

Prof. Dr. Mark A. Zöller

DIE ZWECKÄNDERNDE NUTZUNG VON PERSONENBEZOGENEN DATEN IM STRAFVERFAHREN – GEDANKEN ZU GEGENWART UND ZUKUNFT VON § 161 STPO¹

A. VORBEMERKUNGEN

Der britische Dichter *John Donne* hat bereits im Jahr 1624 einen bis heute viel zitierten Satz geprägt: »No man is an island«. Für die Strafverteidigung erscheint diese verkürzte und leicht aus dem Kontext gegriffene² Formulierung heute aktueller denn je. Sie bringt zum Ausdruck, dass jeder von uns immer nur Teil eines Ganzen ist. Das gilt auch für das deutsche Strafverfahren, das sich längst eingebettet in eine Gesamt-Sicherheitsarchitektur wiederfindet. Deren Rahmenbedingungen haben sich seit den symbolträchtigen Terroranschlägen vom 11. September 2001 und der konstanten Bedrohung durch den islamistisch geprägten Terrorismus erheblich verändert.³ Schon die *Strafverfolgung*

1 Der vorliegende Beitrag stellt die mit Fußnoten versehene Textfassung des Vortrags dar, den der Verfasser am 23.03.2019 auf dem Deutschen Strafverteidigertag in Regensburg gehalten hat. Der Text ist angesichts seiner Aktualität auch in Heft 6/2019 der Zeitschrift »Der Strafverteidiger (StV)« erschienen (*Zöller*, StV 2019, 419 ff.). Für die Möglichkeit, den Vortragstext bereits vorab einem breiteren Leserkreis zugänglich zu machen, dankt der Verfasser den Strafverteidigervereinigungen herzlich.

2 Der Satz ist ein Zitat aus dem Prosatext »Devotions Upon Emergent Occasions and Several Steps in my Sicknes – Meditation XVII« und lautet im Zusammenhang wie folgt: »No man is an island entire of itself; every man is a piece of the continent, a part of the main; if a clod be washed away by the sea, Europe is the less, as well as if a promontory were, as well as any manner of thy friends or of thine own were; any man's death diminishes me, because I am involved in mankind. And therefore never send to know for whom the bell tolls; it tolls for thee.«

3 Zur Debatte über die Erscheinungsformen und das Bedürfnis nach einer neuen Sicherheitsarchitektur aus jüngerer Zeit etwa *Gusy* VerwArch 2010, 309 ff.; *Baldus* Verw 2014, 1 ff.; *Kugelmann* Verw 2014, 25 ff.; *Löffelmann* GSZ 2018, 85 ff.; *Kipker*, Informationelle Freiheit und staatliche Sicherheit – Rechtliche Herausforderungen moderner Überwachungstechnologien, 2016, S. 107 ff.

ist letztlich nur *ein* Baustein in einem übergreifenden Sicherheitskonzept aus Prävention und Repression. Das spiegelt sich zwangsläufig auch auf der Seite der *Strafverteidigung* wider. Auch diese findet heute immer öfter in einer Gemengelage aus Polizeirecht, Strafprozessrecht und Nachrichtendienstrecht statt. Insbesondere, aber nicht nur bei der Bewältigung der Herausforderungen durch Terrorismus, politischen Extremismus und Organisierte Kriminalität fallen auch bei nachrichtendienstlicher Beobachtung oder polizeilichen Gefahrenabwehr personenbezogene Daten an, die entweder einen strafprozessualen Anfangsverdacht begründen oder wertvolles, in der Regel für den Beschuldigten belastendes Beweismaterial für ein bereits laufendes Strafverfahren liefern. Das daraus folgende Streben nach einer strafprozessualen Nutzung von Datenmaterial, das *außerhalb* des strafverfahrensrechtlichen Regelungskontextes gewonnen worden ist, muss dabei gar keinem übertriebenen Verfolgungswahn der Strafverfolgungsbehörden entsprechen. Schließlich gilt im Strafverfahren das *Legalitätsprinzip*. Und die damit zum Ausdruck gebrachte Verpflichtung, bei Vorliegen eines Anfangsverdachts Ermittlungen aufzunehmen und bei Bestehen eines hinreichenden Tatverdachts Anklage zu erheben,⁴ kann selbstverständlich auch durch Informationen ausgelöst werden, die zunächst im Zuge *nachrichtendienstlicher Aufklärung* oder *polizeilicher Gefahrenabwehr* erhoben und dann den Strafverfolgungsbehörden durch Vertreter der Dienste oder der Präventivpolizei übermittelt werden. Zudem gilt im Rahmen des Strafverfahrensrechts auch der *Ermittlungsgrundsatz*, der gesetzlich besonders prominent in § 244 Abs. 2 StPO verankert ist.⁵ Er statuiert gerade die Pflicht der Strafverfolgungsorgane, den Sachverhalt von Amts wegen bestmöglich zu erforschen und aufzuklären. Da nach dem im Strafverfahren geltenden Prinzip der materiellen Wahrheit nach Möglichkeit das wirkliche Geschehen festgestellt werden soll, können hierfür im Einzelfall auch Informationen essentiell sein, die durch *Gefahrenabwehr- oder Nachrichtendienstbehörden* auf der Grundlage ihrer jeweiligen spezialgesetzlichen Befugnisnormen erlangt worden sind. Man kann es auch unter negativen Vorzeichen formulieren: die Außerachtlassung von für die strafrechtliche Sachaufklärung relevanten

⁴ Vgl. nur *Beulke/Swoboda*, Strafprozessrecht, 14. Aufl. 2018, Rn. 17; *Roxin/Schünemann*, Strafverfahrensrecht, 29. Aufl. 2017, § 14.

⁵ Dazu etwa *Beulke/Swoboda* (Fn. 4), Rn. 21.

und praktisch verfügbaren Informationen, die außerhalb des strafprozessualen Regelungskontextes erlangt worden sind, kann bereits per se einen Rechtsfehler darstellen und revisionsrechtlich gedacht die Aufklärungsrüge begründen.⁶

Die rechtlichen Fragen im Zusammenhang mit einer zweckändernden Nutzung von personenbezogenen Daten in Strafverfahren, die ursprünglich im *außerstrafprozessualen* Kontext erhoben worden sind, werden in einem sozialen wie rechtlichen Umfeld, in dem die Grenzen zwischen Gefahrenabwehrrecht, Strafverfahrensrecht und Nachrichtendienstrecht immer stärker verschwimmen, geradezu zwangsläufig an praktischer Bedeutung zunehmen. Von der Beantwortung der Frage, ob Beweismaterial, das auf polizeirechtlicher oder nachrichtendienstrechtlicher Grundlage gewonnen worden ist, legal in ein Strafverfahren gelangt und dort verwendbar und verwertbar ist, kann im Einzelfall der Ausgang des Strafverfahrens gegen die Mandantschaft entscheidend abhängen. Insofern besteht durchaus auch für die Strafverteidigung Anlass, sich den damit zusammenhängenden Fragen, die häufig als sehr formal und technisch empfunden werden, näher zu widmen.

B. VERFASSUNGSRECHTLICHER RAHMEN

Mit Blick auf unser Grundgesetz stellt jede (zweckändernde) Nutzung von personenbezogenen Informationen jedenfalls einen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner besonderen Ausprägung als Recht auf informationelle Selbstbestimmung dar.⁷ Schon seit dem Volkszählungsurteil des Bundesverfassungsgerichts wissen wir, dass das allgemeine Persönlichkeitsrecht auch die – aus dem Gedanken der Selbstbestimmung folgende – Befugnis des Einzelnen enthält, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche

⁶ Allg. zur Geltendmachung einer Verletzung der Amtsaufklärungspflicht mit der Aufklärungsrüge im Revisionsverfahren etwa SK-StPO/*Frister*, 5. Aufl. 2015, § 244 Rn. 243 ff. m.w.N.

⁷ Je nach Art bzw. Herkunft der personenbezogenen Daten kann ein Schutz durch andere Grundrechte in Betracht kommen bzw. spezieller sein, etwa nach Art. 10 Abs. 1 GG bei Eingriffen in das Brief-, Post- und Fernmeldegeheimnis, oder nach Art. 13 Abs. 1 GG bei Daten die durch Eingriff in das Recht auf Unverletzlichkeit der Wohnung erlangt wurden; vgl. dazu nur *Jarass/Pieroth*, GG, 15. Aufl. 2018, Art. 10 Rn. 2 u. Art. 13 Rn. 2, jew. m.w.N.

