III. Fazit

Welche Impulse gibt also nun die Verfassung, wenn es um das Ob und Wie von Absprachen im Ermittlungsverfahren geht? Das Grundgesetz gibt für die Gestaltung des Strafverfahrens unabdingbare Grundsätze vor, insbesondere den Schuldgrundsatz, die Wahrheitserforschungspflicht, das Rechtsstaatsprinzip (in seinen ebenso zahlreichen wie vagen Facetten), das Recht auf ein faires Verfahren und die Aussagefreiheit. Absprachen im Strafverfahren stehen in einem Spannungsverhältnis zu diesen verfassungsrechtlichen Anforderungen. Es ist jedoch aus verfassungsrechtlicher Sicht weder grundsätzlich erforderlich noch angesichts der faktischen Gegebenheiten empfehlenswert,[129] Absprachen im Ermittlungsverfahren zu untersagen, sofern die dargestellten Einschränkungen durch den Rechtsanwender beachtet werden. Im Übrigen obliegt es dem Gesetzgeber, in den Fällen, in denen der „Wildwuchs" bei den Absprachen im Ermittlungsverfahren den verfassungsrechtlichen Vorgaben zuwiderläuft – und damit meine ich vor allem § 153a StPO –, korrigierend einzugreifen.

129 S. hierzu *Kubiciel*, HRRS 2014, 204 (206 f.).

Informationelle Selbstbestimmung und Sachverhaltserforschung im Ermittlungsverfahren – verfassungsrechtliche Anforderungen an Datenerhebung und Datenverarbeitung

Tobias Singelnstein

I. Informationelle Selbstbestimmung als Impuls

Das Strafverfahren ist im Kern Informationsverarbeitung. Die meisten der dabei verarbeiteten Informationen stellen personenbezogene Daten im Sinne des Rechts auf informationelle Selbstbestimmung (RiS) aus Art. 2 I i.V.m. Art. 1 I GG dar. Mit dem Volkszählungsurteil von 1983 und der folgenden verfassungsgerichtlichen Rechtsprechung hat das Bundesverfassungsgericht daher einen denkbar starken Impuls (auch) in Richtung des Strafverfahrens ausgesandt, der gerade für das an Datenerhebungen und Datenverarbeitungen reiche Ermittlungsverfahren von Bedeutung ist.[1] Schließlich stellt das RiS besondere Anforderungen sowohl für die Erhebung als auch für die Verwendung personenbezogener Daten auf. Wo speziellere Grundrechte – insbesondere Art. 10 I GG – dem RiS vorgehen, setzen diese die Anforderungen in entsprechender Weise um.[2]

Die Hürden, die das RiS für die Datenerhebung und -verwendung im Strafverfahren aufbaut, sind grundsätzlich nicht sehr hoch und schnell skizziert. Erstens stellen sowohl die Erhebung wie auch die weitergehende Verarbeitung und Nutzung personenbezogener Daten Grundrechtseingriffe dar. Sie bedürfen daher jeweils einer gesetzlichen Grundlage und müssen sich auf überwiegende Belange des Allgemeinwohls stützen können.[3] Zweitens ist bei jeder Verarbeitung und Nutzung solcher Daten im An-

1 Zusammenfassend *Singelnstein* ZStW 120 (2008), 854, 857 ff.
2 BVerfGE 124, 43, 60 f. zu Art. 10 I GG.
3 KK StPO-*Gieg*, 7. Aufl. 2013, Vor § 474 Rn 1 f.; SK StPO-*Weßlau*, 4. Aufl. 2010 ff., Vor § 474 Rn 4.

schluss an die Erhebung der Zweckbindungsgrundsatz zu beachten.[4] Danach dürfen die Daten ohne Weiteres nur für den Zweck genutzt werden, zu dem sie auch erhoben wurden. Diese Bindung an den Erhebungszweck begrenzt die Eingriffstiefe, die sich mit jeder Nutzung zu weiteren Zwecken intensiviert.[5] Eine Nutzung zu weiteren Zwecken, wie zum Beispiel zur Gefahrenabwehr, ist zwar nicht ausgeschlossen. Sie stellt aber einen Grundrechtseingriff dar, der dem der Datenerhebung entspricht, so dass auch für eine solche Zweckumwidmung eine Rechtsgrundlage sowie überwiegende Belange des Allgemeinwohls gegeben sein müssen. Drittens schließlich ist – wie bei Grundrechtseingriffen stets – der Grundsatz der Verhältnismäßigkeit zu beachten. Insbesondere dürfen Daten nur in dem Umfang erhoben und verarbeitet werden, wie dies für den jeweiligen konkreten Zweck auch erforderlich ist.[6]

