BUCHBESPRECHUNGEN

Thomas Kahler: Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten

von OStA Dieter Kochheim

2017, Nomos Verlag, Baden-Baden, ISBN 978-3-8487-3978-3, S. 193, Euro 49.

Die von *Prof. Dr. Cornelius Prittwitz* und *Prof. Dr. Dres. hc Spiros Simitis* betreute Studie (S. 7)[1] nimmt den Beschluss des *BVerfG* vom 17.2.2009[2] zum Anlass, die verfassungs- und europarechtliche Anwendungsweite der Ermittlungsgeneralklausel des § 161 Abs. 1 StPO[3] zu prüfen, die die Staatsanwaltschaft zu „Ermittlungen jeder Art ermächtigt, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln". Ihm liegt ein Ermittlungsverfahren der Staatsanwaltschaft Halle wegen des Verdachts des Sich-Verschaffens kinderpornografischer Abbilder im Zusammenhang mit einem kostenpflichtigen Internetangebot aus dem Jahr 2006 zugrunde (Aktion Mikado):[4] „Für den Zugang zu der Internetseite mussten 79,99 $ per Kreditkarte gezahlt werden. Die Staatsanwaltschaft … schrieb daher die Institute an, die Master Card- und Visa-Kreditkarten in Deutschland ausgeben, und forderte sie auf, alle Kreditkartenkonten anzugeben, die seit dem 1. März 2006 eine Überweisung von 79,99 $ an die philippinische Bank aufwiesen, über die der Geldtransfer für den Betreiber der Internetseite abgewickelt wurde. Anschließend teilte die Staatsanwaltschaft noch die zwischenzeitlich bekannt gewordene „Merchant-ID", die dem Zahlungsempfänger durch die Bank zugewiesene Ziffernfolge, für den Betreiber der Internetseite mit. Die Unternehmen übermittelten der Staatsanwaltschaft daraufhin die erbetenen Informationen … Insgesamt wurden so 322 Karteninhaber ermittelt." Hierzu mussten – laut *Kahler* – die Kreditkartenkartenunternehmen auf „rund 22 Mio. Kreditkartenkonten zugreifen, um Verdächtige nach bestimmten Suchkriterien auszusondern" (S. 17[5]).

Kahler betrachtet die Ermittlungsmaßnahme als einen Massenzugriff der Staatsanwaltschaft auf die Daten Unbeteiligter im Wege der Auftragsverarbeitung (§ 11 BDSG a.F.; §§ 62 ff. BDSG n.F.) und folgert daraus eine datenschutzrechtliche Mitteilungspflicht gegenüber allen Inhabern von Kreditkartenkonten, die an den Suchläufen beteiligt waren (S. 46 f.; S. 75, 82; nach Maßgabe von Art. 12 der [Datenschutz-] Richtlinie 95/46/EU: S. 87 f.).

Seine Argumentation ist in kurzer Form folgende: Aufgrund des Auskunftsverlangens der Staatsanwaltschaft veranstalten die Finanzinstitute einen Suchlauf über alle Kreditkartenkonten. Die damit verbundene Zweckänderung ist im Interesse der von Verfassungs wegen gebotenen Strafverfolgung gerechtfertigt, so dass jedenfalls das Ergebnis der Datenverarbeitung – 322 Karteninhaber als Verdächtige – eine zulässige Datenübermittlung an die Staatsanwaltschaft ist. Das hat *Kahler* in den Abschnitten 3.1, 3.2 und 4.1 gut und nachvollziehbar hergeleitet. Durch ihre Anfrage soll die Staatsanwaltschaft rechtlich eine Datenverarbeitung veranlasst haben (S. 148), so dass sie eine datenschutzrechtliche Rolle als Auftraggeber nach Maßgabe der DSGVO übernommen habe, die sie schließlich zur Beauskunftung der nichtverdächtigen Kontoinhaber verpflichte (S. 103 oben; S. 114), wozu *Kahler* auch den § 491 Abs. 1 heranzieht (S. 151), wonach eine datenschutzrechtliche Benachrichtigung über die Verarbeitung personenbezogener Daten nur zurückgestellt, nicht aber unterlassen werden darf. Im Weiteren folgert *Kahler*, dass § 161 einer Neufassung oder Ergänzung im Hinblick auf heimliche Eingriffe bedarf (S. 129), die eine ausdrückliche Eingriffsermächtigung schaffen und die Einzelheiten der nach europäischen Datenschutzrecht erforderlichen Mitteilungen ausführen sollen (Details: S. 131).

Unberücksichtigt lässt *Kahler*, dass die Staatsanwaltschaft keine Herrschaft über den Datenpool erlangte, aus dem die Verdächtigendaten selektiert wurden, und keinen Einfluss auf die Datenverarbeitung der Kreditkartenunternehmen nahm, so dass selbst nach den strengen Regeln

---

1 Vorwort, S. 7. Die Seiten aus der Studie werden im Folgenden im laufenden Text zitiert: (S. 7).

2 *BVerfG,* Beschl. v. 17.2.2009 – 2 BvR 1372, 1745/07.

3 Die Vorschriften aus der StPO werden im Folgenden ohne Gesetzeszusatz angegeben.

4 *BVerfG,* Beschl. v. 17.2.2009 – 2 BvR 1372, 1745/07, Rn. 2.