Lebenssachverhalte offenbart werden.⁸ Vor diesem Hintergrund ist nicht nur der erstmalige Informationserhebungsakt, sondern sind auch die sich daran *anschließenden* Verarbeitungsschritte, insbesondere auch die *Datenübermittlung* an weitere Stellen, als eigenständige Grundrechtseingriffe anzusehen.⁹

Dabei bezieht sich der Begriff der »Übermittlung« nicht nur auf klassische technische Übertragungsvorgänge von einem informationstechnischen System zum anderen. In der Terminologie der JI-Richtlinie¹⁰ (Art. 3 Nr. 2 RiLi) und der Datenschutz-Grundverordnung¹¹ (Art. 4 Nr. 2 DSGVO) handelt es sich mittlerweile um einen Unterfall des weit gefassten Begriffs der »Verarbeitung«. Auch wenn dies praktisch häufig der Fall sein wird, müssen nicht zwangsläufig Datensätze von einem Speicher zu einem anderen transportiert werden. Gemeint ist vielmehr, dass neben der datenübermittelnden Behörde einer *zusätzlichen Stelle die Kenntnisnahme von den Daten ermöglicht* wird, die diese Daten zu einem anderen Zweck als die übermittelnde Stelle verwenden soll.¹² Datenübermittlungen erhöhen also faktisch immer die Zahl der datenverwendenden Stellen.¹³ Eine Übermittlung liegt somit auch dann vor, wenn beispielsweise unter dem Dach derselben Polizeibehörde personenbezogene Informationen, die bislang zu Zwecken der Gefahrenabwehr erhoben und verarbeitet worden sind, nunmehr auch zu Strafverfolgungszwecken genutzt werden.

Der Sache nach handelt es sich bei solchen Übermittlungsvorgängen um *Zweckänderungen* hinsichtlich der weitergegebenen Daten. Insoweit erlangt der vom Bundesverfassungsgericht erstmals im Volks-

8 BVerfGE 65, 1 (42).

9 Vgl. BVerfGE 65, 1 (43); 67, 100 (143); 84, 239 (279); *Voigt StV* 2017, 435.

10 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119, 89 v. 04.05.2016).

11 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119, 1 v. 4.5.2016).

12 *Zöller*, in: Roggan/Kutscha (Hrsg.), *Handbuch zum Recht der Inneren Sicherheit*, 2. Aufl. 2006, S. 445 (449).

13 *Zöller*, in: Roggan/Kutscha (Fn. 12), S. 445 (450).

zählungsurteil¹⁴ postulierte *Grundsatz der Zweckbindung von Daten* entscheidende Bedeutung. Nach diesem Zweckbindungsgrundsatz hat der Gesetzgeber den Verwendungszweck personenbezogener Daten bereichsspezifisch und präzise zu bestimmen und grundsätzlich einen amtsilfefesten Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote zu gewährleisten.¹⁵ Der Grundsatz der Zweckbindung ist damit Ausfluss des Verhältnismäßigkeitsprinzips.¹⁶ Dadurch hat das Bundesverfassungsgericht sowohl die Legislative als auch die Exekutive schon früh gezwungen, Abschied vom Wunschtraum eines gemeinsamen Informationsverbundes aller staatlichen Behörden zu nehmen. Die Kenntnis *einer* Behörde, beispielsweise einer Polizeibehörde, von personenbezogenen Daten bestimmter Bürger bedeutet danach gerade nicht, dass diese Informationen dann zwangsläufig auch *anderen staatlichen Stellen*, etwa einer Staatsanwaltschaft, zu ganz anderen Zwecken zur Verfügung stehen. Andererseits ist ein Informationsaustausch zwischen Polizei, Staatsanwaltschaft und Nachrichtendiensten aber auch nicht von vornherein ausgeschlossen. Das belegt schon die Existenz der immer zahlreicher werdenden Übermittlungsvorschriften in den jeweiligen Spezialgesetzen.¹⁷ Jede Übermittlung personenbezogener Daten erfordert als Grundrechtseingriff eine *verfassungsrechtliche Rechtfertigung*. Um das Verdikt der Verfassungswidrigkeit zu vermeiden, ist hierzu eine verfassungsmäßige und bereichsspezifische gesetzliche Grundlage erforderlich, aus der sich die Voraussetzungen und der Umfang der zweckändernden Nutzung von personenbezogenen Daten für den Bürger klar erkennbar ergibt.¹⁸ Zudem muss der Grundsatz der Verhältnismäßigkeit gewahrt sein.¹⁹

14 BVerfGE 65, 1 (44, 54); seitdem st. Rspr., s. etwa BVerfGE 67, 100 (143); 78, 77 (85); 84, 239 (279 f.); 92, 191 (197); 115, 320 (344 f.).

15 BVerfGE 65, 1 (46).

16 *Denninger* KJ 1985, 215 (223); *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, S. 72; *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 260.

17 Vgl. – insoweit jeweils *pars pro toto* – im Gefahrenabwehrrecht etwa die §§ 12 Abs. 2 bis 5, 23 Abs. 2 BKAG, 32 Abs. 2, 33 BPolG sowie im Nachrichtendienstrecht die §§ 19-21, 23 BVerfSchG.

18 BVerfGE 65, 1 (46); 92, 191 (197); 113, 348 (375); 120, 378 (408); 128, 1 (47); 130, 151 (202); 130, 1 (33).

19 BVerfGE 65, 1 (44); 84, 239 (280).

C. RECHTSGRUNDLAGEN ZUR ZWECKÄNDERNDEN NUTZUNG VON DATEN IN DER StPO

I. STRAFPROZESSUALE REGELUNGEN DE LEGE LATA

1. § 161 Abs. 1 und 2 StPO

Eine explizite Befugnisnorm für die Übernahme von personenbezogenen Daten in den repressiven Bereich, die auf der Grundlage des Polizei- oder Nachrichtendienstrechts erhoben wurden, fehlt in der deutschen Strafprozessordnung bislang. Entsprechende Maßnahmen werden deshalb bislang auf die Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 StPO bzw. für die Polizei auf § 163 Abs. 1 S. 2 StPO gestützt.²⁰ Nach § 161 Abs. 1 StPO ist die Staatsanwaltschaft bei Vorliegen eines Anfangsverdachts nicht nur befugt, Ermittlungen jeder Art selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen. Sie kann vielmehr auch von allen Behörden *Auskunft verlangen*. Zu den nach dem Gesetzeswortlaut nicht näher eingegrenzten Kreis von auskunftspflichtigen Behörden zählen auch Polizeibehörden, bei denen präventivpolizeilich erhobene Daten vorliegen,²¹ sowie Nachrichtendienstbehörden, die Informationen über staatschutzrelevante Bestrebungen gesammelt haben.²² Es sind somit die allgemeinen Ermittlungsgeneralklauseln, die nach vorherrschender Auffassung die Tür für außerstrafprozessual erhobene Daten zum Strafverfahren öffnen. Mindestvoraussetzung ist allerdings stets, dass die Informationen dort, d.h. im präventivpolizeilichen oder nachrichtendienstlichen Kontext, *rechtmäßig erhoben* worden sind.²³

20 Zöller JZ 2007, 763 (771); Voigt StV 2017, 435 (436); Gazeas (Fn. 16), S. 495; a.A. König, Trennung und Zusammenarbeit von Polizei und Nachrichtendiensten, 2005, S. 285.

21 LR/Erb, 27. Aufl. 2018, § 161 Rn. 20; SK-StPO/Wohlers/Deiters, 5. Aufl. 2016, § 161 Rn. 21; HK-StPO/Zöller, 6. Aufl. 2019, § 161 Rn. 6; Schnarr StraFo 1998, 217 (222).

22 Gazeas (Fn. 16), S. 505; Rehbein, Die Verwertbarkeit von nachrichtendienstlichen Erkenntnissen aus dem In- und Ausland im deutschen Strafprozess, 2011, S. 119.

23 HK-StPO/Zöller (Fn. 20), § 161 Rn. 3; MüKo-StPO/Kölbel, 2016, § 161 Rn. 46; Wollweber NJW 2000, 3623 f.; Zöller, in: Roggan/Kutscha (Fn. 11), S. 445 (496 ff.); a.A. Brodersen NJW 2000, 2536 (2539).

Nach dem vom Bundesverfassungsgericht in seinem Bestandsdatenbeschluss vom 24. Januar 2012²⁴ konzipierten *Modell der doppelten Tür* ist allerdings zu berücksichtigen, dass es sich bei einer Datenübermittlung naturgemäß immer um einen *zweigliedrigen Vorgang* handelt. Die Übermittlungsbehörde bedarf einer Übermittlungsermächtigung, die Empfangsbehörde einer Empfangsermächtigung für die Daten.²⁵ Der Gesetzgeber muss bei einem Datenaustausch bildlich gesprochen nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten.²⁶ Soweit derselbe Gesetzgeber für Übermittlungs- und Empfangsermächtigung zuständig ist, darf er auch beide Ermächtigungen in einer Norm zusammenfassen.