Zusammenfassend betrachtet bedürfen Maßnahmen der Datenerhebung, Datennutzung und Datenverarbeitung im Strafverfahren damit vor allem jeweils einer gesetzlichen Grundlage und müssen verhältnismäßig sein. Die überwiegenden Belange des Allgemeinwohls können grundsätzlich im Ziel des Strafverfahrens gesehen werden, d. h. in der umfassenden Sachverhaltserforschung mit dem Ziel der Ermittlung der materiellen Wahrheit sowie der Verwirklichung des staatlichen Strafanspruchs.[7]

II. Resonanzen

Bei der Umsetzung dieser Vorgaben hat sich der Gesetzgeber zunächst viel Zeit gelassen. Erst mit dem StVÄG 1999 hat er die §§ 161, 163 StPO zu Ermittlungsgeneralklauseln aufgewertet[8], die insbesondere (niedrigschwellige) Eingriffe in das RiS gestatten sollen.[9] Ebenso wurden im Zuge der Reform umfassendere gesetzliche Regelungen zur Verarbeitung und Verwendung personenbezogener Daten im Strafverfahren in den

4 Allgemein BVerfGE 65, 1, 46; 100, 313, 360; *Eisenberg*, Beweisrecht der StPO, 8. Aufl. 2013, Rn 2470a.
5 *Gusy* ZJS 2012, 155, 156.
6 KK StPO-*Gieg*, § 483 Rn 3; SK StPO-*Weßlau*, § 484 Rn 11.
7 S. allgemein BVerfGE 77, 65, 76 m.w.N.
8 Dazu *Hefendehl* StV 2001, 700 ff.; *Hilger* NStZ 2000, 561, 564.
9 *Meyer-Goßner*, StPO, 57. Aufl. 2014, § 161 Rn 1; LR StPO-*Erb*, 26. Aufl. 2006 ff., § 161 Rn 3b.

§§ 474 ff. StPO eingeführt. Gleichwohl ist der Impuls informationeller Selbstbestimmung auf Seiten des Strafverfahrens nur auf verhaltene Resonanz gestoßen und finden die Anforderungen des RiS hier nur unzureichend Beachtung. Dies lässt sich im Wesentlichen auf zwei Umstände zurückführen.

Zum einen befindet sich informationelle Selbstbestimmung nicht nur in direktem Gegensatz zum Ziel des Strafverfahrens. Das Konzept des Grundrechtsschutzes in diesem Bereich liegt auch quer zu den gewachsenen dogmatischen Strukturen des Strafverfahrensrechts, das im Prinzip von einer allgemeinen Befugnis der Strafverfolgungsbehörden zur Verarbeitung personenbezogener Daten ausgeht.[10] Insbesondere die Praxis tut sich schwer, ihren Alltag den „neuen", deutlich veränderten Anforderungen anzupassen. Zum anderen eröffnet der technische Fortschritt quasi im Wochentakt neue Möglichkeiten zur Erhebung und Auswertung von Daten, die mitunter eine andere Eingriffsstruktur bedeuten als klassische strafprozessuale Eingriffe, wie etwa die Funkzellenabfrage oder das Data Mining zeigen.[11] Besonders bedeutsam sind insofern die Veränderungen, die die Digitalisierung mit sich bringt. Derartige Datenbestände können beliebig vervielfältigt werden, sind einfach zu transferieren und lassen sich automatisiert auswerten.

Weniger Defizite zeigen sich im Bereich der Datenerhebung. Für die zahlreichen Informationseingriffe zur Erhebung personenbezogener Daten kennt die StPO neben den Ermittlungsgeneralklauseln heute eine ganze Reihe von Rechtsgrundlagen, die die verschiedenen Eingriffe speziell regeln.[12] Als problematisch erweisen sich hier insbesondere die überdehnende Anwendung der Generalklauseln der §§ 161 I, 163 I StPO wie auch spezieller Eingriffsbefugnisse[13] – etwa im Fall neuer technischer Möglichkeiten, für die noch keine eigenständige Rechtsgrundlage zur Verfügung steht – sowie die kumulative Anwendung einer Vielzahl von Erhe-

10 *Singelnstein* ZStW 120 (2008), 854, 865 ff.
11 Zur Funkzellenabfrage *Singelnstein* JZ 2012, 601 ff.
12 Allgemein zum Vorbehalt des Gesetzes LR StPO-*Menges*, 26. Aufl. 2006 ff., Vor § 94 Rn 23 ff.
13 *Hefendehl* StV 2001, 700, 702; SK StPO-*Wohlers*, 4. Aufl. 2010 ff., § 161 Rn 9.

bungsmaßnahmen[14], die ggf. bis zur Erstellung eines umfassenden Persönlichkeitsprofils reichen kann.

