Freie Universität Berlin

Fachbereich Rechtswissenschaft

Freie Universität Berlin, Fachbereich Rechtswissenschaft,
Prof. Dr. Carsten Momsen, Van't-Hoff-Str. 8, 14195 Berlin

Prof. Dr. Carsten Momsen
Van't-Hoff-Str. 8
14195 Berlin

Telefon +49 (0)30 838-59408
+49 (0)30 838-58707
Fax +49 (0)30 838-458707
E-Mail carsten.momsen@fu-berlin.de
Internet www.jura.fu-berlin.de
Gebäude Boltzmannstr. 3, Raum 5502
14195 Berlin

Bearb.-Zeichen
Bearbeiter Frau Korth-Ndiaye

Berlin, 8. Mai 2017

Stellungnahme für den Rechtsausschuss des Deutschen Bundestags zu dem `Gesetzentwurf der Bundesregierung zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (BR-Drs. 163/17)´ für den 15.5.2017

Der Gesetzentwurf ist grundsätzlich zu begrüßen. Die nachfolgende Stellungnahme befasst sich aus strafrechtlicher Sicht insbesondere mit § 203 StGB-E und § 43e BRAO-E.

A. Grundidee

Der Entwurf zielt darauf, umfänglich praktizierte Formen des Datenoutsourcings, namentlich des „Non-Legal-Outsourcing" mit den Bedürfnissen eines strafrechtlich wirksamen Geheimnisschutzes in Einklang zu bringen.

Eine grundsätzliche – und richtige – Weichenstellung ist die Aufgabe einer Unterscheidung zwischen internen und externen Mitwirkenden. Eine entsprechende klare Unterscheidung war mit Blick auf die Behandlung elektronisch gespeicherter Daten schon lange nicht mehr durchzuführen. Der

„Grundgedanke des geschlossenen Geheimnisträgerkreises“[1] wird damit aufgegeben, was zu begrüßen ist. Allerdings bedarf es dann, schon aus Gründen der Gesetzesbestimmtheit, strafrechtlich tragfähiger Differenzierungen der Zuordnung zum Kreis der strafrechtlich verpflichteten Geheimnisträger. Zudem entstehen für bestimmte Personenkreise erstmals unmittelbar strafrechtliche (Schweige-) Verpflichtungen.[2]

Im neuen § 203 Abs. 3 StGB-E werden Voraussetzungen benannt, bei deren Vorliegen ein strafbares Offenbaren gerade nicht vorliegt, auch wenn das Geheimnis den Kreis der ursprünglich „zur Kenntnis Berufenen“ verlässt. Der Entwurf legt richtigerweise eine Differenzierung zugrunde zwischen den Gehilfen des Berufsträgers, an welche auch bislang eine Weitergabe prinzipiell straflos erfolgen konnte und anderen Dritten, welche nicht der Sphäre des Berufsträgers zuzuordnen sind. Exemplarisch für den letztgenannten Personenkreis sind bspw. Personen, die auf Seiten eines Cloud-Diensteanbieters mit den Informationen in Kontakt kommen, zu nennen. Der Kreis der Personen, an die straflos eine Informationsweitergabe erfolgen kann, ist danach im Grundsatz hinreichend bestimmt. Allerdings bestehen infolge der sehr unterschiedlichen Strukturen potentieller Dritter noch Klarstellungsbedürfnisse (s.u. D.). Auch bleibt der Gehilfenbegriff mit dem des § 53a StPO abzugleichen, insbesondere ist zu klären, ob auch im Rahmen des § 203 StGB-E an dem Erfordernis des „funktionalen Zusammenhangs festgehalten werden soll (s.u.D).[3]

Die Erweiterung des Personenkreises führt zwar zu einer Verringerung des strafrechtlichen Geheimnisschutzes, trägt aber den technischen Bedürfnissen im digitalen Zeitalter Rechnung, sowie dem bestehenden Problem, dass nach überwiegender Ansicht externe Personen für den Bereich des § 203 Absatz 1 StGB gerade nicht als berufsmäßige Gehilfen gelten. Dieses relativ restriktive Ergebnis wird zumindest teilweise kompensiert, indem Abs. 4 den Täterkreis auf diese Personen erweitert.