Vor diesem Hintergrund stellen sich die §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO nicht als zusammengefasste Regelungen sowohl für die Übermittlung als auch für den Empfang von personenbezogenen Daten dar.²⁷ Es handelt sich stattdessen nur um *Empfangsermächtigungen* für Daten, die beispielsweise auf der Grundlage von Polizeirecht oder Nachrichtendienstrecht erhoben worden sind, also nur um *eine* von zwei benötigten Türen. Die jeweils *zweite Tür*, also die Übermittlungsermächtigung, ist im jeweiligen Polizei- oder Nachrichtendienstgesetz zu suchen. Auf Einzelheiten der zahlreichen und vielgestaltigen, im dortigen Regelungskontext existierenden Übermittlungsvorschriften kann im vorliegenden Rahmen nicht einmal ansatzweise eingegangen werden. Insofern ist auf das einschlägige Spezialschrifttum zu verweisen. Die nachfolgenden Ausführungen müssen sich daher auf die »Tür zum Strafverfahren« beschränken.

24 BVerfGE 130, 151.

25 *Gazeas* (Fn. 16), S. 501.

26 BVerfGE 130, 151 (184).

27 *Gazeas* (Fn. 16), S. 496.

Keine »Tür«, sondern eher einen »Türriegel« stellt allerdings § 161 Abs. 2 S. 1 StPO dar. Entgegen einer häufig anzutreffenden Fehleinschätzung²⁸ handelt es sich hierbei nicht um eine *Ermächtigungsgrundlage* zum Datenempfang, sondern um eine Regelung zur *Beschränkung der Verwendbarkeit* von außerstrafprozessual erhobenen Daten im Strafverfahren. Sie folgt dem sog. *Prinzip des hypothetischen Ersatzeingriffs*. Danach sollen Beweismittel trotz Verfahrensverstößen jedenfalls dann verwertet werden dürfen, wenn sie auch auf rechtmäßigem Wege hätten erlangt werden können.²⁹ Sofern die Erhebung von Daten durch strafprozessuale Maßnahmen nur bei Verdacht bestimmter Straftaten zulässig ist und personenbezogene Daten, die durch entsprechende hoheitliche Maßnahmen nach anderen Gesetzen, z.B. den Polizeigesetzen des Bundes und der Länder oder den Nachrichtendienstgesetzen, erhoben wurden, in Strafverfahren verwendet werden sollen, ist diese Verwendung zu Beweis Zwecken gem. § 161 Abs. 2 S. 1 StPO nur zulässig, wenn sie zur Aufklärung einer Straftat dient, aufgrund derer einer solche Maßnahme auch nach der StPO angeordnet werden dürfte. Der hypothetische Ersatzeingriff soll eine unnötige »Förmelei« verhindern. Wenn beispielsweise personenbezogenen Daten nun schon einmal zufällig auf gefahrenabwehrrechtlicher Grundlage zulässig erhoben worden sind, dann soll die Nutzung dieser Informationen als Beweismaterial im Strafverfahren nicht ausscheiden, wenn diese bei hypothetischer Betrachtung ohne Weiteres auch auf strafprozessualer Grundlage hätten erlangt werden können. Den Strafgerichten den Rückgriff auf solches Beweismaterial zu verwehren, ließe sich keinem juristischen Laien sinnvoll erklären. Andererseits bietet der hypothetische Ersatzeingriff auch Schutz. Mit seiner Hilfe soll verhindert werden, dass durch Rückgriff

28 Vgl. etwa BGHSt 62, 123: »Ob auf präventiv-polizeilicher Grundlage gewonnene Beweise im Strafverfahren verwendet werden dürfen, bestimmt sich nach § 161 Abs. 2 Satz 1 StPO.«; BGH StV 2017, 435: »Ist eine Durchsuchung gefahrenabwehrrechtlich zulässig, können die darauf gewonnenen Erkenntnisse gem. § 161 Abs. 2 StPO auch im Strafverfahren gegen den Angeklagten verwendet werden.«; BGH NStZ 2018, 296: »Die Verwendung der aus einer solchen Maßnahme gewonnenen Beweismittel richtet sich nach § 161 Abs. 2 S. 1 StPO.«; BGH StraFo 2018, 348 (349): »Die Verwertbarkeit der dabei gewonnenen Beweismittel im Strafverfahren bestimmt sich nach § 161 Abs. 2 S. 1 StPO.«.

29 BGHSt 31, 304 (306); BGH NStZ 1989, 375 (376); vgl. auch BVerfG NStZ-RR 2005, 203 (204 f.); HK-StPO/Gercke (Fn. 20), Vor §§ 94 ff. Rn. 32; krit. hierzu etwa Fezer NStZ 2003, 625 (629); Bernsmann/Sotelsek StV 2004, 113 ff.

auf *außerstrafprozessuale* Eingriffsermächtigungen die – ggf. strengeren – strafprozessualen Anordnungsvoraussetzungen für bestimmte Ermittlungsmaßnahmen umgangen werden.

2. § 161 Abs. 3 StPO

Eine weitere *Verwendungsbegrenzung* für außerstrafprozessual erhobene, personenbezogene Daten findet sich in § 161 Abs. 3 StPO. Der Anwendungsbereich dieser Vorschrift ist allerdings äußerst schmal gehalten. Es geht hier lediglich um die strafprozessuale Nutzung von personenbezogenen Daten, die in oder aus einer Wohnung aus einem Einsatz technischer Mittel zur Eigensicherung im Zuge nicht offener Ermittlungen *auf polizeirechtlicher Grundlage*, also etwa beim präventivpolizeilichen Einsatz Verdeckter Ermittler, erlangt worden sind. Für eine Verwendung derart erlangter Daten im Strafverfahren ist zunächst in materieller Hinsicht der Grundsatz der Verhältnismäßigkeit zu beachten. Daneben ist in formeller Hinsicht erforderlich, dass das nach § 162 StPO zuständige Amtsgericht die Rechtmäßigkeit der präventivpolizeilichen Maßnahme *vor* einer strafprozessualen Nutzung der dabei erlangten Daten festgestellt hat.³⁰

3. § 100e Abs. 6 Nr. 3 StPO

Speziell für die strafprozessuale Online-Durchsuchung nach § 100b StPO und die akustische Wohnraumüberwachung nach § 100c StPO findet sich schließlich seit dem Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017³¹ eine spezielle Normierung des hypothetischen Ersatzeingriffs in § 100e Abs. 6 Nr. 3 StPO. Auch diese bezieht sich nur auf personenbezogene Daten, die *auf polizeigesetzlicher Grundlage* erlangt worden sind. Sofern diese aus einer präventivpolizeilichen Online-Durchsuchung oder akustischen Wohnraumüberwachung stammen, sind sie ohne Einwilligung der Betroffenen nur dann im Strafverfahren nutzbar, wenn es um die Aufklärung von Straftaten oder die Ermittlung des Aufenthaltsorts eines Beschuldigten einer

30 HK-StPO/Zöller (Fn. 21), § 161 Rn. 34; Satzger/Schmitt/Widmaier/Ziegler, StPO, 3. Aufl. 2018, § 161 Rn. 30.

31 BGBl. I S. 3202; in Kraft seit 24.08.2017.

Straftat geht, hinsichtlich derer auch eine *strafprozessuale* Online-Durchsuchung oder akustische Wohnraumüberwachung hätte angeordnet werden dürfen. § 100e Abs. 6 Nr. 3 StPO ist damit ebenfalls keine Befugnisnorm zur zweckändernden Nutzung gefahrenabwehrrechtlich erhobener Daten, sondern wiederum nur eine *Eingrenzung des allgemeinen Auskunftsanspruchs* nach § 161 Abs. 1 S. 1 bzw. § 163 Abs. 1 S. 2 StPO.

II. PRAKTISCHE KONSEQUENZEN

Über die Sondernormen der §§ 161 Abs. 2 und 3, 100e Abs. 6 Nr. 3 StPO hinaus sieht unsere Strafprozessordnung überraschenderweise *keine weiteren ausdrücklichen Einschränkungen* hinsichtlich der strafprozessualen Verwendbarkeit von auf präventivpolizeilicher oder nachrichtendienstrechtlicher Grundlage erhobenen Daten vor. Dabei ist es nicht so, als hätte darüber noch niemand nachgedacht. Vor rund 20 Jahren, im Regierungsentwurf zum Strafverfahrensänderungsgesetz 1999, waren Beschränkungen der Verwertbarkeit auch für präventivpolizeilich erlangte Erkenntnisse vorgesehen, die durch Rasterfahndung, Einsatz technischer Mittel oder Verdeckter Ermittler gewonnen worden sind (§ 161 Abs. 2 StPO-E).³² Dieser Filter ist jedoch damals im Vermittlungsausschuss wieder gestrichen worden.³³ Im Umkehrschluss folgt daraus, dass aktuell keine generellen Verwendungsbeschränkungen für personenbezogene Informationen aus hoheitlichen Maßnahmen nicht-strafprozessualer Art bestehen, deren Anordnung nach der StPO *keinen Verdacht bezüglich bestimmter Straftaten voraussetzt*.³⁴