Deutlich defizitärer ist die strafprozessuale Resonanz auf den Impuls durch das RiS im Bereich der Nutzung und Verarbeitung der gewonnenen personenbezogenen Daten. Während die Verwertung der Daten in dem Strafverfahren, für das sie erhoben wurden, grundsätzlich durch die jeweilige Erhebungsnorm – ggf. i.V.m. §§ 244 II, 261 StPO – gedeckt ist, und „nur" durch den Grundsatz der Verhältnismäßigkeit begrenzt wird, muss jede darüber hinausgehende Verarbeitung und Verwendung den eingangs beschriebenen Anforderungen genügen. Dies gilt sowohl für die Speicherung in Dateien und die Nutzung der Daten als insbesondere auch die zweckändernde Verwendung der Daten über das jeweilige konkrete Strafverfahren hinaus – etwa in weiteren Strafverfahren, aber auch zu sonstigen staatlichen Zwecken.[15]

III. Einzelne Fragestellungen

Wo das Gegensatzpaar informationelle Selbstbestimmung und Sachverhaltserforschung in Streit gerät, setzen sich in der Praxis eher die überkommenen strafprozessualen als die verfassungsrechtlichen Maßstäbe durch – obgleich das RiS und die mit diesem gewachsene Dogmatik einen rechtlichen Rahmen für den Umgang mit personenbezogenen Daten bereitstellt, der nicht nur verbindlich ist, sondern für zahlreiche strafprozessuale Problemkonstellationen auch eine wertvolle Grundlage für Lösungsansätze darstellen könnte.

1. Datenbeschlagnahme

Die Beschaffung von gespeicherten Daten bei Beschuldigten und Dritten – auf Computern, mobilen Endgeräten, in Cloud-Speichern u.a.m. – hat eine nach wie vor zunehmende Relevanz.[16] Dabei bestehen in der Praxis offenbar divergierende Auffassungen darüber, auf welche Rechtsgrundlage solche Maßnahmen zu stützen sind. Erfolgt die Erhebung im Rahmen einer Durchsuchung, wird sie wohl zumeist mit § 94 StPO gerechtfertigt, und zwar auch dann, wenn nicht die Datenträger als Gegenstände, sondern nur die darauf befindlichen Daten sichergestellt werden.[17] Begehren die Strafverfolgungsbehörden hingegen alleine, also unabhängig von einer Durchsuchung, die Herausgabe bestimmter, für das Verfahren bedeutsamer Daten – etwa von Unternehmen als Dritten –, wird dies in der Praxis häufig auch auf die §§ 161 I, 163 I StPO als Ermittlungsgeneralklauseln gestützt.[18]

Diese divergierende Vorgehensweise ist nicht sachgerecht und die Beschaffung von Daten für das Strafverfahren vielmehr einheitlich auf eine Rechtsgrundlage zu stützen. Die §§ 94 ff. StPO sind dabei in der Vergangenheit mit gewichtigen Argumenten abgelehnt worden.[19] Zentral ist insbesondere das des Wortlauts, der in § 94 I, II StPO von „Gegenständen" spricht.[20] Versteht man den Begriff eng, kann dies zwar den jeweiligen Datenträger, nicht aber die darauf gespeicherten Daten erfassen – auf die es aber gerade ankommt und auf deren Vervielfältigung sich die Strafverfolgungsbehörden aus Gründen der Verhältnismäßigkeit oft auch zu beschränken haben werden. Angesichts dessen wird teilweise vertreten, dass die Sicherstellung alleine der gespeicherten Daten als Minusmaßnahme von §§ 94 ff. StPO gedeckt sei.[21] Für eine Lösung in diese Richtung spricht, dass die Ermittlungsgeneralklauseln als Rechtsgrundlage keine bessere Lösung bereithalten. Zudem ist die neuere Rechtsprechung des Bundesverfassungsgerichts zum strafprozessualen Zugriff auf Datenbestände zu berücksichtigen. In der Entscheidung zum Zugriff auf E-Mails hat das Gericht entschieden, dass auch gespeicherte Daten als nichtkörperliche Dinge unter den Wortsinn des Begriffs „Gegenstände" in § 94 I, II