5 Einschränkend (S. 21), wonach es sich um eine Schätzung anhand von zwei Literaturquellen handelt. (S. 20, Fn. 12; S. 21, Fn. 17) verweisen auf *AG Halle* Beschl. o.D. – 395 Gs **43**/07; *BVerfG* Beschl. v. 17.2.2009 – 2 BvR 1372/07 – verweist auf *AG Halle* Beschl. v. 30.5.2007 – 395 Gs **49**/07; so auch der Verweis bei *LG Halle* Beschl. v. 5.7.2007 – 13 Qs 125/07 (jurion.de). Wenn das *AG Halle* nach § 98 Abs. 2 S. 2 entschieden hat, war das eine (erste) gerichtliche Entscheidung und nicht die eines Beschwerdegerichts (S. 33). Eine „weitere Beschwerde" (S. 22) zum LG (§ 310) ist in den angesprochenen Fällen nicht zulässig.

der DSGVO kein Fall der Auftragsdatenverarbeitung vorliegt, sondern ein Fall der Funktionsübertragung, bei dem der Auskunftspflichtige die vollständige Prozessherrschaft über alle Datenverarbeitungsvorgänge behält, von der Datenerhebung über ihre Verarbeitung bis hin zu ihrem Ergebnis (Output). Erst nach dem Abschluss der Datenverarbeitung erfolgte die Übermittlung des Ergebnisses, so dass die Staatsanwaltschaft nur Kenntnis von dem Output erlangte und nicht auch von den personenbezogenen Daten, die der Datenverarbeitung der Kreditkartenunternehmen im Übrigen unterlagen.

Verfassungsrecht: Ermittlungsgeneralklausel als Eingriffsnorm

Die gesetzlichen Hierarchiestufen, auf denen *Kahler* diskutiert, werden nicht immer ganz deutlich. Bei den Fragen nach der informationellen Selbstbestimmung[6] (die Einschlägigkeit des Telekommunikationsgeheimnisses nach Art. 10 GG [S. 116] und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[7] schließt *Kahler* richtigerweise aus) und dem Zitiergebot (Art. 19 Abs. 1 S. 2 GG) (S. 118 f.) befinden wir uns auf der verfassungsrechtlichen Ebene. Insoweit hat das *BVerfG* die Ermittlungsgeneralklausel des § 161 Abs. 1 als „die Ermächtigungsgrundlage für Ermittlungen jeder Art" anerkannt, „die nicht mit einem erheblichen Grundrechtseingriff verbunden sind und daher keiner speziellen Eingriffsermächtigung bedürfen".[8] Sie unterliegt als vorkonstitutionelles Recht nicht dem Zitiergebot des Art. 19 Abs. 1 S. 2 GG.[9] Das verfassungsrechtliche Erfordernis einer neuen Eingriffsermächtigung stellt sich deshalb nur dann, wenn die Auskunftserteilung nicht nur oberflächlich, sondern überhaupt messbar in die Persönlichkeitsrechte mittelbar Betroffener eingreifen würde. Dem entgegnet *Kahler* mit dem Volkszählungsurteil, wonach es keine belanglosen Daten gebe (S. 60; S. 123).[10] Das beantwortet aber nicht die Frage nach der Tiefe des Eingriffs in die Persönlichkeitsrechte in Bezug auf die informationelle Selbstbestimmung. Im Ergebnis stellt *Kahler* zwar fest, dass die Eingriffe in das Recht auf informationelle Selbstbestimmung „nicht überaus erheblich" seien (S. 124, 126 f., ausdrücklich: S. 128), setzt dem aber entgegen, dass sie sich „außerhalb der Zugriffssphäre des Staates" befanden (S. 128). Allein das ist ein vorgeschobenes Argument, weil es dem Grundrechtsschutz in erster Linie um die Abwehr staatlicher Eingriffe geht und erst das Datenschutzrecht im Übrigen auch auf die Gesellschaft reguliert.

Europarechtskonforme Auslegung der StPO

Die StPO sowie die BDSGe in alter und in neuer Fassung (seit dem 25.5.2018) sind miteinander konkurrierendes Bundesrecht. Soweit europarechtliche Verordnungen unmittelbar geltendes Recht sind (wie die DSGVO seit dem 25.5.2018[11]), sind sie als europäisches Sekundärrecht verbindlich und sogar dem Verfassungsrecht in den Grenzen des Art. 79 GG übergeordnet (Art. 288 Abs. 2 AEUV; Art. 23 Abs. 1 S. 2 GG).[12] Europarechtliche Richtlinien müssen hingegen vom nationalen Gesetzgeber erst umgesetzt werden; ihre Regeln sind unabhängig davon bei der richtlinienkonformen Auslegung des allgemeinen Rechts als Anwendungsregeln zu berücksichtigen (arg. aus Art. 4 Abs. 3 EUV):[13] „Es ist Sache des nationalen Gerichts, das zur Durchführung der Richtlinie erlassene Gesetz unter voller Ausschöpfung des Beurteilungsspielraums, den ihm das nationale Recht einräumt, in Übereinstimmung mit den Anforderungen des Gemeinschaftsrechts auszulegen und anzuwenden." Darüber hinaus ist die verfassungsrechtliche Überprüfung europarechtlicher Vorschriften auch dem *BVerfG* entzogen.[14]