Diese Handhabung erscheint in dem Kontext der fortschreitenden Digitalisierung als sinnvoll. Die Idee, Dienstleistungen auszulagern, steht dabei im

---

* Für die Mitwirkung an der Stellungnahme gebührt Dank Prof. Dr. Lambert Grosskopf LL.M.Eur., Bremen, und Wiss. Mit. Dipl. iur. Laura Savic, Berlin,

[1] BT-Drs 18/11936, S. 16.

[2] Vgl. BT-Drs- 18/11936, S. 21 ff., so auch die Stellungnahme des Bundesrats, BT-Drs- 18/11936, S.45.

[3] Reschke BB 2017, S. 582; auf die Stellungnahme des DAV zum Entwurf nehme ich zur Vermeidung von Wiederholungen für § 203 StGB-E, § 43e BRAO-E sowie § 53a StPO Bezug (vgl. dort S. 10-12)

Vordergrund. Dabei geht es in dem Gesetzesentwurf um Formen des „Non Legal Outsourcing“, also nicht um die Übertragung von konkreten juristischen Aufgaben auf Dritte, sondern um Tätigkeiten wie Aktenvernichtung, Wartungsarbeiten an EDV-Anlagen, Schreib- oder Rechnungsarbeiten. Greift man sich in diesem Kontext nur die – trotz der damit verbundenen Risiken zumindest in weiten Bereichen als sozialadäquat eingeordnete – Möglichkeit der Nutzung dezentraler IT-Ressourcen (Cloud)[4] heraus, so ist diese im privaten und unternehmerischen Alltag nicht mehr wegzudenken. So sollen 2015 bereits über 50 % der in Deutschland tätigen Unternehmen Cloud-Computing genutzt haben.[5] Berufsgeheimnisträger, die letztlich auch unternehmerisch tätig werden, wollen sich dieser Möglichkeit nicht entziehen. Neben der reinen Kostenersparnis spielen auch Qualitäts- und Verfügbarkeitsgesichtspunkte eine Rolle.[6] Daher muss klar sein, ob der Auftraggeber und der Auftragnehmer sich nach § 203 StGB strafbar machen, wenn diese Daten in die Cloud übermitteln bzw. übermitteln lassen. Die Verlagerung vorhandener Informationen in die Cloud sowie die Nutzung dieser Informationen bedingt spezifische Sicherheitsstandards.[7] Als Beispiel kann auf den Anforderungskatalog Cloud-Computing (C5) „Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“[8] verwiesen werden.

Weiterhin gewinnt der Bereich der IT-Compliance oder Datenschutz-Compliance unmittelbare Bedeutung für die Anwendung des § 203 StGB.[9] Damit erlangen untergesetzliche Complianceregelungen („Soft-Law“) eine konkretisierende Wirkung für die Grenze der Strafbarkeit („Hard Law“). Zudem entsteht u.U. eine bereichsspezifische Akzessorietät zwischen Berufsrecht (§

---

[4] Conrad/Fechtner, CR 2013, 137 ff.; Hilgendorf in Hilgendorf (Hrsg.), Informationsstrafrecht und Rechtsinformatik, 2004, S. 83; Leupold, Münchener Anwalthandbuch IT-Recht, 3. Aufl. 2013, 4/18 ff.; Preuß, DuD 2016, 802 ff.

[5] Preuß, a.a.O. (Fn.4), Fn. 2 mit Verweis auf KPMG, Bitkom.

[6] Zu verschiedenen Erscheinungsformen näher Preuß, a.a.O. (Fn. 4), S. 802 f.

[7] https://www.heise.de/newsticker/meldung/BSI-setzt-Regeln-fuer-Cloud-Kunden-3704637.html?; vgl auch Kemmerich/Agrawal/Momsen, Secure migration to the cloud - in and out, in: Ryan Ko/Raymond Choo (Hrsg.), The Cloud Security Ecosystem Technical, Legal, Business and Management Issues, Oxford 2015, S. 205-230.

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog.pdf;jsessionid=7368279B6067AAF1D98DD8FB82A60892.2_cid341?__blob=publicationFile&v=7

[9] Vgl. Schmidl in Momsen/Grützner, Wirtschaftsstrafrecht, Handbuch für die Unternehmens- und Anwaltspraxis, 2013, S. 169 – 205.

