unmittelbar) drohende Konsequenzen eine diffuse Angst[41] und ggf. erheblichen psychischen Stress auszulösen vermag; wer ungewollt beobachtet wird, fühlt sich unwohl und wird ggf. auch dazu veranlasst, sein Verhalten notgedrungen an diesen Umstand anzupassen bzw., wie es im Stalking-Paragrafen (§ 238 StGB) heißt, in seiner „Lebensgestaltung beeinträchtigt". Dieses unter dem Begriff „chilling effect" behandelte Phänomen ist – trotz gelegentlicher Zweifel an der empirischen Datenlage –[42] äußerst plausibel[43] (s.o.: „Jeder fünfte Chinese …") und im Recht als belastbares Argumentationsfundament weithin anerkannt.[44] So schützt bspw. § 201 StGB, der die Verletzung der Vertraulichkeit des Wortes pönalisiert, nach zutr. verfassungsgerichtlicher Interpretation die „Unbefangenheit der menschlichen Kommunikation";[45] und der Richterbund wehrt sich deshalb gegen Filmaufnahmen im

40 BVerfG, NJW 2022, 1583 Rn. 169: „Dies entspricht dem besonderen Eingriffscharakter. Die Wohnraumüberwachung ermöglicht der überwachenden Behörde, jegliches Tun und Unterlassen und jede Regung der überwachten Person in ihrem privaten Rückzugsraum unmittelbar akustisch und optisch mitzuerleben. Die betroffene Person ist direkt und vollständig der Beobachtung durch die Behörde ausgesetzt. Wegen der besonderen Vertraulichkeitserwartung, die der eigenen Wohnung entgegengebracht werden darf, ist die überwachte Person hier in besonderem Maße in Gefahr, unbewusst und ungewollt breite und tiefe Einblicke in ihre Persönlichkeit zu geben."

41 BVerfGE 150, 244 Rn. 98 spricht vom „Gefühl des Überwachtwerdens".

42 Der hochrangige bayerische Verfassungsschützer *Unterreitmeier*, Folgewirkungen des BKAG-Urteils für die Nachrichtendienste?, NWVBl. 2018, S. 227, 228 etwa meint, die Annahme eines *chilling effects* basiere auf „alternativen Fakten".

43 Ausf., überzeugend und m.w.N. *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, S. 140 ff.

44 Vgl. bereits BVerfG 65, 1, 43: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

45 BVerfG, NStZ-RR 2005, 119.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

Gerichtssaal, „weil Zeug:innen nach aller Erfahrung nicht mehr frei sprächen, sobald sie vor einer Kamera sitzen."[46]

Zwischenergebnis: Überwachtwerden ist geeignet, Gefühle massiver Beklemmung und Peinlichkeit auszulösen. Die Vorstellung, eine (schriftliche, visuelle, akustische) Dokumentation dieser Überwachung könnte später anderen präsentiert und evtl. sogar zur Begründung von Maßnahmen der Sozialkontrolle (z.B. Bestrafung) herangezogen werden, verstärkt dieses Gefühl noch. Ähnliches gilt, wenn die Zusammenfügung einzelner Daten mit für sich betrachtet geringem Persönlichkeitsbezug im Ergebnis zu einer als unangenehm und peinlich imaginierten Präsentation eines Persönlichkeitsbildes genutzt werden könnte. Diese Auswirkungen der Verarbeitung von personenbezogenen Daten begründen eine im Zeitpunkt des jeweiligen Datenverarbeitungsvorgangs liegende Interessenverletzung. § 42 BDSG ist daher ein Verletzungsdelikt.

3. Überwachungsunrecht und Völkerstrafrecht

Intensive Verletzungen des Rechts auf informationelle Selbstbestimmung überschreiten zweifellos die Schwelle zum Strafunrecht (d.h. die Grenze der Strafwürdigkeit). Das BVerfG hat bereits herausgearbeitet, wann Dateneingriffe als ganz besonders intensiv (d.h. aus strafrechtlicher Perspektive: mit einem hohen Unrechtsgehalt verbunden) anzusehen sind: Informationelle Eingriffe in den Kernbereich privater Lebensgestaltung verletzen die Menschenwürde und sind (dem Staat) ausnahmslos verboten.[47] Was genau zum unantastbaren Kernbereich gehört, ist zwar nach wie vor nicht abschließend geklärt. Dazu gehört aber jedenfalls menschliches Verhalten besonders intimer Natur (etwa Ausdrucksformen der Sexualität,[48] Kommu-

46 Zit. nach LTO-Meldung „Staatsanwälte und Richter gegen Videos von Verhandlungen" v. 30.1.2023, www.lto.de/recht/justiz/j/video-aufzeichnungen-verhandlungen-strafverfahren-prozess-gesetzentwurf-kritik-richter-richterbund-general-staatsanwaelte; ausf. Deutscher Richterbund, Stellungnahme zum Gesetz zur digitalen Dokumentation der strafgerichtlichen Hauptverhandlung, Februar 2023, S. 6 ff.; krit. zu dem Argument *Th. Fischer*, Hilfe, Kamera!, Spiegel-Online v. 17.2.2023, www.spiegel.de/kultur/videoaufzeichnung-von-strafprozessen-hilfe-kamera-kolumne-a-e99882e6-61f3-4c55-a0ee-8f77936d6311.