Kahler schließt die unmittelbare Anwendung der DSGVO zu Recht nach ihrem Wortlaut auf das Ermittlungsrecht aus (Art. 2 Abs. 2 lit. d DSGVO) (S. 103) und konzentriert sich auf die Richtlinie 2016/680/EU vom 27.4.2016 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, die teilweise bereits in nationales Recht umgesetzt ist[15] und sich im Übrigen im Entwurfsstadium befindet.[16] Die Regelungen sind auch im Wege der richtlinienkonformen Auslegung anzuwenden. Insoweit spricht ihre Erwägung 11 auf die Finanzinstitute an, die „bestimmte personenbezogene Daten … verarbeiten, und … den zuständigen nationalen Behörden in bestimmten Fällen und in Einklang mit dem Recht der Mitgliedstaaten zur Verfügung" stellen, was die Richtlinie als keine Auftragsverarbeitung versteht. In der Erwägung heißt es weiter: „Eine Stelle …, die personenbezogene Daten im Rahmen des Anwendungsbereichs dieser Richtlinie für solche Behörden verarbeitet, sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments und durch die für Auftragsverarbeiter nach dieser Richtlinie geltenden Bestimmungen gebunden sein." Sie betrachtet somit die Finanzinstitute gerade nicht

---

6 Volkszählungsurteil: *BVerfG*, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83.

7 Onlinedurchsuchung: *BVerfG*, Urt. v. 27.2.2008 – 1 BvR 370, 595/07.

8 *BVerfG*, Beschl. v. 17.2.2009 – 2 BvR 1372, 1745/07, Rn. 26.

9 E-Mail-Beschlagnahme: *BVerfG*, Beschl. v. 16.6.2009 – 2 BvR 902/06, Rn. 77. Die Ermittlungsgeneralklausel ist bereits Bestandteil der Urfassung der StPO aus 1877 gewesen und nicht erst 2000 *eingeführt* worden; so aber (S. 17); S. 24, Fn. 40 trifft auch nicht zu, weil 2000 der § 161 StPO nur neu gefasst wurde. Genauer differenziert (S. 39), verschweigt aber, dass nur die Ausführungsregeln ergänzt wurden, nicht aber, dass die Ermittlungsgeneralklausel als solche unverändert blieb.

10 *BVerfG*, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, Rn. 158.

11 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

12 So auch *BVerfG*, Beschl. v. 19.7.2011 – 1 BvR 1916/09, Rn. 78.

13 *EuGH*, Urt. v. 10.4.1984 – Rechtssache 14/83, Antwort 3.

14 *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 105, 106 m.w.N.

15 Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG).

16 Überblick bei BT-Drs. v. 9.7.2018 – 19/3341, Anlage 2. *Kahlers* Anregungen im Hinblick auf § 161 StPO nehmen die Drucksachen hingegen nicht auf.

als Auftragsdatenverarbeiter, sondern will sie ihnen datenschutzrechtlich gleichstellen, was etwas anderes ist.

Auftragsverarbeitung ist schließlich die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen Dritten (§ 11 Abs. 1 BDSG a.F.), wobei der Grundgedanke herrscht, dass der Auftraggeber entweder von ihm rechtmäßig erhobene Daten zur Datenverarbeitung zur Verfügung stellt oder seine Datenerhebungsbefugnis (Kompetenz) auf den Dritten überträgt.[17] Nach Maßgabe der DSGVO und ihrer Vorgängerin muss ergänzt werden: … oder auf den Datenverarbeitungsprozess Einfluss nimmt.

Kahler betrachtet die grundsätzlich zulässige Auskunftsermächtigung der Staatsanwaltschaft als die rechtliche Veranlassung eines Datenverarbeitungsvorganges im Wege der Auftragsdatenverarbeitung, weil es sich aus der Sicht der auskunftgebenden Banken – wegen der Daten der Verdächtigen – um eine Datennutzung durch Übermittlung handele (S. 47) (§ 3 Abs. 4 ff. BDSG a.F.). Seine Ausführungen zur Rechtfertigung der Datenverarbeitung der betroffenen Banken bis hin zur Übermittlung der Verdächtigendaten sind spannend und gut nachvollziehbar. In dem Abschnitt 3.2.1 (S. 93 ff.) kommt er schließlich zur „Datenverarbeitung zur Strafverfolgung gem. DSGVO", die er als unvollständig ansieht, „weil erstens eine Datenverarbeitung bei Nichtverdächtigen nur bei Vorliegen einer Straftat von erheblichen Gewicht zulässig ist und zweitens deren Rechte besonders geschützt werden müssen durch Aufnahme des Wortlauts 'und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse unbeteiligter Dritter an dem Ausschluss der Verarbeitung überwiegt' " (S. 99). Die Beschränkung auf Straftaten von erheblichem Gewicht folgert *Kahler* daraus, dass die Datenverarbeitung der auskunftgebenden Banken einer Zweckänderung unterliegt (S. 103). Schon das erste Argument ist in Anbetracht der Rechtsprechung des *BVerfG* fragwürdig, weil es wegen der Auskunftserteilung (hier: nach § 113 TKG) nicht nach der Schwere der Kriminalität unterscheidet und selbst Ordnungswidrigkeiten umfasst sieht, wenn denn ein Anfangsverdacht besteht.[18] Auch Art. 6 lit. a) der Richtlinie 2016/680/EU spricht nur von „Straftat", ohne nach der Schwere zu differenzieren. Das von *Kahler* nicht unterlegte Zitat entstammt den §§ 26 Abs. 3, 33 Abs. 1 Nr. 2a und 36 BDSG n.F. und betrifft dort die Arbeitnehmerrechte, den zivilrechtlichen Schutz und den Ausschluss des Widerspruchsrechts. Knapp ist *Kahlers* Hinweis auf § 28 Abs. 1 Nr. 2, Nr. 3 BDSG a.F. (S. 139) (Datenverarbeitung für eigene Geschäftszwecke), ohne dass er Gründe für die Analogie nennt, die immerhin eine gesetzliche Lücke voraussetzen würde.[19]