43e BRAO-E), Datenschutzrecht (§ 11 BDSG)[10] und Strafrecht (§ 203 StGB-E) mit im Einzelnen noch konturierungsbedürftigen Überschneidungen (insoweit auch zum Strafverfahrensrecht, § 53a StPO)[11]. Diese Konturierung wird zwar zu einem nicht geringen Teil erst durch die Gesetzesanwendung in der Praxis erfolgen können, einige im Folgenden benannte Punkte könnten aber auch durch den Gesetzgeber konkretisiert werden um eine einheitliche Rechtsanwendung zu gewährleisten.

B. Einzelne Punkte im Bereich des § 203 StGB-E

Im Entwurf bedingt ein „unbefugtes" Offenbaren i.S.d. Abs. 3 Satz 1 d.E. insoweit per se, dass datenschutzrechtliche Belange betroffen sind. [12]

§ 203 StGB dient dem Schutz von Mandantengeheimnissen, die der Mandant dem Rechtsanwalt im Rahmen seiner Tätigkeit anvertraut hat. Die in § 203 StGB normierte Schweigepflicht des Rechtsanwalts gehört zum Kernbestand seines Berufsrechts (§ 43a BRAO, § 2 BORA). Möchte der Rechtsanwalt diese Geheimnisse weitergeben, bedarf es zunächst einer Einwilligung durch den Mandanten, auch wenn externe Dienstleister beauftragt werden und im Rahmen der Beauftragung vertrauliche Mandatsgeheimnisse weitergegeben werden müssen. Die Übertragung der Mandatstätigkeit auf den externen Auftraggeber ohne Einverständnis des Mandanten birgt derzeit noch das Strafbarkeitsrisiko des § 203 Abs. 2 StGB.

Nach § 203 Abs. 3 StGB-E soll kein „Offenbaren" vorliegen, wenn bei dem Rechtsanwalt „berufsmäßige Gehilfen oder bei diesem zur Vorbereitung auf den Beruf tätige Personen" Zugang zu den Geheimnissen bekommen. Externe Dienstleister zählen jedoch nicht dazu, weil sie nicht in den organisatorischen und weisungsgebundenen internen Bereich mit einbezogen sind. In Zukunft soll ein „Offenbaren" auch bei solchen Personen nicht mehr vorliegen, die an der beruflichen oder dienstlichen Tätigkeit des Rechtsanwaltes mitwirken (Absatz 3 Satz 2). Dadurch werden externe Dienstleister (Auftragnehmer) als Gehilfen qualifiziert und somit in den Kreis der Verpflichteten aufgenommen.

---

[10] Ausf. zu datenschutzrechtlichen Aspekten Cornelius, StV 2016, S. 381 ff.
[11] Dazu Reschke, a.a.O. (Fn.3), 582 ff.
[12] Näher i.S. Abs. 1, Cornelius, a.a.O. (Fn.9), S. 385.

Sie müssen in irgendeiner Art und Weise in die berufliche Tätigkeit eingebunden sein und dazu Beiträge leisten.[13] Erforderlich ist nicht mehr eine Eingliederung in die Sphäre des Berufsgeheimnisträgers. Eine Weitergabe mandatsbezogener Informationen wäre damit zwar tatbestandsmäßig, aber erlaubt. Davon umfasst wären Anbieter von Cloud-Plattformen, die eine verschlüsselte Speicherung zulassen. Dabei muss zwischen Transportverschlüsselung und der verschlüsselten Speicherung unterschieden werden, siehe dazu den BSI Anforderungskatalog Cloud-Computing (C5).[14] Aus dem Entwurf geht nicht hervor, ob alle Cloud-Lösungen darunter zu fassen sind, weil keine *Differenzierung möglicher Cloud-Anwendungen* vorgenommen wird (was ist mit Software as a Service?). Darüber hinaus gibt es keine Hinweise darauf wie Cloud-Lösungen auszugestalten sind[15], damit sie darunter zu fassen sind. Rechtlich muss davon ausgegangen werden, dass es sich bei den Vorgaben des BSI um den „Stand der Technik" handelt, der etwa nach § 13 Abs. 7 TMG bereits heute von jedem Diensteanbieter beachtet werden muss.[16] Stand der Technik ist die Verschlüsselung vor dem Ablegen in der Cloud beim Rechtsanwalt und zudem eine Transportverschlüsselung, denn dann kann der Cloud-Anbieter die Daten nicht zur Kenntnis nehmen.[17] Ein entscheidendes Abgrenzungskriterium wäre sicherlich darin zu sehen, ob die Berufsträger selbst oder deren Gehilfen unabhängig vom Cloud-Anbieter auf die gespeicherten Daten zugreifen können, was der Regelfall sein dürfte. Weiterhin gilt zu differenzieren, ob und in welcher Form der Cloud-Anbieter zugangsberechtigt ist, sowie, ob eine differenzierte Zugangsberechtigung in der Sphäre des Berufsträgers gegeben ist.[18]

---

[13] S.u. D.