47 Zusf. *Schneider*, Kernbereich privater Lebensgestaltung, JuS 2021, S. 29 ff.; *Zimmermann*, Das Selbstgespräch und der Kernbereich privater Lebensgestaltung, GA 2013, S. 162 ff.

48 BVerfGE 109, 279, 313.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

nikation mit engen Vertrauten[49] und das Schmieden von Gedanken im eigenen Gehirn[50]). Kernbereichsverletzend sind ferner die Erhebung und Zusammenfügung einer Vielzahl von Einzelinformationen, die in einer Totalausforschung der beobachteten Person münden (bei „Rundumüberwachung"[51] und bei der Erstellung von totalen Persönlichkeitsprofilen durch Datenakkumulation[52]).

Ist ein Unrecht so gravierend, dass der damit verbundene Eingriff in die Rechte des Individuums zugleich eine Verletzung der Menschenwürde darstellt, ist prinzipiell auch der „Zuständigkeitsbereich" des Völkerstrafrechts erreicht.[53] Jedenfalls die systematisch-massenhafte Begehung von würdeverletzenden Eingriffen in das Recht auf informationelle Selbstbestimmung könnte daher als Begehungsweise des Menschlichkeitsverbrechens vertatbestandlicht werden. Ein entsprechender § 7 I Nr. 10a VStGB könnte etwa wie folgt formuliert werden:

> „Wer … personenbezogene Daten verarbeitet, um entwürdigende Persönlichkeitsprofile einer großen Zahl von Personen zu erstellen, wird … bestraft."[54]

49 Zuletzt BVerfG, GSZ 2023, 98, 99 f.

50 Vgl. *Stübinger*, Lügendetektor ante portas, ZIS 2008, S. 538, 554.

51 BVerfG 109, 279, 323; Lisken/Denninger/*Schwabenbauer* (Fn. 15), Kap. G. Rn. 171; MüKo-StPO/*Singelnstein*, 2019, Vor § 474 Rn. 14; ausf. *Schwabenbauer* (Fn. 43), S. 292 ff.

52 BVerfGE 141, 220 Rn. 130: „Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung […] derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können."

53 Exemplarisch ICTY, Prosecutor v. Furundžija, TC, Judgement, IT-95-17/1-T, 10 Dec. 1998, para. 183: „The essence of the whole corpus of international humanitarian law as well as human rights law lies in the protection of the human dignity of every person […]. The general principle of respect for human dignity is the basic underpinning and indeed the very *raison d'être* of international humanitarian law and human rights law […]. This principle is intended to shield human beings from outrages upon their personal dignity, whether such outrages are carried out by unlawfully attacking the body or by humiliating and debasing the honour, the self-respect or the mental well being of a person."

54 Vgl. auch den Vorschlag von *Golla* (Fn. 16), S. 235 für einen nationalen Straftatbestand „Verletzung der informationellen Selbstbestimmung".

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

V. Zusammenfassung

Wer ahnt, selbst bei intimen Vorgängen beobachtet oder in seiner Gesamtpersönlichkeit ausgeforscht zu werden, fühlt sich bereits hier und jetzt schlecht – und nicht erst später, wenn die auf diese Weise erhobenen personenbezogenen Daten tatsächlich für Maßnahmen der Sozialkontrolle verwendet werden. Massive Eingriffe in das Recht auf informationelle Selbstbestimmung sind daher als von etwaigen Folgeeingriffen eigenständige Interessenverletzungen anzuerkennen. Strafrechtliche Sanktionsnormen zur Unterbindung von Überwachungsunrecht sind deshalb als Verletzungsdelikte zu denken. Formen besonders intensiver Überwachung berühren den Kernbereich privater Lebensgestaltung und verletzen die Menschenwürde. Daher können und sollten in großem Rahmen angelegte (staatliche) Überwachungskampagnen künftig als eigenständiges Menschlichkeitsverbrechen völkerstrafrechtlich erfasst werden.

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb

https://doi.org/10.5771/9783748944782-141, am 25.02.2025, 17:37:49
Open Access – (cc) BY – https://www.nomos-elibrary.de/agb