Auftragsdatenverarbeitung und Funktionsübertragung

In der strafrechtlichen Diskussion im Zusammenhang mit den §§ 202a, 303a u.a. StGB steht die Frage nach der Dateninhaberschaft im Vordergrund, die bevorzugt an dem Skripturakt festgemacht wird, also dem Erheben und Speichern von Daten,[20] worauf der Auftragsverarbeiter zum Datenmitinhaber mit eingeschränkten Verarbeitungsrechten wird.[21] Davon gesondert ist die Verantwortung für die Datenverarbeitung zu betrachten, die § 3 Abs. 7 BDSG a.F. in verständlichen Worten zusammengefasst hat: „Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies *durch andere im Auftrag* vornehmen lässt". Nach einem jüngeren (an der Datenschutz-Richtlinie 95/46/EG ausgerichtetem) Urteil des *EuGH* ist der „Begriff des „für die Verarbeitung Verantwortlichen" in Art. 2 Buchst. d der Richtlinie weit definiert als natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten *entscheidet*".[22] Infolgedessen kann es auch mehrere Verarbeitungsverantwortliche mit unterschiedlichen datenschutzrechtlichen Pflichten geben.[23] Entscheidend ist jedoch, ob und inwieweit der Mitverantwortliche auf die Datenverarbeitung Einfluss nehmen kann.[24] Das deckt sich weitgehend mit der Auffassung des *BVerwG*, das in dem einschlägigen Vorlagebeschluss ausgeführt hat:[25] „Die Fähigkeit, über die Zwecke und Mittel der jeweiligen Datenverarbeitung *auch entscheiden* zu können, ist aber ein prägendes, unverzichtbares Element des Art. 2 Buchst. d) der Richtlinie 95/46/EG. Eine Stelle, die weder einen rechtlichen noch einen tatsächlichen Einfluss auf die Entscheidung hat, *wie personenbezogene Daten verarbeitet werden*, kann nicht als für die Verarbeitung Verantwortlicher angesehen werden."[26] Maßgebend ist somit, dass der Auftraggeber eine rechtliche oder tatsächliche Herrschaft auf die Datenverarbeitung des Auftragnehmers ausübt, worauf er erst vom Datenschutzrecht in die Pflicht genommen wird.

Diese Fragen bewegen schon länger die Diskussion über die *Funktionsübertragung*, bei der der Empfänger eines Outputs (Auskunft) keine Weisungsbefugnisse über die Datenerhebung und die Datenverarbeitung im Übrigen ausübt, so dass der Datenverarbeiter wegen der Datenverarbeitung weisungsfrei und der Empfänger ohne datenschutzrechtliche Verantwortung bleibt. Genau das hat der *EuGH* bestätigt, indem er die datenschutzrechtliche Verantwortung mit der rechtlichen oder tatsächlichen Herrschaft über die zu verarbeitenden Daten und dem damit verbundenen Datenverarbeitungsprozess verknüpft.

Durch die allenfalls hilfsweise geltende DSGVO ist die Auftragsdatenverarbeitung stärker in die Verantwortung

17 Zur Strafbarkeit der gesetzwidrigen Auftragsdatenverarbeitung: *BGH*, Urt. v. 10.10.2012 – 2 StR 591/11.
18 *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 177 am Ende.
19 *BVerfG*, Beschl. v. 6.12.2005 – 1 BvR 1905/02, Rn. 56.
20 *OLG Naumburg*, Urt. v. 27.8.2014 – 6 U 3/14, S. 6.
21 *OLG Nürnberg*, Beschl. v. 23.1.2013 – 1 Ws 445/12.
22 *EuGH*, Urt. v. 5.6.2018 – C-210/16, Rn. 27; Hervorhebung vom Verfasser.
23 *EuGH*, Urt. v. 5.6.2018 – C-210/16, Rn. 29 (Mitverantwortung des Betreibers einer Facebook-Seite).
24 *EuGH*, Urt. v. 5.6.2018 – C-210/16, Rn. 39.
25 *BVerwG*, Beschl. v. 25.2.2016 – 1 C 28.14, Rn. 27.
26 Hervorhebung vom Verfasser.

genommen worden, was nichts daran ändert, dass „die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen" außerhalb des Anwendungsbereiches des europäischen Datenschutzrechts bleibt.[27] Das ULD nennt als Beispiele für die Funktionsübertragung die Berufsgeheimnisträger, Inkassobüros, Postdienste und schließlich auch die „Bankinstitut(e) für den Geldtransfer".