Darüber hinaus muss man sehen, dass sich jedenfalls die Verwendungsbeschränkungen in § 161 StPO ausdrücklich nur auf die Verwendung »zu Beweis Zwecken« beziehen. Daraus wird im Umkehrschluss regelmäßig gefolgert, dass Informationen, die auf gefahrenabwehrrechtlicher oder nachrichtendienstrechtlicher Grundlage gewonnen wurden, im Strafverfahren als *Ermittlungs- bzw. Spurenansatz* zur Gewinnung weiterer Beweismittel ohne jede Einschränkung genutzt

32 BT-Drs. 14/1484, S. 6.

33 BT-Drs. 14/3525, S. 2.

34 Vgl. Zöller, in: Roggan/Kutscha (Fn. 12), S. 445 (493).

werden dürfen.³⁵ Diese Ansicht, die sich durchaus auf den Wortlaut des Gesetzes und auf seine Entstehungsgeschichte³⁶ berufen kann, führt zu weitreichenden Konsequenzen für die Praxis. Sie erlaubt es den Strafverfolgungsbehörden, bei jedem auch noch so vagen und nicht näher belegten Hinweis von Seiten der Präventivpolizei oder der Dienste, strafrechtliche Ermittlungen aufzunehmen und durchzuführen. Ein bloßer Anruf bei den Strafverfolgungsbehörden genügt schon, etwa mit dem Hinweis »Genaueres können wir Euch im Moment nicht sagen, aber schaut Euch doch mal heute Nachmittag den X mit seinem Auto auf der A3 genauer an, der könnte Rauschgift dabeihaben.« Mit einer allzu unkritischen Zulassung der Verwendung als Spuren- bzw. Ermittlungsansatz wird aber übersehen, dass damit regelmäßig weitere, auch schwerwiegende Grundrechtseingriffe zwangsläufig verbunden sind. Um diese zu rechtfertigen, ist eine bereichsspezifische und normenklare ausdrückliche Ermächtigungsgrundlage erforderlich. Dass diese Aufgabe von den allgemeinen Ermittlungsgeneralklauseln der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO erfüllt werden kann, darf getrost bezweifelt werden.³⁷

Zumindest faktisch entschärft ist die Verwendung von auf polizeigesetzlicher Grundlage gewonnenen Daten als Spurenansatz im Strafverfahren bereits de lege lata in den Fällen des § 161 Abs. 3 StPO. Zwar bezieht sich die Verwendungsbeschränkung nach dem Gesetzeswortlaut auch hier auf die bloße Verwendung »zu Beweis Zwecken«. Allerdings handelt es sich bei § 161 Abs. 3 StPO um eine einfachgesetzliche Ausführungsnorm zur verfassungsrechtlichen Schrankenregelung zum Grundrecht auf Unverletzlichkeit der Wohnung in Art. 13 Abs. 5 S. 2 GG. Da letzterer eine Ausnahme zur Verwendung als Spurenansatz nicht vorsieht, kommt eine Differenzierung zwischen der Verwendung zu Beweis Zwecken und als Spurenansatz bei verfassungskonformer Auslegung

35 SK-StPO-Wohlers/Deiters (Fn. 21), § 161 Rn. 48; Müko-StPO-Kölbel (Fn. 23), § 161 Rn. 45; Satzger/Schmitt/Widmaier/Ziegler (Fn. 29), § 161 Rn. 27; Puschke/Singelstein NJW 2008, 113 (117); a.A. HK-StPO/Zöllner (Fn. 20), § 161 Rn. 32; Radtke/Hohmann/Kretschmer, StPO, 2011, § 161 Rn. 14.

36 Vgl. BT-Drs. 16/5846, S. 64.

37 So bereits Zöllner, in: Roggan/Kutscha (Fn. 12), S. 445 (497 f.); krit. auch Singelstein ZStW 120 (2008), 854 (878); Voigt StV 2017, 435 (436); Gazeas (Fn. 16), S. 497 ff.

im Ergebnis nicht in Betracht.³⁸ Faktisch unterliegt damit auch die Verwendung auf polizeigesetzlicher Grundlage erlangter Erkenntnisse als Spurenansatz den Beschränkungen des § 161 Abs. 3 StPO.³⁹

III. VERFASSUNGSWIDRIGKEIT DER GELTENDEN RECHTSLAGE

Blickt man nach alledem auf das *Gesamtbild* der Rechtslage zur zweckändernden Nutzung von personenbezogenen Daten im Strafverfahren, so bestehen doch erhebliche Zweifel an deren Verfassungsmäßigkeit.⁴⁰ Faktisch ermöglicht § 161 StPO eine weitgehende *Durchbrechung* des Grundsatzes der Zweckbindung von Daten. Der Auskunftsanspruch nach § 161 Abs. 1 S. 1 StPO, der den Empfang der Daten im Strafverfahren faktisch voraussetzungslos zulässt, wird nur bei Ermittlungsmaßnahmen, die nach der StPO lediglich bei Verdacht bestimmter Straftaten zulässig sind, durch das Prinzip des hypothetischen Verdachtseingriffs begrenzt und selbst dann durch eine weitgehende Zulassung der Nutzung als Spurenansatz wieder entwertet. Bei vielen Standardmaßnahmen, deren Anordnung auf strafprozessualer Grundlage nicht an den Verdacht bestimmter Straftaten gebunden ist, beispielsweise die molekulargenetische Untersuchung (§§ 81e, 81f StPO), die Durchsuchung (§§ 102 ff. StPO) oder die Identitätsfeststellung (§ 163b StPO), ist die strafprozessuale Nutzung außerstrafprozessual erhobener Daten ohne jede Einschränkung zulässig. Diese Rechtslage widerspricht schon angesichts ihrer Pauschalität sowohl dem Bestimmtheitsgrundsatz als auch dem Verhältnismäßigkeitsprinzip.⁴¹ Es fehlt an klaren Kriterien für eine Eingrenzung, die den unterschiedlichen Anwendungsvoraussetzungen von Polizeirecht, Strafprozessrecht und Nachrichtendienstrecht Rechnung trägt.

Denkbar wäre es z.B., die Verwendung von präventivpolizeilich oder nachrichtendienstlich erhobenen Informationen de lege ferenda nur dann zu repressiven Zwecken zu erlauben, wenn die zu verfolgende

38 HK-StPO/Zöller (Fn. 21), § 161 Rn. 35; Hilger NStZ 2000, 561 (564).

39 LR/Erb (Fn. 21), § 161 Rn. 72; SK-StPO/Wohlers/Deiters (Fn. 21), § 161 Rn. 55; HK-StPO/Zöller (Fn. 21), § 161 Rn. 35; Wolter, FS Hilger, 2003, S. 275 (281).

40 Krit. auch Hefendehl GA 2011, 209 (222 f.); vgl. im Übrigen die Nachw. in Fn. 36.

41 So bereits Zöller, in: Roggan/Kutscha (Fn. 11), S. 445 (497).

Straftat ein gewisses Gewicht besitzt.⁴² Nach geltender Rechtslage ist erstaunlicherweise gerade bei der Verfolgung von Straftaten aus dem Bereich der leichten und mittleren Kriminalität (z.B. von Fahrrad- und Ladendiebstählen oder einfachen Internetbetrügereien) eine Übernahme von präventivpolizeilich oder nachrichtendienstrechtlich erlangten Daten in das Strafverfahren nahezu voraussetzungslos möglich, sofern die jeweilige Übermittlungsermächtigung im Gefahrenabwehr- oder Nachrichtendienstrecht nur weit genug formuliert ist. Damit bewegt man sich nur scheinbar auf verfassungsrechtlich sicherem Boden. Zwar hat das Bundesverfassungsgericht in seinem Urteil zum BKA-Gesetz vom 20. April 2016 das von ihm als »hypothetischen Datenenerhebung« bezeichnete Kriterium in Reinform nur auf die zweckändernde Nutzung von personenbezogenen Daten aus *eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen* wie Online-Durchsuchungen und Wohnraumüberwachungen bezogen. Bei Daten, die durch andere Maßnahmen erlangt worden sind, sollen es Gesichtspunkte der Vereinfachung und der Praktikabilität rechtfertigen, dass nicht alle Einzelanforderungen, die für die *Datenerhebung* gelten, auch für die Übermittlung solcher Daten zu anderen Zwecken einzuhalten sind.⁴³ Diese Absenkung der Anforderungen betrifft aber nur den *Anlass der Datenerhebung*, also etwa den Konkretisierungsgrad für den strafprozessualen Anfangsverdacht oder die polizeirechtliche Gefahr.⁴⁴ Diese Rechtsprechungslinie des Bundesverfassungsgerichts ist schon deshalb wenig überzeugend, weil sie einer Beliebigkeit und Unbestimmtheit von bereichsspezifischen Empfangs- und Übermittlungsvorschriften für personenbezogene Daten im Sicherheitsrecht letztlich Tür und Tor öffnet.⁴⁵ Aber klar ist, dass auch Karlsruhe *keine voraussetzungslose* Zweckänderung von Daten zulassen wollte.