[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/Anforderungskatalog.pdf;jsessionid=7368279B6067AAF1D98DD8FB82A60892.2_cid341?__blob=publicationFile&v=7

[15] Dazu näher Cornelius, a.a.O. (Fn.9), S. 380.

[16] Vgl. wiederum BSI –C5, a.a.O. (Fn. 13).

[17] Die etwa ehemals von DAVIT empfohlene Lösung „doculife", hinter der ein Schweizer Anbieter steht und die von der Telekom vermarktet wurde, übermittelte das „Master-Secret", also den „privaten Schlüssel" (sic!) bei jedem Aufruf des Dienstes an den Dienstleister zur Entschlüsselung der beim Dienstleister liegenden Dokumente und Daten. Zum „Security-Konzept doculife": https://www.t-systems.com/blob/651436/b57154598372f8dbfb3a3adde0d32c3c/dl-doculife-dokumentenmanagement-data.pdf

[18] Vgl. Preuß, a.a.O. (Fn. 4), S. 803.

Weiterhin macht sich der Berufsgeheimnisträger strafbar, wenn eine sonstige mitwirkende Person ein Geheimnis offenbart, dieser aber nicht dafür Sorge getragen hat, dass die Person zur Geheimhaltung verpflichtet ist (Abs. 4 Satz 2). Trotz des Fehlverhaltens einer dritten Person, die die eigentliche Tathandlung (Offenbaren eines Geheimnisses) begangen hat, wird der Berufsgeheimnisträger dann bestraft, wenn er den Dritten nicht zur Geheimhaltung verpflichtet hat.

Dabei ergibt sich erst aus § 203 StGB-E in Verbindung mit spezifischem Berufsrecht, etwa § 43e BRAO-E, dass eine Belehrung nicht ausreicht, sondern regelmäßig auch eine Überwachung erforderlich ist. Nur dann stehen die neuen Regelungen im Einklang mit Art. 35 DSGVO und den allgemeinen Anforderungsprofilen im Bereich der IT-Compliance.[19]

Die Befugnis, sich der Inanspruchnahme von Dienstleistern zu bedienen, tritt nur dann ein, wenn gewährleistet ist, dass die Verschwiegenheitspflicht bei diesen Dienstleistern vertraglich sichergestellt ist. Der Gesetzgeber normiert damit strafbewehrte Sorgfaltspflichten für die Berufsgeheimnisträger, die bei der Einbeziehung dritter Dienstleister zu beachten sind. Regelungstechnisch deutet Abs. 4 Satz 2 auf ein sog. „echtes *Unterlassungsdelikt*“[20] hin. Nr. 1 und 2 beschreiben eine Pflichtenkaskade, insoweit eine Unterlassensstrafbarkeit bspw. des Rechtsanwalts auch dann besteht, wenn er seine Hilfspersonen nicht über die abgeleitete Pflichtenstellung i.S. Nr. 2 belehrt. Im Zusammenspiel mit § 43e BRAO-E (s.u. c)) besteht m.E. weiterer Konkretisierungsbedarf im Hinblick auf „sonstige mitwirkende Personen“. Etwa im Hinblick auf den Mandanten.[21]

Fraglich ist dabei, ob es sich um eine *einmalige* Pflicht handelt oder der Berufsgeheimnisträger den Dritten *kontinuierlich* über die Geheimhaltungspflicht informieren, also ob er ständig dazu angehalten ist die Geheimhaltungspflicht des Dritten zu überwachen. Aus dem Wortlaut des Entwurfes „nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person […] „zur Geheimhaltung verpflichtet wurde“ lässt sich nur eine einmalige Pflicht entnehmen. Sollte der Gesetzgeber hingegen eine kontinuierliche Pflicht fordern, so müsste der Wortlaut dahingehend geändert werden, dass sich der Rechtsanwalt dann strafbar macht, wenn er nicht dafür Sorge „trägt“, dass […], zur Geheimhaltung verpflichtet „ist“. Eine Belehrung der Geheimhaltungsverpflichtung in regelmäßigen Abständen könnte danach angebracht sein. Wann die Verschwiegenheitsverpflichtung vorzunehmen ist, regelt §

---

[19] Vgl. unten c).
[20] Vgl. BT-Ds- 18/11936, S.28.
[21] S.u. am Ende des Abschnitts.