Die Richtlinie 2016/680/EU vom 27.4.2016 unterwirft die Strafverfolgungs- und anderen auskunftsberechtigten Behörden keinen Pflichten im Hinblick auf die Datenverarbeitung, die der Auskunft vorausgeht, sondern nur wegen der eigenen Datenverarbeitung (Erwägung 49): „Werden personenbezogene Daten im Zusammenhang mit strafrechtlichen Ermittlungen und Gerichtsverfahren in Strafsachen verarbeitet, so sollten die Mitgliedstaaten vorsehen können, dass die Ausübung des Rechts auf Unterrichtung, Auskunft, Berichtigung oder Löschung personenbezogener Daten oder Einschränkung der Verarbeitung nach Maßgabe des einzelstaatlichen Strafverfahrensrechts erfolgt." Der von der behördlichen Datenverarbeitung Betroffene soll „das Recht haben …, zu wissen und zu erfahren, zu welchen Zwecken die Daten verarbeitet werden, wie lange sie verarbeitet werden und wer deren Empfänger, einschließlich solcher in Drittländern, sind" (Erwägung 43). Eine Erstreckung auf die Datenverarbeitung Dritter, die der eigenen Datenerfassung der Behörden vorausgeht, fehlt an dieser oder an anderen Stellen. Nach der Definition in Art. 4 Nr. 9 DSGVO und Art. 3 Nr. 10 der Richtlinie 2016/680/EU ist der *Empfänger* jeder, dem Auskunft erteilt wird. Soweit daraus Pflichten entstehen können, werden die Behörden, die nach europäischem oder dem Recht der Mitgliedsstaaten Auskunft verlangen können, nicht als Empfänger im datenschutzrechtlichem Sinne angesehen (Erwägung 22 der Richtlinie 2016/680/EU). Sie werden weder von der DSGVO noch von der Richtlinie 2016/680/EU wegen ihrer unmittelbaren Aufgabenwahrnehmung angesprochen und den nationalen Gesetzgebern die Gestaltung überlassen. Wegen der Auskunft erlangenden Behörden lässt die Richtlinie 2016/680/EU schließlich auch die Weitergabe von Informationen zu, wenn sie aufgrund einer gesetzlichen Ermächtigung erfolgt (Art. 9; hypothetischer Ersatzeingriff).

Kahler ist darin Recht zu geben, dass der Auftraggeber im Zusammenhang mit der Auftragsdatenverarbeitung stärkeren datenschutzrechtlichen Pflichten unterliegt. Er ist aber nur dann Auftraggeber im datenschutzrechtlichen Sinne, wenn er rechtlich oder tatsächlich auf den Prozess der Datenverarbeitung von der Eingabe über die Datenverarbeitung als solche bis hin zur Schöpfung des Datenverarbeitungsergebnisses Einfluss nimmt oder nehmen kann. Die Ermittlungsgeneralklausel des § 161 Abs. 1 ermächtigt die Staatsanwaltschaft nur, Auskünfte zu verlangen, die womöglich eine Datenverarbeitung voraussetzen, gestaltet aber nicht die Datenerhebung und die Datenverarbeitung selber. Auf das Datenverarbeitungsrecht nimmt die Ermittlungsgeneralklausel – und die Staatsanwaltschaft – ebenso wenig Einfluss wie darauf, wie und welche Daten erhoben werden und wie das Ergebnis beim Output zustande kommt. Ihre rechtliche und tatsächliche Tragweite beschränkt sich auf die Qualität des Ergebnisses der Datenverarbeitung und umfasst nicht auch den Prozess, wie es zustande kommt.

Der tragende Gedanke *Kahlers*, die Staatsanwaltschaft als Auftraggeber im Rahmen einer Auftragsdatenverarbeitung in die Pflicht zu nehmen, beruht somit auf einem verkürzten Verständnis von der Auftragsdatenverarbeitung, das weder vom Verfassungs- noch vom Datenschutzrecht getragen wird. Jedoch müssen noch weitere einfach- und verfassungsrechtliche Aspekte betrachtet werden.

Eingriffstiefe und Streubreite

Dem *BVerfG* sind zwei Aspekte besonders wichtig: Die Eingriffstiefe im Einzelfall und die Streubreite, also die Beeinträchtigung der Grundrechte Unbeteiligter durch eine Eingriffsmaßnahme.[28] Unter dem Aspekt der Streubreite sind besonders schwerwiegend die Vorratsdatenspeicherung im engeren Sinne, wobei die gesetzlich bestimmten Verkehrsdaten innerhalb eines begrenzten Zeitrahmens von den Zugangsprovidern zu speichern sind (§§ 100g StPO, 113 ff. TKG), die Rasterfahndung nach den §§ 98a, 98b,[29] bei der verschiedene Datenquellen auf Gemeinsamkeiten überprüft werden, und die Nachrichtenmittler,[30] die keine Beschuldigten sind, mit ihnen aber in enger kommunikativer Beziehung stehen (§§ 100a Abs. 3, 100b Abs. 3 S. 2, 100c Abs. 2 S. 2).[31] Die Streubreite beginnt dann bedeutsam zu werden, wenn der Eingriff gegen Unbeteiligte tiefer als oberflächlich wirkt. Allein in diesem Zusammenhang ist nach meinem Verständnis auch danach zu unterscheiden, ob der Datenverarbeitungsvorgang auf Echtdaten oder auf pseudonymisierte Daten beruht. Der technische Standard für die Verarbeitung von Datenbanken ist die relationale Datenverarbeitung, wobei aus Gründen der Effektivität und der Verarbeitungszeit nicht auf die gespeicherten Datensätze insgesamt, sondern auf Indexe zugegriffen wird, also auf Datentabellen mit pseudonymisierten Datensätzen. Dazu hat *Kahler* keine

---

27 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – ULD, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DSGVO, 10.1.2018, Anhang B.

28 Statt vieler: *BVerfG*, Beschl. v. 8.6.2016 – 1 BvR 229/16, Rn. 22; *BVerfG*, Urt. V. 20.4.2016 – 1 BvR 966/09; Rn. 101.

29 *Kahler* stellt auf die Zusammenführung der Datenquellen ab (S. 35); das Problem der Streubreite stellt sich hingegen nicht bei der Zusammenführung, sondern bei der Erhebung der Datenquellen, die zwangsläufig eine Vielzahl von Daten Unverdächtiger enthalten, die in den Herrschaftsbereich der Strafverfolgungsbehörden gelangen. Zur polizeirechtlich zulässigen Rasterfahndung: *BVerfG,* Beschl. v. 4.4.2006 – 1 BvR 518/02.