Infolgedessen spricht jedenfalls mit Blick auf die Zukunft Vieles dafür, das Prinzip des hypothetischen Ersatzeingriffs zum generellen Leitprinzip der Strafprozessordnung zu erheben, auch wenn sich die Strafverfolgungspraxis hiergegen mit Händen und Füßen wehren

42 Zöller, in: Roggan/Kutscha (Fn. 12), S. 445 (497).

43 Vgl. BVerfGE 141, 220 (328).

44 Vgl. BVerfGE 141, 220 (328).

45 Zöller, in: *Dietrich/Gärdtitz/Graulich/Gusy/Warg* (Hrsg.), *Nachrichtendienste im demokratischen Rechtsstaat*, 2018, S. 185 (192 f.).

mag. Das würde bedeuten, dass man personenbezogene Daten, die auf gefahrenabwehrrechtlicher oder nachrichtendienstrechtlicher Grundlage erhoben wurden, ganz allgemein, und damit unabhängig von der Art und Schwere der zu verfolgenden Straftat, nur dann als Beweismaterial in Strafverfahren zulässt, wenn sie bei hypothetischer Betrachtung (ex post) rechtmäßig auch auf strafprozessualer Grundlage hätten erhoben werden können. Erkenntnisse aus einer präventivpolizeilichen Durchsuchungsmaßnahme dürften somit beispielsweise nur dann strafprozessual genutzt werden, wenn auch die Voraussetzungen für eine strafprozessuale Durchsuchung nach den §§ 102 ff. StPO vorgelegen haben. Und Erkenntnisse aus einer nachrichtendienstlichen Telekommunikationsüberwachung dürften nur dann ihren Weg in ein Strafverfahren finden, wenn auch eine Telekommunikationsüberwachung nach § 100a StPO hätte angeordnet werden dürfen. Nur dann sind die Strafverfolgungsbehörden von vornherein gegen den Vorwurf gefeit, in Verfahrensordnungen auszuweichen, die ihnen die Informationserhebung erleichtern, etwa weil präventivpolizeiliche Maßnahmen keinen Richtervorbehalt vorsehen oder die nachrichtendienstliche Aufklärung nicht an die Eingriffsschwelle des strafprozessualen Anfangsverdachts gebunden ist. Und nur dann stellt sich im Strafverfahren von vornherein auch nicht die Frage nach einem Beweisverwertungsverbot wegen bewusster Missachtung der Anordnungsvoraussetzungen für strafprozessuale Eingriffe.⁴⁶

IV. ZUR REFORM DES § 161 STPO

1. Aktueller Beratungsstand

An dieser Stelle wendet sich der Blick hoffnungsvoll auf die aktuellen Reformvorschläge für die bereichsspezifischen Datenschutzregelungen in der StPO. Konkret geht es um den Gesetzentwurf der Bundesregierung vom 1. Oktober 2018 zur Umsetzung der EU-Richtlinie 2016/680 im Strafverfahren sowie zur Anpassung daten-

⁴⁶ Vgl. etwa zum Beweisverwertungsverbot bei bewusster Umgehung des Richtervorbehalts bei Durchsuchungsmaßnahmen BGH NStZ 2012, 104 (105); OLG Düsseldorf StraFo 2009, 280 (281); StV 2017, 12 (14 f.); AG Tiergarten StV 2015, 624 (625).

schutzrechtlicher Bestimmungen an die EU-Verordnung 2016/679⁴⁷. Hiermit sollte das Strafverfahrensrecht an die JI-Richtlinie und die Datenschutz-Grundverordnung angepasst werden.⁴⁸ Und in diesem Rahmen sollte auch § 161 StPO neu gefasst werden. Zugleich wollten die Entwurfsverfasser die Sonderregelung für die Online-Durchsuchung und die akustische Wohnraumüberwachung aufheben und im Rahmen von § 161 StPO gebündelt regeln.⁴⁹ Dieser neue § 161 StPO sollte – soweit es um die zweckändernde Nutzung von personenbezogenen Daten für Zwecke des Strafverfahrens geht – wie folgt lauten:

§ 161 StPO-E [Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft und Verwendungsbeschränkungen]

(1) Soweit nicht andere gesetzliche Vorschriften die Befugnisse der Staatsanwaltschaft besonders regeln, ist sie zu den in § 160 bezeichneten Zwecken befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und sind in diesem Falle befugt, von allen Behörden Auskunft zu verlangen. Maßnahmen nach den Sätzen 1 und 2 sind unzulässig, soweit besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen. [...]

(3) Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen erlangten verwertbaren personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen im Strafverfahren verwendet werden

1. zur Aufklärung solcher Straftaten, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz jeweils angeordnet werden könnte, sowie zur Aufklärung jeweils vergleichbar bedeutender Straftaten oder

47 BT-Drs. 19/4671.

48 BT-Drs. 19/4671, S. 1.

49 Vgl. BT-Drs. 19/4671, S. 61.

2. zur Ermittlung des Aufenthalts der einer in Nummer 1 genannten Straftat verdächtigen Person,

wenn sich den Daten im Einzelfall konkrete Ermittlungsansätze für die in den Nummern 1 und 2 genannten Zwecke entnehmen lassen.

(4) Sofern es sich um lediglich vergleichbar bedeutende Straftaten handelt (Absatz 3 Nummer 1), dürfen im Strafverfahren nicht verwendet werden

1. die in Absatz 3 genannten Daten zu Beweis Zwecken und

2. Daten, die durch eine Maßnahme nach anderen Gesetzen erlangt wurden, wenn diese Maßnahme einer der folgenden Maßnahmen entspricht:

a) Maßnahmen nach den §§ 100b und 100c oder

b) Maßnahmen nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 1 Satz 3 oder Absatz 3 Satz 2.

(5) In oder aus einer Wohnung erlangte personenbezogene Daten aus einem Einsatz technischer Mittel zur Eigensicherung im Zuge nicht offener Ermittlungen auf polizeirechtlicher Grundlage dürfen unter Beachtung des Grundsatzes der Verhältnismäßigkeit in einem Strafverfahren nur verwendet werden (Artikel 13 Absatz 5 des Grundgesetzes), wenn das Amtsgericht (§ 162 Absatz 1), in dessen Bezirk die anordnende Stelle ihren Sitz hat, die Rechtmäßigkeit der Maßnahme festgestellt hat; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen.«

Ergänzend hierzu soll in § 163 Abs. 1 StPO folgender Satz 3 angefügt werden:⁵⁰

»§ 161 Absatz 1 Satz 3 und Absatz 2 bis 5 gilt entsprechend.«

2. BEWERTUNG

Dieser Entwurf enthielt, soweit er sich mit der zweckändernden Nutzung außerstrafprozessual erhobener Daten im Strafverfahren befasste, nur wenig Licht, dafür aber viel Schatten. Bedauerlich ist zunächst, dass die Chance vertan worden ist, eine bereichsspezifische und normenklare Ermächtigungsgrundlage für die zweckändernde

⁵⁰ BT-Drs. 19/4671, S. 10.

Nutzung außerstrafprozessual erhobener personenbezogener Daten zu schaffen. Nach § 161 Abs. 1 StPO-E, der im Vergleich zur bisherigen Gesetzeslage lediglich redaktionell leicht angepasst wurde, würden als Empfangsermächtigungen für präventivpolizeilich oder nachrichtendienstlich erhobene Daten im Strafverfahren auch in Zukunft die Ermittlungsgeneralklauseln fungieren. Nach den Vorstellungen der Entwurfsverfasser sollten lediglich neue Absätze 3 und 4 an die Stelle des bisherigen § 161 Abs. 2 S. 1 StPO treten und die allgemeinen Voraussetzungen der Verwendung von Daten regeln, die durch besonders eingriffsintensive nicht strafprozessuale Maßnahmen erhoben wurden, welche nach der StPO an das Vorliegen des Verdachts bestimmter Straftaten geknüpft sind.⁵¹ Im Gegensatz zur bisherigen Rechtslage sollte die Formulierung »zu Beweis Zwecken« jedenfalls in § 161 Abs. 3 StPO-E gestrichen werden. Damit sollte auch die Verwendung als Ermittlungsansatz oder zur Ermittlung des Aufenthaltsorts eines Verdächtigen beschränkt werden.⁵² Entsprechendes gilt für § 161 Abs. 5 StPO-E, der an die Stelle des bisherigen § 161 Abs. 3 StPO treten sollte.⁵³