14 Dazu *Puschke*, Die kumulative Anordnung von Informationsbeschaffungsmaßnahmen im Rahmen der Strafverfolgung, 2006.
15 Zu den zahlreichen offenen Fragen in diesem Feld *Singelnstein* ZStW 120 (2008), 854, 873 ff.
16 S. zum Ganzen *Singelnstein* NStZ 2012, 593, 602 ff.
17 Dazu BVerfGE 113, 29, 49; *Meyer-Goßner*, StPO, § 94 Rn 16a.
18 S. etwa *BVerfG* NJW 2009, 1405; s. auch *BVerfG* K&R 2011, 320, 323.
19 *Roxin/Schünemann*, Strafverfahrensrecht, 27. Aufl. 2012, § 34 Rn 4; SSW StPO-*Eschelbach*, 2014, § 94 Rn 7; zur Beschaffung von Daten bei TK-Anbietern *Brodowski* JR 2009, 402, 406; *Gaede* StV 2009, 96, 98 ff.; *Kudlich* GA 2011, 193, 202 f.; *Klesczewski* ZStW 123 (2011), 737, 746 ff.; SK StPO-*Wolter*, 4. Aufl. 2010 ff., § 100a Rn 32 ff.
20 SK StPO-*Wohlers*, § 94 Rn 26.
21 LR StPO-*Menges*, § 94 Rn 14; *Schlegel* HRRS 2008, 23, 24 f.

StPO gefasst werden könnten.[22] Auch wenn eine eigenständige bzw. jedenfalls eine im Wortlaut klare Rechtgrundlage für die Sicherstellung von Daten vorzugswürdig wäre, ist es vor diesem Hintergrund überzeugender, für entsprechende Eingriffe die §§ 94 ff. StPO heranzuziehen.[23] Bei Privaten gespeicherte Daten können dementsprechend nach § 94 I StPO sichergestellt oder nach § 94 II i.V.m § 98 I StPO beschlagnahmt werden; neben dem Richtervorbehalt sind dabei weitere Verfahrensregelungen zu beachten, insbesondere handelt es sich um eine offene Maßnahme[24]. Dies bedeutet im Gegenzug aber auch, dass die §§ 161 I, 163 I StPO keine geeigneten Rechtsgrundlagen für die Sicherstellung von Daten bzw. ein entsprechendes Auskunftsverlangen darstellen, sondern vielmehr als subsidiär zurücktreten, so dass die §§ 94 ff. StPO die alleinigen Rechtsgrundlagen für alle Formen der (offenen) Beschaffung von bei Privaten gespeicherten Daten darstellen.[25]

Angesichts der niedrigen Eingriffsvoraussetzungen einerseits sowie des Umfangs und der Aussagekraft gespeicherter Daten andererseits kommt bei derartigen Maßnahmen dem Grundsatz der Verhältnismäßigkeit eine ganz besondere Bedeutung zu.[26]

2. Verwertungsverbote als Frage informationeller Selbstbestimmung

Weiterhin lässt sich auch die Frage der Verwertungsverbote aus der Perspektive informationeller Selbstbestimmung betrachten. Beweisverwertung im Strafverfahren ist wie eingangs festgestellt Informationsverarbeitung und stellt also eine spezielle Form der Verwendung personenbezogener Daten dar, soweit es sich um solche Daten handelt.[27] Sie muss daher den eingangs genannten Anforderungen aus dem RiS genügen, d.h. sie muss sich auf eine Rechtsgrundlage stützen können, überwiegenden Allgemeinwohlbelangen dienen und verhältnismäßig sein.

22 BVerfGE 124, 43, 58 ff.; s. auch schon BVerfGE 113, 29, 50; 115, 166, 190 ff.
23 *Meyer-Goßner*, StPO, § 94 Rn 16a m.w.N.
24 Dazu *Singelnstein* NStZ 2012, 593, 603.
25 *Singelnstein* NStZ 2012, 593, 602 f.
26 BVerfGE 124, 43, 66 f.; *Meyer-Goßner*, StPO, § 94 Rn 18a ff.
27 *Singelnstein* ZStW 120 (2008), 854, 865 ff. m.w.N.

Vergleichsweise unproblematisch ist dies im Fall der Verwertung rechtmäßig erlangter Beweismittel. Hier können als Rechtsgrundlage die jeweiligen Erhebungsbefugnisse – ggf. i.V.m. §§ 244 II, 261 StPO – fungieren. Da eine Erhebung ohne Befugnis zur Nutzung der erhobenen Daten wenig Sinn machen würde, kann davon ausgegangen werden, dass die Regelungen eine solche Befugnis enthalten.[28] Auch die Einhaltung der beiden anderen Voraussetzungen bereitet kaum Probleme: Sofern das Beweismittel für das Verfahren relevant ist und die Erhebung rechtmäßig war, ist die Verwertung grundsätzlich verhältnismäßig und dient im Rahmen des Strafverfahrens überwiegenden Allgemeinwohlbelangen.