30 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 116.

31 Die Aufzählung ließe sich ergänzen um die Observation, dem Einsatz eines IMSI-Catchers, dem kleinen Lauschangriff und andere Maßnahmen, so auch um die Durchsuchung beim nur Verdächtigen, der nicht zum Beschuldigten wird.

Erhebungen angestellt; schon vom Grundsatz her kann damit in Frage stehen, ob es sich bei den Kontodaten der Unbeteiligten wirklich um (relevante) personenbezogene Daten handelt und wie tief sie wirklich betroffen sind. Wer vor etlichen Jahren ein gedrucktes Telefonbuch beim Rückenaufdruck „K" nutzte, um nach „*Kochheim*" zu suchen, kam nicht ernsthaft auf den Gedanken, auch die personenbezogenen Daten von „Appel" oder „Zeppelin" zu verarbeiten.

Das betrifft schließlich nicht nur die Streubreite, sondern auch die Eingriffstiefe: Die datentechnische Suche nach Zahlungsbeträgen und -empfängern sagt nichts über die Motive des Zahlers aus; er bleibt anonym, solange die Suchkriterien nicht genau auf ihn passen. Mit anderen Worten: Datenschutzrechtlich mag auf seine (pseudonymisierten) personenbezogenen Daten zugegriffen worden sein, ein messbarer Grundrechtseingriff ist damit jedoch nicht verbunden gewesen.

Den von *Kahler* bemühten Massendaten als Grundlage einer Datenverarbeitung bemisst jedenfalls das *BVerfG* keine außerordentliche Bedeutung zu, wie seine Rechtsprechung zu den Bestandsdaten, ihre Beauskunftung und zu dem damit im Einzelfall verbundenen Rückgriff auf Vorratsdaten belegt.[32] Vorratsdaten sind auch dann nach Art. 10 GG stärker geschützt als die Persönlichkeitsrechte, wenn der Vorgang der Telekommunikation bereits abgeschlossen ist,[33] so dass auch der Rückgriff auf dynamische IP-Adressen im Zusammenhang mit der Bestandsdatenauskunft nach Maßgabe des Art. 10 GG zu betrachten ist.[34] Es bedarf deshalb wegen der Verkehrsdaten einer gesetzlichen Ermächtigung für den Zugriff seitens des Auskunftspflichtigen – jetzt geschaffen im TKG – und für das Auskunftsrecht des Auskunftsverlangenden – jetzt geschaffen in § 100j,[35] ohne dass das *BVerfG* auf die Datenbasis und ihre Verarbeitung anspricht, sondern nur auf die Auskunft, die auf der Datenverarbeitung beruht:[36] „Dennoch ist der hierin liegende Eingriff nicht von sehr großem Gewicht. ... Denn auch wenn § 111 TKG eine große Streubreite hat, beschränkt sich der Zugriff inhaltlich doch auf eng begrenzte Daten, die aus sich heraus noch keinen Aufschluss über konkrete Aktivitäten Einzelner geben und deren Verwendung der Gesetzgeber zu näher bestimmten Zwecken geregelt hat."

Strafverfahrensrechtliche Mitteilungspflichten

§ 33 überträgt das Gebot des rechtlichen Gehörs (Art. 103 Abs. 1 GG) in das Strafverfahrensrecht und lässt Ausnahmen davon nur zu, „wenn die vorherige Anhörung den Zweck der Anordnung gefährden würde" (§ 33 Abs. 4 S. 1). In diesen Fällen wird die Entscheidung verkündet (zum Beispiel der Haftbefehl) oder durch Vollstreckung zugestellt (zum Beispiel der Durchsuchungsbeschluss). Wegen der verdeckten Ermittlungsmaßnahmen benennt § 101 die Maßnahmen und die Personen, die von der Maßnahme unterrichtet werden müssen. Das sind immer die Betroffenen (Beschuldigter, Nachrichtenmittler) und sonstige Personen immer nur dann, wenn sie *erheblich* mitbetroffen sind (§ 101 Abs. 4 S. 1 mit den verschiedenen Anwendungsfällen). § 101 Abs. 4 S. 4 untersagt im Ergebnis die Ermittlung der Identität unbekannter Mitbetroffener, wenn nicht besondere Gründe im Einzelfall dafürsprechen. Die Behandlung der Verkehrs-, Funkzellen-, Standort- und Vorratsdaten ist systematisch etwas unglücklich in § 101a geregelt mit dem Ergebnis, dass auch insoweit die direkt Betroffenen und nicht auch die Mitbetroffenen zu unterrichten sind (§ 101a Abs. 6), ohne dass es darauf ankommt, ob sie bereits „erheblich" mitbetroffen sind. Soweit die StPO darüber hinaus von Mitteilungen spricht, regelt sie damit besondere Einzelfälle.

Soweit *Kahler* auf § 491 verweist und daraus eine Öffnung (Doppeltürmodell) zum Datenschutzrecht mit dem Ergebnis ableitet, die Staatsanwaltschaft müsste alle Inhaber von Kreditkartenkonten unterrichten, bewegt er sich systematisch in dem Abschnitt über die Datenverarbeitung für die Zwecke des Strafverfahrens in den §§ 483 ff. StPO und diese betreffen nur die eigene Datenverarbeitung der Staatsanwaltschaft mit selbst erhobenen personenbezogenen Daten und den Datenaustausch im Hinblick auf dauerhaft oder vorübergehend, jedenfalls aber selbst gespeicherten Daten zwischen den beteiligten Strafverfolgungsbehörden (besonders der Polizei, eingeschränkt wegen des Strafvollzuges). § 491 Abs. 2 spricht ausdrücklich auf die „speichernde Stelle" an und schränkt die Auskunftspflichten auf die personenbezogenen Daten ein, die nicht nur verarbeitet, sondern tatsächlich gespeichert sind.