Hoch problematisch erscheint jedoch eine gleichzeitige *Erweiterung* der Zulassung einer zweckändernden Nutzung außerstrafprozessual erhobener Daten, die ebenfalls unter formaler, aber inhaltlich fehlerhafter Berufung auf das BKAG-Urteil des Bundesverfassungsgerichts vorgenommen wird. Insofern sollte in Fällen, in denen eine Maßnahme nach der StPO nur bei Verdacht bestimmter Straftaten zulässig ist, die Verwendung gemäß § 161 Abs. 3 Nr. 1 StPO-E nicht mehr nur zur Aufklärung der in der StPO genannten Anlasstaten, sondern auch zur Aufklärung »jeweils vergleichbar bedeutender Straftaten« zugelassen werden. Das BVerfG wollte in der in Bezug genommenen Urteils passage⁵⁴ gerade einen mit besonders eingriffsintensiven Überwachungsmaßnahmen gleichgewichtigen Rechtsgüterschutz sicherstellen und hat hierfür konkrete Ermittlungsansätze eingefordert. Infolgedessen wurde § 20v Abs. 5 S. 1 Nr. 3 BKAG a.F. für mit der Verfassung

51 BT-Drs. 19/4671, S. 63.

52 BT-Drs. 19/4671, S. 63.

53 Vgl. BT-Drs. 19/4671, S. 64.

54 BVerfGE 141, 220 (337).

unvereinbar erklärt. Das Gericht hat für die Neuregelung im bereichsspezifischen Datenschutzrecht aber gerade nicht erklärt, dass man bei Ermittlungsmaßnahmen, die mit Blick auf die Gewichtigkeit des damit erstrebten Rechtsgüterschutzes an – teilweise sehr weite und heterogene (vgl. nur §§ 100a Abs. 2, 100b Abs. 2 StPO) – Kataloge von Anlassstraftaten anknüpfen, eine zweckändernde Nutzung von personenbezogenen Daten auch zur Aufklärung von Straftaten nutzen darf, die den explizit genannten Katalogtaten wertungsmäßig entsprechen. Insofern ist das in § 161 Abs. 3 StPO-E vorgeschlagene Regelungskonzept schon vom Ansatz her kurios. Denn um welche Straftaten soll es sich denn handeln, die der Gesetzgeber zwar nicht als Anlassstaten in den Straftatenkatalog der jeweiligen StPO-Norm aufgenommen hat, die aber dennoch »vergleichbar bedeutend« sein sollen? Das wirft nicht nur Bedenken im Hinblick auf den Grundsatz der Gewaltenteilung auf, wenn im Ergebnis die Strafgerichte zu entscheiden haben, was den Wertentscheidungen des demokratisch legitimierten Gesetzgebers entspricht und was nicht. Faktisch dürften auf diese Weise z.B. Erkenntnisse aus Telekommunikationsüberwachungsmaßnahmen auch für die Verfolgung von Straftaten genutzt werden, die nicht im Katalog des § 100a Abs. 2 StPO genannt sind.⁵⁵ Der Verweis auf das BKAG-Urteil des BVerfG in der Entwurfsbegründung⁵⁶ ist somit eine grobe Entstellung des verfassungsgerichtlichen Votums. Dieses vollkommen unbestimmte Merkmal erfuhr auch in den Gesetzgebungsmaterialien keinerlei Präzisierung und würde daher einer willkürlichen Ausdehnung der Nutzung von auf polizeirechtlicher und nachrichtendienstrechtlicher Grundlage erhobenen Daten im Strafverfahren Tür und Tor öffnen. Was vergleichbar ist und was nicht, bleibt ohne nähere Kriterien hierfür eine offene Wertungsfrage. Entsprechendes gilt auch für die damit nur pro forma einschränkende Formulierung, dass »sich den Daten im Einzelfall konkrete Ermittlungsansätze [...] entnehmen lassen« müssen, die weder von Seiten des BVerfG in der Entscheidung zum BKAG noch durch die Entwurfsverfasser näher konkretisiert wird.

55 Vgl. Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Umsetzung der EU-Richtlinie 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die EU-Verordnung 2016/679 v. 16.11.2018, S. 4.

56 BT-Drs. 4671, S. 63 f.

Dass die Entwurfsverfasser diesem Ansatz vor dem Hintergrund des Bestimmtheits- und des Verhältnismäßigkeitsgrundsatzes selbst nicht so recht über den Weg trauen, zeigt auch der ebenfalls weitgehend misslungene § 161 Abs. 4 StPO-E. Zum einen wird hier ohne jede Begründung für lediglich vergleichbar bedeutenden Straftaten i.S. des § 161 Abs. 3 Nr. 1 StPO-E der Zusatz »zu Beweis Zwecken« wieder eingefügt (§ 161 Abs. 4 Nr. 1 StPO-E). Das bedeutet im Klartext, dass man diesbezüglich die Nutzung als Spuren- bzw. Ermittlungsansatz offenbar wieder zulassen will und stellt einen erkennbaren Wertungswiderspruch zur Strafverfolgung der in der StPO konkret bestimmten Anlasstaten dar. Zudem dürfen nach § 161 Abs. 4 Nr. 2 StPO-E außerstrafprozessual erhobene Daten zur Aufklärung lediglich vergleichbar bedeutender Straftaten i.S. von § 161 Abs. 3 Nr. 1 StPO-E dann nicht verwendet werden, wenn die polizeirechtliche oder nachrichtendienstliche Maßnahme der strafprozessualen Online-Durchsuchung, akustischen Wohnraumüberwachung oder Verkehrsdatenauskunft entspricht. Das verstehe in dieser inhaltlichen Auswahl wer will. Und es stellt auch sprachlich ein Musterbeispiel für unverständlich formulierte Gesetze dar, ohne dass dies etwa durch zwingende Vorgaben der JI-Richtlinie vorgegeben wäre. Der gesamte Regelungsvorschlag war mit derart vielen inhaltlichen Widersprüchen und gesetzestechnischen Fehlern behaftet, dass er auf Empfehlung des Ausschusses für Recht und Verbraucherschutz⁵⁷ im weiteren Gesetzgebungsverfahren zu Recht aufgegeben wurde. Das Gesetz zur Umsetzung der EU-Richtlinie 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die EU-Verordnung 2016/679 vom 20. November 2019⁵⁸, sieht in Art. 1 Ziff. 13 für einen neuen § 161 StPO somit nur noch eine formale Anpassung des Gesetzestextes an das neue Datenschutzrecht ohne nennenswerte inhaltliche Änderungen vor. Das ist für eine derartig praxisrelevante und grundrechtssensible Materie deutlich zu wenig.

57 vgl. BT-Drs. 19/11190, S. 3

58 BGBl. I S. 1724

D. VERDEUTLICHUNG AM BEISPIEL SOG. LEGENDIERTER KONTROLLEN

Was bedeutet nun all dies für die Praxis des Strafverfahrens und für die Strafverteidigung? Um dieser Frage nachzugehen, sollen die praktischen Probleme, die sich bei der zweckändernden Nutzung von außerstrafprozessual erhobenen Daten in Strafverfahren stellen, zum Abschluss an einer Fallgruppe verdeutlicht werden, die derzeit besonders stark diskutiert wird: Es geht um sog. *legendierte Kontrollen*.

I. LEGENDIERTE KONTROLLEN

Diese erfreuen sich insbesondere im Zusammenhang mit der polizeilichen Bekämpfung der organisierten Betäubungsmittelkriminalität großer Beliebtheit.⁵⁹ Das Strickmuster ist immer dasselbe. Die deutschen Polizeibehörden erlangen, häufig in Zusammenarbeit mit Ermittlungsbehörden im europäischen Ausland, im Zuge verdeckt erfolgreicher strafprozessualer Ermittlungen Informationen über bevorstehende Rauschgifttransporte in das Bundesgebiet. Infolgedessen will die Polizei die Betäubungsmittel aus dem Verkehr ziehen, um zu verhindern, dass große Mengen hiervon in den Umlauf gelangen. Zudem müssen natürlich die Beweise für das Strafverfahren gegen den Rauschgiftkurier gesichert werden. Man will aber regelmäßig auch an die »dicken Fische«, also die Hintermänner der Organisation herankommen. Diese würden durch die gezielte Festnahme des Transporteurs der Betäubungsmittel auf- und abgeschreckt werden, da sie davon ausgehen müssen, dass ihre Organisationsstrukturen »aufgeflogen« sind. Die sich häufig im Ausland aufhaltenden Hintermänner sollen sich stattdessen in Sicherheit zu wiegen, bis auch sie in die Bundesrepublik einreisen und die Aushebung der gesamten Organisation erfolgsversprechend erscheint. Vor diesem Hintergrund werden dann die allgemeinen Polizeibehörden vor Ort auf den Betäubungsmitteltransport aufmerksam gemacht. Diese sollen dann eine vermeintlich allgemeine, in Wirklichkeit natürlich gezielte und damit legendierte Verkehrskontrolle durchführen. Bei der anschließenden Durchsuchung des Fahrzeugs auf polizeigetzlicher Grundlage werden dann »rein zufällig« die transportierten Betäubungsmittel aufgefunden und sichergestellt.

⁵⁹ Lenk NVwZ 2018, 38 (39).