Deutlich anders liegen die Dinge hingegen, wenn die Erhebung der Beweismittel rechtswidrig erfolgt ist, so dass sich die Frage nach einem Verwertungsverbot stellt. Während die strafprozessuale Perspektive angesichts der herrschenden Abwägungsdoktrin an dieser Stelle keine prinzipiellen Probleme mit einer Nutzung rechtswidrig erlangter Daten hat und vielmehr ein Verbot dessen für begründungsbedürftig hält[29], stellt sich die Sache aus Perspektive des RiS genau entgegengesetzt dar. Zwar schließt Art. 2 I i.V.m. Art. 1 I GG eine Nutzung derart erlangter personenbezogener Daten nicht generell aus. Diese stellt aber einen erheblich intensiveren Eingriff dar, als wenn die Daten rechtmäßig erlangt worden wären.[30] Es handelt sich um eine begründungsbedürftige Sondersituation[31]. Die sich aus der Verfassung ergebenden Anforderungen an eine Verwendung personenbezogener Daten gelten hier daher in gesteigertem Maße. Aus der Perspektive informationeller Selbstbestimmung lautet die Frage demnach nicht, ob ein Verwertungsverbot besteht, sondern ob die Verwendung der rechtswidrig erhobenen personenbezogenen Daten im Einzelfall trotzdem gestattet ist.[32]

28 *Dallmeyer*, Beweisführung im Strengbeweisverfahren, 2. Aufl. 2008, 123; aus dem Grundsatz der freien Beweiswürdigung alleine ableitend *Rogall* JZ 2008, 818, 824 ff.
29 S. zu diesem Ansatz die Darstellungen bei *Eisenberg*, Beweisrecht der StPO, Rn 364 ff.; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus – Gutachten C zum 67. Deutschen Juristentag Erfurt 2008, 2008, C 38, C 58 ff.
30 *Singelnstein* NStZ 2012, 593, 604.
31 *Petri*, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Rn 378.
32 *Singelnstein* NStZ 2012, 593, 604; s. auch *Gusy* HRRS 2009, 489, 490 ff.

Auch hierfür bedürfte es zunächst einer dies gestattenden Rechtsgrundlage. Die jeweiligen Erhebungsbefugnisse scheiden dabei aus, da deren Voraussetzungen ja gerade nicht vorgelegen haben.[33] In Betracht kämen somit noch die §§ 244 II, 261 StPO.[34] Allerdings sind beide Vorschriften deutlich älter als das RiS, weisen schon nicht die Struktur einer Eingriffsbefugnis auf und können auch hinsichtlich des Bestimmtheitsgebots kaum als Rechtsgrundlage für einen Grundrechtseingriff herhalten. Nach zutreffender Auffassung fehlt es daher an einer hinreichenden Befugnis für die Verwertung rechtswidrig erlangter Beweismittel.[35]

Die inhaltlichen Anforderungen, die eine solche Rechtsgrundlage umsetzen müsste – in der Regel vor allem überwiegendes Allgemeinwohl bei einer Abwägung mit den Interessen des Betroffenen im Einzelfall und Verhältnismäßigkeit –, werden zwar auch im Rahmen der Abwägungslehre berücksichtigt. Dies geschieht in der Praxis jedoch in unsystematischer[36] und zu recht vielfach kritisierter Weise.[37] Die Schaffung einer Rechtsgrundlage böte für den Gesetzgeber die Gelegenheit, die Kriterien für eine solche Abwägung – die sich in weiten Teilen aus der Verfassung ableiten lassen[38] – und deren Gewicht zu regeln und die Abwägung damit klarer und hinsichtlich des Ergebnisses vorhersehbarer zu machen. Der Praxis wäre damit eine Struktur für die Beantwortung der Frage nach der Verwendbarkeit rechtswidrig erhobener Beweise an die Hand gegeben, die auch der damit verbundenen Fachdebatte stärkere Konturen verleihen

33 Vgl. *Jahn/Dallmeyer* NStZ 2005, 279, 303.

34 So BVerfGE 130, 1, 29; für § 244 II StPO *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus – Gutachten C zum 67. Deutschen Juristentag Erfurt 2008, 2008, C 38, C 68 f.; für § 261 StPO *Rogall* JZ 2008, 818, 825.

35 So bereits *Dallmeyer*, Beweisführung im Strengbeweisverfahren, S. 124; *Singelnstein* FS Eisenberg, 653 ff.

36 Zu den Kriterien der Abwägungslehre zusammenfassend *Gusy* HRRS 2009, 489, 490 ff.

37 S. nur die Nachweise bei *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus – Gutachten C zum 67. Deutschen Juristentag Erfurt 2008, 2008, C 38, C 47 f.

38 *Gusy* HRRS 2009, 489, 491 ff.

würde, so wie dies derzeit im Zusammenhang mit § 257c StPO für die Absprachen zu beobachten ist.