Ergebnisse und methodische Fragen

Besonders gelungen sind die informativen Kapitel 3.1 (S. 61 ff.) und 4 (S. 111 ff.).

Im Übrigen macht *Kahler* aus meiner Sicht zwei gedankliche Fehler: Er spricht von einem Massenzugriff auf die personenbezogenen Daten von Kreditkartenkunden, ohne den Prozess der damit verbundenen Datenverarbeitung tatsächlich zu hinterfragen und dabei zu prüfen, auf welche Daten mit welcher personenbezogenen Bedeutung wirklich zugegriffen wird. Allein der Hinweis darauf, dass es keine belanglosen Daten gebe, reicht nach den Anforderungen des *BVerfG* nicht, um die Tiefe des Grundrechtseingriffs auszuloten. Um es auf die Spitze zu treiben[37]: Hätte Kahler recht, dann müsste jede Suchanfrage bei einer Suchmaschine als eine Auftragsdatenverarbeitung angesehen werden, die den Anwender allein deshalb, weil er ein Suchwort mit Personenbezug verwendet, zum datenschutzrechtlichen Auftraggeber macht, weil er die tatsächlichen Voraussetzungen für eine Datenverarbeitung schafft. Das birgt bereits eine gewisse Absurdität, die in Bezug auf den Ausgangsfall nicht besser, sondern unter

32 *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05. Zwischen dem Schutz der Persönlichkeitsrechte und dem TK-Geheimnis differenziert *Kahler* nicht deutlich: S. 162.
33 Ebenda, Leitsatz 1.
34 *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 110.
35 Doppeltürmodell: *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 123.
36 *BVerfG*, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn. 138.
37 Mein streitbares Argument blendet die Frage nach der Zustimmung und der Umwidmung ausdrücklich aus.

verfassungsrechtlichen Gesichtspunkten noch schlimmer wird: Anstelle der nur 322 Verdächtigen soll die Staatsanwaltschaft die 22.000.000 Unverdächtigen deanonymisieren, die von der Beauskunftung am Rande – also unerheblich – auch betroffen seien. Dazu müsste sie Daten erheben, die sie nicht hat und die bei den Auskunftspflichtigen verblieben sind. Die Staatsanwaltschaft wurde nie Inhaberin und nie Herrschaftsberechtigte über die Daten der Unbeteiligten. Ihre Erhebung würde 22.000.000 verfassungsrechtlich nicht mehr unerhebliche und damit unzulässige Grundrechtseingriffe mit großer Streubreite voraussetzen. Genau das schließt § 101 in weiser Umsetzung der verfassungsrechtlichen Rahmenbedingungen aus.

Datenschutzrechtlich gesprochen würde es sich um eine Datenerhebung handeln, die nicht von den strafverfahrensrechtlichen Eingriffsnorm geboten ist, die der Datensparsamkeit widerspricht, eine Vertiefung des Eingriffs bedeutet und die einfach nur sinnlos ist, weil die zugrundeliegenden Datenverarbeitungsvorgänge vom Auskunftsberechtigten nicht nur nicht erhoben wurden, sondern die Daten im Detail auch nicht erhoben werden sollten.[38]

Der zweite Gedankenfehler beruht auf *Kahlers* undifferenzierten Vorstellung von der Auftragsdatenverwaltung. Ihre Abgrenzung zur Funktionsübertragung ist lange der Gegenstand der datenschutzrechtlichen Diskussion gewesen und durch die zitierte Entscheidung des *EuGH* aus 2018, die *Kahler* nicht bekannt gewesen ist, ist die Haftung des Auftraggebers auf die Prozesssteuerung erweitert worden. Die noch unklare Rechtslage ist bis zum Abschluss der Studie ein Grund mehr gewesen, sich mit dem damaligen Meinungsstreit auseinanderzusetzen. Dabei hätte dem *Autor* auch auffallen müssen, dass die einschlägige Richtlinie 2016/680/EU die auskunftsberechtigten Behörden gerade nicht in die Pflicht wegen der Mitteilungspflichten nimmt, sondern sie sogar von der Haftung als Empfänger ausnimmt.

Bestimmte Besonderheiten haben mir den Zugang zu der Studie erschwert:
Kahler unterlegt mehrfach klare gesetzliche Aussagen mit Sekundärquellen.[39] Soweit das Gesetz bestimmte Aussagen trifft, kann eine Fußnote allenfalls auf alternative Interpretationen oder sinnvolle Erweiterungen hinweisen.