II. DIE RECHTSPRECHUNG DES BGH

Der Bundesgerichtshof hatte bereits in verschiedenen Verfahren seit dem Jahr 2010 Gelegenheit, sich mit solchen vorgetäuschten allgemeinen Polizeikontrollen zu beschäftigen.⁶⁰ Zudem dürfte das Dunkelfeld der tatsächlichen Durchführung solcher Maßnahmen erheblich sein. Schließlich werden die dem vermeintlichen Zufallsfund vorausgegangenen Ermittlungen häufig weder bei den polizeilichen Vernehmungen noch bei der hafrichterlichen Anhörung erwähnt und finden somit keinen Niederschlag in der Akte. So schreibt etwa *Christoph Krehl*, Mitglied des 2. Strafsenats des BGH, zum Thema folgenden schönen Satz:⁶¹

»So häufig, wie man als Revisionsrichter in landgerichtlichen Entscheidungen von »allgemeinen Verkehrskontrollen« liest, ohne dass sich in den Urteilsgründen im Übrigen Hinweise auf ihren Ausgangspunkt finden, ist davon auszugehen, dass so manche »legendierte Kontrolle« gar nicht »enttarnt« worden ist.«

In den Fokus der strafrechtlichen Fachöffentlichkeit sind legendierte Kontrollen vor allem durch eine Entscheidung des 2. Strafsenats des BGH vom 26. April 2017⁶² geraten. Hier hatte die Staatsanwaltschaft Frankfurt am Main ein Ermittlungsverfahren gegen eine Tätergruppierung wegen des Verdachts von Betäubungsmittelstraftaten geführt. Im Zuge von durch den Frankfurter Ermittlungsrichter angeordneten, verdeckten Ermittlungsmaßnahmen ergab sich der Verdacht, dass der in die Niederlande ausgereiste Angeklagte Betäubungsmittel nach Deutschland einführen würde. Nachdem die Frankfurter Kriminalpolizei mit Hilfe eines Peilsenders festgestellt hatte, dass der Angeklagte nach Deutschland eingereist war, entschloss sie sich, die mitgeführten Betäubungsmittel sicherstellen zu lassen, um zu verhindern, dass diese in Umlauf kommen, und um Beweise zu sichern. Hierüber informierte sie die Verkehrspolizei in Wiesbaden mit dem Hinweis »es

60 Vgl. BGH NStZ 2010, 294; BGH StraFo 2011, 358; BGH StV 2017, 435; zu untergerichtlichen Entscheidungen vgl. die Nachw. bei *Lenk* StV 2017, 692 (693).

61 *Krehl* StraFo 2018, 265.

62 BGHSt 62, 123; dazu *Albrecht* HRRS 2017, 446 ff.; *Brodowski* JZ 2017, 1124 ff.; *Kochheim* KriPoZ 2017, 316 ff.; *Lenk* StV 2017, 692 ff.; *Lange-Bertalot/Aßmann* NZV 2017, 572 ff.; *Löffelmann* JR 2017, 596 ff.; *Mitsch* NJW 2017, 3124 ff.; *Schiemann* NStZ 2017, 657; *Börner* StraFo 2018, 1 ff.; *Krehl* StraFo 2018, 265 ff.; *Roggan* GSZ 2018, 52 ff.

wäre schön, wenn sich für die Kontrolle ein Vorwand fände«. Es sollte verhindert werden, dass ein sich in Marokko aufhaltender Hintermann von den laufenden Ermittlungen erfuhre. Die Verkehrspolizei wurde an das Fahrzeug des Angeklagten herangeführt und kontrollierte es nach einer geringfügigen Geschwindigkeitsüberschreitung. Dabei wurden acht Kilogramm Kokain gefunden. Die Beamten der Verkehrspolizei informierten den damaligen Beschuldigten vor seiner Vernehmung nicht über die vorangegangenen verdeckten Ermittlungen und erwähnten sie auch nicht in ihrem schriftlichen Bericht, der für den Ergreifungs-ort zuständigen Kriminalpolizei zugeleitet wurde. So entstand der Eindruck einer zufälligen Verkehrskontrolle. Auch die Kriminalpolizei gab keinen Hinweis auf das Ermittlungsverfahren in Frankfurt am Main. Auf Antrag der Staatsanwaltschaft erließ der Ermittlungsrichter des Amtsgerichts Limburg gegen den Beschuldigten Haftbefehl wegen Beihilfe zum unerlaubten Handeltreiben mit Betäubungsmitteln in nicht geringer Menge. Einige Wochen später, nachdem der sich wieder in Deutschland aufhaltende Hintermann aufgrund eines Haftbefehls des Amtsgerichts Frankfurt am Main festgenommen worden war, übersandte die Kriminalpolizei Frankfurt einen Vermerk an ihre Kollegen in Limburg, der die Erkenntnisse aus dem Ermittlungsverfahren der Staatsanwaltschaft Frankfurt zusammenfasste. Daraus ergab sich auch, dass die Fahrzeugkontrolle nicht zufällig durchgeführt worden war. Der Angeklagte erhielt diesen Bericht erst einige Wochen vor Anklageerhebung.

Der 2. Strafsenat des BGH hat diese Vorgehensweise der hessischen Polizei ausdrücklich gebilligt und die Revision des Angeklagten verworfen. Dabei betonte er, dass die Durchsuchung des Fahrzeugs ohne vorherige richterliche Anordnung nach hessischem Gefahrenabwehrrecht zulässig war.⁶³ Der polizeilichen Rechtmäßigkeit der Maßnahme stehe nicht entgegen, dass zum Zeitpunkt der Fahrzeugdurchsuchung bereits ein Anfangsverdacht einer Straftat gegen den Angeklagten vorlag, der auch ein Vorgehen nach den §§ 102, 105 StPO ermöglicht hätte.⁶⁴ Bei solchen doppelfunktionalen Maßnahmen gebe es weder einen allgemeinen Vorrang der Strafprozessordnung gegenüber dem Gefahrenabwehrrecht

63 BGHSt 62, 123 (128).

64 BGHSt 62, 123 (130).

noch umgekehrt.⁶⁵ Die Polizei könne deshalb auch während eines bereits laufenden Ermittlungsverfahrens aufgrund präventiver Ermächtigungsgrundlagen zum Zweck der Gefahrenabwehr tätig werden. Die Verwendung der auf präventivpolizeilicher Grundlage gewonnenen Beweise im Strafverfahren bestimme sich nach § 161 Abs. 2 S. 1 StPO und sei im vorliegenden Fall zulässig.⁶⁶ Eine den Rückgriff auf hypothetische Erwägungen hindernde rechtsmissbräuchliche Umgehung der Anordnungsvoraussetzungen der strafprozessualen Eingriffsmaßnahme sei nicht ersichtlich.⁶⁷ Auch mit Blick auf den Grundsatz des fairen Verfahrens ergebe sich daher kein Beweisverwertungsverbot.

Diese Rechtsprechungslinie hat der 2. Strafsenat seitdem in zwei weiteren, ähnlich gelagerten Fällen konsolidiert.⁶⁸ Sie wirft eine Reihe von Folgefragen auf, denen im vorliegenden Rahmen nicht näher nachgegangen werden kann. Dazu zählen etwa, inwiefern es mit dem aus dem Recht auf ein faires Verfahren folgenden Gebot der Aktewahrheit und Aktenvollständigkeit zu vereinbaren ist, die Hintergrundermittlungen nicht aktenkundig zu machen⁶⁹ oder ob bei der Beschuldigtenbelehrung einzelne Tatvorwürfe aus ermittlungstaktischen Gründen verschwiegen werden dürfen.⁷⁰ Stattdessen sollen abschließend zwei kritische Bemerkungen zur Rechtsprechung des 2. Strafsenats unter dem Blickwinkel der zweckändernden Nutzung von außerstrafprozessual erhobenen Daten im Strafverfahren folgen.