Etwas anderes kann im Fall geschriebener Verwertungsverbote gelten, die aus Sicht des RiS als spezielle Verwendungsregelungen zu verstehen sind.[39] Sie schließen die Nutzung von Beweisen in den von ihnen erfassten Konstellationen unter bestimmten Voraussetzungen aus, woraus umgekehrt ggf. geschlossen werden kann, dass die Nutzung der Daten bei Nichtvorliegen der Voraussetzung gestattet sein soll.

Genau genommen fehlt es somit in den meisten Fällen rechtswidriger Beweiserhebung an einer hinreichend bestimmten und differenzierten Rechtsgrundlage für eine Verwertung, so dass die Beweise nicht verwendet werden dürften. Gerade an dieser Stelle setzen Praxis und Gesetzgeber indes den Impuls des RiS nicht um, sondern räumen den überkommenen Strukturen des Strafverfahrensrechts den Vorrang ein. Dies bedeutet nicht alleine, dass Grundrechtseingriffe durch die Verwendung rechtswidrig erhobener personenbezogener Daten ohne hinreichende Rechtsgrundlage Alltag sind. Die Rechtsprechung überträgt diesen bislang noch auf den speziellen Bereich der Beweisverwertung beschränkten Maßstab vielmehr auch auf andere Formen der Datenverwendung – etwa die Frage der Zweckumwidmung rechtswidrig erhobener Daten[40] – und drängt die Anforderungen aus dem RiS damit sogar noch zurück.[41]

3. Zweckumwidmung

Nur verhaltene Aufmerksamkeit genießt in der Praxis des Strafverfahrens weiterhin auch der Zweckbindungsgrundsatz. Dieser stellt wie eingangs beschrieben verfassungsrechtliche Anforderungen für eine Verwendung erhobener Daten zu weiteren Zwecken als dem Erhebungszweck auf, da dies wie ein neuerlicher Grundrechtseingriff wirkt. Der Erhebungszweck im Strafverfahren besteht in der Aufklärung der jeweiligen prozessualen Tat, die Gegenstand des Verfahrens ist.[42] Daher stellt sowohl die Nutzung für andere Strafverfahren wie auch für präventivpolizeiliche oder sonstige

39 *Singelnstein* ZStW 120 (2008), 854, 865 ff. m.w.N.

40 BVerfGE 130, 1, 27 zu BGHSt 54, 69.

41 Dazu *Singelnstein* NStZ 2012, 593, 604 f.

42 BVerfGE 109, 279, 375 f.; 113, 29, 51 f.; 115, 166, 191; 124, 43, 61; s. auch LR StPO-*Hilger*, 26. Aufl. 2006 ff., Vor § 474 Rn 7 f.

staatliche Zwecke eine rechtfertigungsbedürftige Zweckentfremdung dar.[43]

Für eine derartige Zweckumwidmung gilt nach überwiegender Auffassung das Zwei-Türen-Modell. Danach muss die Zweckumwidmung sowohl auf Seiten des ursprünglichen Erhebungszwecks durch eine Rechtsgrundlage gestattet sein, als auch auf Seiten des neuen Verwendungszwecks.[44] Bei den angesichts dessen erforderlichen Rechtsgrundlagen differenziert die StPO zwischen Daten, die mit besonders eingriffsintensiven Maßnahmen erlangt wurden, die nur beim Verdacht bestimmter Straftaten zulässig sind, und Daten die mittels sonstiger Maßnahmen erlangt wurden. Zudem lassen sich drei Konstellationen der Zweckumwidmung differenzieren.[45]

Sollen in einem Strafverfahren erhobene Daten in einem anderen Strafverfahren genutzt werden, richtet sich dies bei einfach erhobenen Daten nach den §§ 474 I, 479 StPO, die nur die Erforderlichkeit verlangen.[46] Besonders eingriffsintensiv erlangte Daten dürfen hingegen nach § 477 II S. 2 StPO nur umgewidmet werden, wenn die Erhebungsmaßnahme in dem neuen Verfahren ebenfalls hätte angeordnet werden dürfen. Für diesen hypothetischen Ersatzeingriff müssen die Voraussetzungen der jeweiligen Erhebungsbefugnis umfassend vorliegen.[47]

Die Nutzung von in einem Strafverfahren erhobenen Daten für sonstige staatliche Zwecke bestimmt sich bei einfach erhobenen Daten nach § 474 II StPO[48] sowie für die Gefahrenabwehr nach der Generalklausel des § 481 StPO. Besonders eingriffsintensiv erlangte Daten dürfen nach § 477 II S. 3 StPO nur zu den dort genannten Zwecken umgewidmet werden. Auf Seiten des neuen Verwendungszwecks sind jeweils dem entsprechende Rechtsgrundlagen erforderlich.