Kahler spricht wiederholt von einem „hinreichenden Anfangsverdacht".[40] Dieser ist der Strafprozessordnung fremd und sie kennt drei andere Verdachtsgrade: Das ist zunächst der auf tatsächlichen Anhaltspunkten fußenden Anfangsverdacht nach § 152 Abs. 1, der durch Allgemein-, Fachwissen und kriminalistischen Erfahrungen untermauert werden darf.[41] Den Anfangsverdacht meint *Kahler*, wie auch die von ihm verwendeten Quellen vermitteln (S. 49, Fn. 199), und diskutiert anschließend die grundsätzliche Zulässigkeit der Erhebung der Verdächtigendaten (S. 50 bis 54).[42]

Der Vollständigkeit wegen: Im Hinblick auf die Untersuchungshaft (§ 112) und anderer vorläufiger Freiheitsbeschränkungen gilt der dringende Verdacht, der eine nachhaltige Verurteilungswahrscheinlich gegenüber dem Beschuldigten voraussetzt. Der hinreichende Verdacht betrifft schließlich die Anklageerhebung und die Zulassung der Anklage zur Hauptverhandlung im Zwischenverfahren und verlangt prognostisch nach einer überwiegenden Verurteilungswahrscheinlichkeit (§ 203). Ein „hinreichender Anfangsverdacht", wie er von *Kahler* wiederholt bemüht wird, ist der StPO fremd. Die Rechtsprechung hat einen vierten Verdachtsgrad im Zusammenhang mit tiefen Grundrechtseingriffen entwickelt, den ich einen angereicherten Anfangsverdacht nenne (Wohnungsdurchsuchung, TKÜ u.ä.).[43] Er betrifft die Untermauerung einer Eingriffsentscheidung durch gesicherte Tatsachen und hat nichts mit einer überwiegenden Verurteilungswahrscheinlichkeit im Sinne eines hinreichenden Verdachts zu tun.

Der Umgang des *Autors* mit dem Strafverfahrensrecht birgt auch andere Überraschungen, wenn er zum Beispiel von einer sofortigen Beschwerde nach einer gerichtlichen Entscheidung gemäß § 98 Abs. 2 S. 2 spricht und die Mitteilungspflichten in der StPO schildert, ohne auf den § 101 wegen der verdeckten Maßnahmen (seit 2007), den § 101a wegen der Verkehrs- und Vorratsdaten (seit 2015) und vielleicht noch den § 100j Abs. 4 wegen der dynamischen IP-Adressen einzugehen (seit 2013). Dabei wäre ihm die klare Struktur der StPO aufgefallen, Mitteilungspflichten nur wegen solcher Daten zu bestimmen, über die die Staatsanwaltschaft tatsächlich Herrschaft erlangt hat. Seine stattdessen vorgenommenen Erörterungen der §§ 483 ff. kranken daran, dass sie nur die aktiven Datenverarbeitsermächtigungen betreffen, nicht aber auch die Behandlung von Auskünften und Datensammlungen, die aufgrund von Eingriffshandlungen im Einzelnen erhoben wurden.

… noch ein Fazit

Das Datenschutzrecht hat spannende Auswirkungen auf andere Rechtsmaterien, deren wesentliches Regulativ die Verhältnismäßigkeit ist.[44] Die durch die Rechtsprechung entwickelten Grundrechte in Bezug auf die informationelle Selbstbestimmung[45] und zur Gewährleistung der In-

---

38 Das unterscheidet die Auskunft von der Datenerhebung für die Rasterfahndung, wobei die Strafverfolgung die Datenherrschaft über personenbezogene Daten Unverdächtiger erlangt.

39 S. 22, Fn. 20; S. 35, Fn. 105, 107; S. 36, Fn. 117, 118; S. 40, Fn. 137; S. 41, Fn. 143; S. 43, Fn. 164 (unter Verkennung, dass § 30a AO nur die Veranlagungsbehörden betrifft und nicht auch die Steuerfahndung); Unnötiges Sekundärzitat (S. 23, Fn. 28); das Original wurde bei jurion.de veröffentlicht.

40 S. 33; S. 48; S. 49 ff.

41 *BVerfG*, Beschl. v. 15.8.2014 – 2 BvR 969/14, Rn. 38, 41.

42 Am Ende vergleicht *Kahler* die „Aktion Mikado" mit den Datenzugriffen der NSA und verkennt auch an dieser Stelle, dass die Daten Unverdächtiger gerade nicht übermittelt und nicht in die Herrschaft staatlicher Behörden überführt werden.

43 Mit steigender Eingriffstiefe muss der bestehende Verdacht durch Anhaltspunkte angereichert sein. Vergleiche zum Nachrichtenmittler: *BVerfG*, Beschl. v. 30.04.2007 – 2 BvR 2151/06, Rn. 19.

44 *BVerfG*, Beschl. v. 16.6.1981 – 1 BvR 1094/80, Rn. 40, 44.

45 Volkszählungsurteil: *BVerfG*, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83.

tegrität und Vertraulichkeit informationstechnischer Systeme[46] sind neben den namentlich kodierten Freiheitsrechten (Post, Wohnung; beide mit Richtervorbehalt ausgestattet) zur maßgeblichen Messlatte für strafverfahrensrechtliche und andere staatliche Eingriffsmaßnahmen geworden. Datenschutz als Europa- und Bundesrecht ist jedoch kein absolutes Recht wie etwa der Kernbereich der persönlichen Lebensgestaltung[47] oder das Recht auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 S. 1 GG). Es muss sich anderen Freiheitsrechten beugen, damit auch sie ihre Wirkung entfalten können,[48] und steht auch – gemessen am Einzelfall und der Tiefe des individuellen Eingriffs – hinter dem Interesse der Allgemeinheit an einer effektiven Strafverfolgung zurück.[49] Das gerät gelegentlich in Vergessenheit.

46 Onlinedurchsuchung: *BVerfG*, Urt. v. 27.2.2008 – 1 BvR 370, 595/07.
47 *BVerfG*, Urt. v. 16.1.1957 – 1 BvR 253/56, Rn. 32 (Elfes).
48 „Schaukeltheorie“: *BVerfG*, Urt. v. 15.1.1958 – 1 BvR 400/51.
49 *BVerfG*, Beschl. v. 18.3.2009 – 2 BvR 2025/07, Rn. 16.