III. ABSCHLIESSENDE BEMERKUNGEN

1. Bemerkung

Der 2. Strafsenat geht für die Beurteilung der Verwendbarkeit der auf der Grundlage des Hessischen Gesetzes über die öffentliche Sicherheit

65 BGHSt 62, 123 (133).

66 Vgl. BGHSt 62, 123 (136).

67 BGHSt 62, 123 (138).

68 Vgl. BGH NStZ 2018, 296 (zollrechtliche Kontrolle des Fahrzeugs nach § 10 ZollVG); BGH StraFo 2018, 348.

69 Dazu etwa *Krehl* StraFo 2018, 265 (270).

70 Albrecht HRRS 2017, 446 (453 ff.); *Brodowski* JZ 2017, 1124 (1128); *Lenk* StV 2017, 692 (698 f.); *Löffelmann* JR 2017, 596 (602); mit geradezu bemerkenswert »praxisfreundlicher« Tendenz *Nowroustian* NStZ 2018, 254 ff.

und Ordnung erlangten Beweismaterials, also insbesondere der bei der Fahrzeugdurchsuchung aufgefundenen Betäubungsmittel, im Strafverfahren gegen den Angeklagten schon formal von der falschen Rechtsgrundlage aus. Die Ermächtigung zum Empfang der präventivpolizeilich erlangten, personenbezogenen Informationen folgt – ungeachtet der hiergegen vorzutragenden verfassungsrechtlichen Bedenken – wenn überhaupt, dann aus der Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 bzw. des § 163 Abs. 1 S. 2 StPO.⁷¹ Für Erwägungen nach dem Prinzip des hypothetischen Ersatzeingriffs auf der Grundlage des vom 2. Strafsenat herangezogenen § 161 Abs. 2 S. 1 StPO bestand vorliegend eigentlich kein Anlass. Nach der StPO ist die Anordnung einer Durchsuchungsmaßnahme gerade nicht auf den Verdacht bestimmter Straftaten beschränkt. Insofern kann aus § 161 Abs. 2 StPO von vornherein keine Verwendungsbeschränkung für das Strafverfahren folgen. Aber selbst wenn man die entsprechenden Ausführungen im Urteil so deutet, dass der 2. Strafsenat das Prinzip des hypothetischen Ersatzeingriffs *contra legem* zum generellen Maßstab für die zweckändernde Nutzung von personenbezogenen Daten im Strafverfahren erheben will,⁷² führt dies im konkreten Fall nicht zu einer Einschränkung. Vielmehr stellt das Gericht ausdrücklich fest, dass hier keine Zweifel daran bestehen, dass die Anordnung einer Durchsuchung auch auf strafprozessualer Grundlage möglich gewesen wäre.

2. Bemerkung

Die Feststellung des Senats, dass es keinen allgemeinen Vorrang der Strafprozessordnung gegenüber dem Gefahrenabwehrrecht gibt, klingt zwar außerordentlich schön, führt aber letztlich nicht weiter. Richtig ist, dass sich polizeiliche Einsatzsituationen in der Praxis ganz häufig als Gemengelagen von Prävention und Repression darstellen. Für sog. *doppelfunktionale Maßnahmen*,⁷³ mit denen sowohl Zwecke der Gefahrenabwehr als auch Strafverfolgungszwecke verfolgt werden,

⁷¹ Vgl. *Brodowski* JZ 2017, 1124 (1127); *Löffelmann* JR 2017, 596 (602); s. auch *Mitsch* NJW 2017, 3124 (3125).

⁷² So interpretiert von *Brodowski* JZ 2017, 1124 (1127).

⁷³ Allg. hierzu etwa *Kingreen/Poscher*, Polizei- und Ordnungsrecht, 10. Aufl. 2018, § 2 Rn. 9 ff.; *Schoch* Jura 2013, 1115 ff.; *Danne* JuS 2018, 434 ff.; *Roggan* GSZ 2018, 52 ff.

hat die Verwaltungsgerichtsbarkeit⁷⁴ die sog. »Schwerpunkttheorie« entwickelt. Entscheidend ist danach, ob die Maßnahme im Schwerpunkt gefahrenabwehrrechtlich geprägt war (dann ist sie insgesamt als präventiv einzustufen und nach § 40 Abs. 1 VwGO vor den Verwaltungsgerichten anzufechten), oder sich nach ihrer Zielrichtung und dem Gesamteindruck für einen verständigen Bürger als strafprozessuale Maßnahme darstellt (so dass sich der Rechtsweg nach den Regelungen der StPO oder nach § 23 EGGVG richtet). Hinter der verwaltungsrechtlichen Schwerpunkttheorie versteckt sich somit die praktisch höchst bedeutsame Frage der Rechtswegzuständigkeit. Der 2. Strafsenat schließt sich mit seinem Postulat vom Nebeneinander von Strafprozess- und Polizeirecht faktisch einer im polizeirechtlichen Schrifttum vertretene Mindermeinung⁷⁵ an, wonach der Betroffene bei doppelfunktionalen Maßnahmen der Polizei sowohl den Verwaltungsrechtsweg als auch den Rechtsweg zu den ordentlichen Gerichten beschreiten müsse. Diese Auffassung, die letztlich möglichen Einschränkungen der Effektivität polizeilicher Aufgabenwahrnehmung begegnen will,⁷⁶ wird überwiegend zu Recht mit dem Hinweis darauf abgelehnt, dass das Nebeneinander zweier Gerichtszuständigkeiten für eine einheitliche polizeiliche Maßnahme weder zumutbar noch für die Klärung von Rechtsfragen zweckdienlich ist.⁷⁷

Will man den Schwerpunkt der Maßnahme bestimmen, so lag dieser hier ohne Zweifel schon mit Blick auf das bereits laufende Ermittlungsverfahren und die zuvor auf strafprozessualer Grundlage angeordneten Überwachungsmaßnahmen auf dem Strafverfahren.⁷⁸ Dass daneben auch die Gefahren durch das Inumlaufbringen der konkreten Menge Kokain abgewehrt werden sollten, fällt daneben kaum ins Gewicht. Schließlich ist das geradezu ein typischer Nebeneffekt jeder

74 BVerwGE 47, 255 (264 f.); 121, 345 (348); OVG Berlin NJW 1971, 637; VGH München NVwZ 1986, 655; VGH Kassel NJW 1999, 3793; VGH Mannheim NVwZ-RR 2005, 540; OVG Lüneburg NVwZ-RR 2014, 327 f.; HambOVG DÖV 2019, 37.

75 S. insbesondere *Schenke*, Polizei- und Ordnungsrecht, 10. Aufl. 2018, Rn. 424; *ders.* NJW 2011, 2838 ff.

76 *Schenke* NJW 2011, 2838 (2842).

77 S. nur *Gusy*, Polizei- und Ordnungsrecht, 10. Aufl. 2017, Rn. 483; *Hufen*, Verwaltungsprozessrecht, 10. Aufl. 2016, § 11 Rn. 61 ff.; *Lenk* NVwZ 2018, 38 (41).

78 Vgl. *Albrecht* HRRS 2017, 446 (449 f.); *Lenk* StV 2017, 692 (695).

strafrechtlichen Verfolgung von Betäubungsmittelkriminalität.⁷⁹ Das Ausweichen auf eine gefahrenabwehrrechtliche Ermächtigungsgrundlage für die Durchsuchung des Fahrzeugs erfolgte auch nicht deshalb, weil es der Polizei vor allem um die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung ging. Die legendierte allgemeine Verkehrskontrolle wird vielmehr nur aus ermittlungstaktischen Erwägungen durchgeführt, um das Ermittlungsverfahren gegen die Hintermänner nicht zu gefährden. Der Rückgriff auf das Gefahrenabwehrrecht ist damit nichts anderes als ein Etikettenschwindel. Dass eine rechtsmissbräuchliche Umgehung der Anordnungsvoraussetzungen für eine strafprozessuale Ermittlungsmaßnahme ein Beweisverwertungsverbot zur Folge hat, ist mittlerweile ein weitgehend anerkannter Grundsatz unseres Strafverfahrensrechts. Entgegen dem 2. Strafsenat liegt ein solcher Missbrauch aber nicht nur dann vor, wenn ein Ausweichen auf das Polizei- oder Nachrichtendienstrecht zur Informationserhebung bewusst das Nichtvorliegen der strafprozessualen Anordnungsvoraussetzungen umschiffen soll. Richtigerweise muss man auch die Fälle des Ausweichens aus sonstigen ermittlungstaktischen Erwägungen wie bei den legendierten Kontrollen entsprechend behandeln, also die Konsequenz eines Beweisverwertungsverbotes ziehen.⁸⁰ Jede Umgehung der StPO als gesamte Rechtsordnung ist per se Rechtsmissbrauch.⁸¹ Wer das mit dem 2. Strafsenat anders sieht, vermengt Polizeirecht, Strafprozessrecht und Nachrichtendienstrecht mit ihren unterschiedlichen Zielsetzungen und Eingriffsschwellen faktisch zu einem »Einheitsbrei« eines allgemeinen Sicherheitsrechts, in dem die strafprozessualen Verfahrenssicherungen entwertet werden und alles dem kollektiven Interesse an effektiver Strafverfolgung untergeordnet ist.⁸² In einem solchen Umfeld aus beliebigem Forum- und Befugnis-Shopping hätte auch die engagierteste Strafverteidigung nicht den Hauch einer Chance.

79 Eindeutig insoweit HambOVG DÖV 2019, 37: »Bei polizeilichen Maßnahmen, die nur deswegen auch präventiven Charakter besitzen, weil durch die Strafverfolgung ein entsprechender unselbständiger präventiver Nebeneffekt erzielt wird, ist das polizeiliche Vorgehen schon nach seiner alleinigen Zwecksetzung ausschließlich strafprozessualer Natur«.

80 *Gubitz* NStZ 2016, 128; *Albrecht* HRRS 2017, 446 (453); *Löffelmann* JR 2017, 596 (601).

81 *Mitsch* NJW 2017, 3124 (3125).

82 Ähnlich *Lenk* StV 2017, 692 (696); *Mitsch* NJW 2017, 3124 (3125); *Roggan* GSZ 2018, 52 (56).