Sollen zu sonstigen staatlichen Zwecken erhobene Daten in einem Strafverfahren genutzt werden, ist dies bei einfach erhobenen Daten nach

43 BVerfGE 100, 313, 360 f., 385; 109, 279, 375 ff.; 110, 33, 68 ff.; umfassend *Singelnstein* ZStW 120 (2008), 854, 857 ff.

44 SK StPO-*Weßlau*, Vor § 474 Rn 15; *Wolter*, FS Rieß, 633, 646 f.; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, 211 f.

45 S. zum Folgenden bereits *Singelnstein* NStZ 2012, 593, 605 f.

46 Dazu LR StPO-*Hilger*, § 474 Rn 6; SK StPO-*Weßlau*, § 474 Rn 8.

47 *Singelnstein* ZStW 120 (2008), 854, 880 ff.

48 Dazu *Brodersen* NJW 2000, 2536, 2540 f.

den §§ 161 I, 163 I StPO möglich, die das Auskunftsersuchen gegenüber anderen Behörden ausdrücklich regeln.[49] Für besonders eingriffsintensiv erlangte Daten finden sich wiederum spezielle Regelungen in § 161 II, III StPO. Auch hier bedarf es darüber hinaus grundsätzlich auch auf Seiten des ursprünglichen Erhebungszwecks einer Rechtsgrundlage, die die Zweckumwidmung erlaubt.[50]

Nach richtiger, aber bestrittener Auffassung können diese Vorschriften, die eine Umwidmung rechtswidrig erhobener Daten nicht speziell regeln, nur für eine Umwidmung rechtmäßig erlangter Daten herhalten.[51] Weiterhin darf die Zweckumwidmung nicht durch strafprozessuale Verwendungsregelungen ausgeschlossen sein, die die Daten absolut an einen bestimmten Zweck binden oder ein Verwendungsverbot vorsehen (s. beispielsweise § 100a IV S. 2 StPO, § 101 VIII S. 3 StPO).[52]

4. Data Mining

Vor neuen Herausforderungen steht das Strafverfahrensrecht schließlich im Bereich der Auswertung personenbezogener Daten. Neue technische Möglichkeiten, die sich noch sehr stark in der Entwicklung befinden, ermöglichen umfassendere und vielseitigere Auswertungen von gespeicherten Datenbeständen. Neben den bereits bestehenden polizeilichen Datenbanken etabliert sich an dieser Stelle derzeit ein Markt für spezielle Ermittlungsprogramme, die die Zusammenführung und komplexe Auswertung von sehr unterschiedlichen Datenarten ermöglichen, um so einen Mehrwert an Erkenntnis zu gewinnen.[53]

Dabei können verschiedene Formen der Anwendung unterschieden werden. Rechtlich weniger problematisch ist es, wenn entsprechende Da-

49 HK StPO-*Zöller*, 5. Aufl. 2012, § 161 Rn 3; KK StPO-*Griesbaum*, § 161 Rn 2.

50 Allgemein dazu *Singelnstein* ZStW 120 (2008), 854, 860 ff.

51 *Singelnstein* NStZ 2012, 593, 604 f.; SK StPO-*Weßlau*, § 477 Rn 16; BeckOK StPO-*Wittig*, 18. Ed. 2014, § 477 Rn 5; s. aber BGHSt 54, 69, 87 f.; s. auch KK StPO-*Griesbaum*, § 161 Rn 40; *Hefendehl* StV 2001, 700, 706; *Zöller*, in: Roggan/Kutscha, Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006, S. 497 f.

52 SK StPO-*Weßlau*, § 477 Rn 9.

53 S. etwa *Henrichs/Wilhelm* Kriminalistik 2010, 30, 32 f.; *Schulzki-Haddouti* CILIP 1/2011, 32, 37 f.

tenbanken und Auswertungen im Rahmen eines konkreten Ermittlungsverfahrens genutzt werden. Beschränkt sich die Auswertung auf personenbezogene Daten, die im Rahmen der Ermittlungen zulässig erhoben wurden, wird die Speicherung und Nutzung der Daten regelmäßig von § 483 StPO gedeckt sein.[54] Ein maschineller Abgleich mit sonstigen zur Strafverfolgung oder Gefahrenabwehr bereits gespeicherten Daten ist nach § 98c StPO zulässig.

Deutlich anders stellt sich die Sachlage dar, wenn personenbezogene Daten zu anderen Zwecken als einem bestimmten Ermittlungsverfahren weiterverwendet werden sollen, insbesondere zur Strafverfolgungsvorsorge oder zur Gefahrenabwehr vor allem in entsprechenden polizeilichen Datenbanken. Hier stellen die bestehenden Regelungen, bspw. § 484 StPO, deutlich höhere Hürden auf und gestatten häufig nur die Speicherung bzw. Übermittlung und Nutzung bestimmter Daten. Zugleich sorgt auch die Erforderlichkeitsprüfung für einen strengeren Maßstab, da konkret dargelegt werden muss, warum welche Daten in Zukunft für Strafverfolgungsvorsorge oder Gefahrenabwehr notwendig sind und daher gespeichert und genutzt werden dürfen.[55] Hintergrund dessen ist die mit einer solchen Übermittlung und Speicherung verbundene Zweckumwidmung.[56] Die Daten sollen nun nicht mehr nur für ein bestimmtes Ermittlungsverfahren genutzt werden, sondern allgemein für Zwecke der Strafverfolgungsvorsorge und Gefahrenabwehr zur Verfügung stehen. Diese starke Erweiterung der Zweckbestimmung bedeutet eine erheblich gesteigerte Eingriffsintensität.

Data Mining und vergleichbare Formen der Datenauswertung sind damit auf die Anwendung in konkreten Ermittlungsverfahren beschränkt, wo sie in den genannten Grenzen (nur) zur Aufklärung der jeweiligen prozessualen Tat zulässig sind. Nicht gestattet sind eine solche Nutzung personenbezogener Daten und die damit verbundene Zweckumwidmung hingegen für die allgemeinen Zwecke der Gefahrenabwehr und Strafverfolgungsvorsorge. Für diese darf einerseits nur ein bestimmter Bestand an Daten gespeichert werden; andererseits sind auch die Befugnisse zur Nutzung an bestimmte Anlässe und Zwecke gebunden.[57] Insbesondere eine

54 S. für intelligente Analyse- und Verknüpfungsprogramme im Wirtschaftsstrafrecht SK StPO-*Weßlau*, § 483 Rn 6.
55 Hierzu *Gusy* ZJS 2012, 155, 158 f.
56 Dazu allgemein bereits oben 3.
57 S. allgemein *Gusy* ZJS 2012, 155, 158.

anlassunabhängige Lageaufklärung oder statistische Auswertung solcher Datenbestände sind daher nicht zulässig, soweit die Daten nicht anonymisiert sind und also den Schutz des RiS genießen.

IV. Ausblick

Wesentliche Voraussetzung für eine gezielte Entwicklung des Rechts des Ermittlungsverfahrens aufgrund des Impulses informationeller Selbstbestimmung scheint mir zunächst zu sein, ein stärkeres Bewusstsein für die Rolle des RiS als grundlegendem Maßstab im Kontext des Strafverfahrens zu etablieren. Insofern wäre es hilfreich, die verschiedenen Befugnisse und Institute der StPO systematisch aus dieser Perspektive zu untersuchen, wie dies hier im Ansatz für die Beweisverbotslehre getan wurde, und die Befunde dessen mit der strafprozessualen Perspektive zusammenzubringen.

Darüber hinaus scheint mir besonders bedeutsam, den sich aus dem RiS ergebenden rechtlichen Grenzen und Anforderungen im Strafverfahren stärker zu praktischer Geltung zu verhelfen. Dies gilt erstens für materielle Grenzen wie den Kernbereichsschutz und das Verbot der Erstellung von Persönlichkeitsprofilen. Zweitens ist der Schutz des RiS wie dargestellt stark abhängig davon, dass personenbezogene Daten einem konkreten Verwendungszweck zugeordnet sind. Dies macht es einerseits erforderlich, personenbezogene Daten entsprechend zu kennzeichnen und untereinander zu trennen. Andererseits müssen die Möglichkeiten der Zweckumwidmung beschränkt sein und dürfen nur zu festgelegten Zielen und konkret bestimmten Voraussetzungen zugelassen werden. Gerade hier können die bestehenden Regelungen noch klarer und bestimmter wie auch enger gefasst werden und wäre ein kohärentes System strafprozessualer Verwendungsregelungen anzustreben.[58] Ebenso wäre es denkbar, die Zweckumwidmung besonders eingriffsintensiv erhobener Daten einem Richtervorbehalt zu unterstellen.[59] Drittens schließlich muss die Speicherung personenbezogener Daten zeitlich begrenzt sein, wofür die Einrichtung und Einhaltung von flächendeckenden Überwachungspflichten und Löschungsgeboten erforderlich sind.

58 Dazu auch *Gusy* HRRS 2009, 489, 491 f.; *Vogel* ZIS 2012, 480, 483 f.
59 So ein Gesetzentwurf der Grünen, BT-Drs. 17/7033 v. 21.9.2011.