203 StGB-E nicht. Dies ist nicht problematisch, da für die Strafbarkeit noch das „Offenbaren“ durch die mitwirkende Person als Erfolg von Nöten ist. Daher ist eine sofortige Verpflichtung zur Verschwiegenheit mit Eintritt in das Vertragsverhältnis vorzunehmen. Wie konkret die Sorgfaltspflicht ausgestaltet ist, kann § 203 StGB-E nicht entnommen werden. Soweit spezifisches Berufsrecht gilt (vgl. § 43e BRAO-E, unten c)) sind die Pflichten teilweise weitergehend konkretisiert. Soweit keine solchen Regelungen existieren, sollte ggf. es nicht allein auf eine Einzelfallwertung, welche durch die Rechtsprechung mittelfristig erfolgen kann, hinauslaufen, da Rechtssicherheit möglichst unmittelbar geschaffen werden sollte.[22] Eine weitergehende gesetzliche Ausformung der Pflichtenstruktur erschiene daher vorzugswürdig. Mögliche *Konkretisierungen* der Pflicht könnten hinsichtlich der Adressaten und des jeweiligen Gefahrenpotenzials vorgenommen werden (s.u. § 43e BRAO-E).[23] Auch insoweit erlangt eine Differenzierung der „mitwirkenden Personen“ Bedeutung. Um keine hypertrophe gesetzliche Regelung zu schaffen, bietet sich eine *funktionsbezogene Betrachtungsweise* an, die jedenfalls im Gesetz angelegt werden könnte.[24] Funktionsbezug wäre jedenfalls gegeben, wenn der „sonstige Mitwirkende“ bei Ausübung der ihm übertragenen Aufgaben „bestimmungsgemäß“ oder „regelmäßig“ mit Geheimnissen in Berührung kommt.

Weiteren Aufschluss über den Inhalt der Pflicht kann den berufsrechtlichen Befugnisnormen der BRAO, der BNotO, der PAO, dem StBerG und der WPO entnommen werden. Für diese Berufsträger kann der Inhalt der Sorgfaltspflicht durch die benannten Spezialgesetze als hinreichend bestimmt angesehen werden, für alle weiteren in § 203 StGB(-E) erwähnten Berufsgruppen, die der Schweigepflicht unterliegen, wird der Inhalt durch das jeweilige Berufsrecht näher zu klassifizieren sein, insbesondere ihre Voraussetzungen und Grenzen.

Begrüßenswert erscheint, dass der Berufsgeheimnisträger die Pflicht nicht nur erfüllt, wenn er die erforderliche Verpflichtung selbst vornimmt, sondern dies auch durch einen Dritten geschehen kann, da sich die strafbewehrte Verpflichtung zur Geheimhaltung insbesondere in mehrstufigen Verhältnissen bis zur letztlich tätig werdenden Person fortsetzt, § 203 Abs. 4 Nr. 2 StGB-E. Somit kann ein weitgehend lückenloser Schutz des fremden Geheimnisses erreicht werden.

---

[22] Reschke, a.a.O. (Fn. 3), S. 580 f.
[23] Auf entsprechende Defizite weist hin: Reschke, a.a.O. (Fn. 3), S. 581.
[24] Dazu ausf. Cornelius, a.a.O. (Fn.9), S. 384 ff.

Im Zuge der Weitergabe von Informationen stellt sich die Frage, ob § 203 StGB-E auch die Weitergabe an den eigenen Mandaten erfasst, also ob der Mandant als sonstige Person i.S.v. § 203 Abs. 3 Satz 2 StGB-E angesehen werden kann. Dagegen spricht, dass die von der Norm erfasste sonstige Person, an der beruflichen Tätigkeit oder dienstlichen Tätigkeit des Rechtsanwalts in irgendeiner Weise mitwirken muss. Eine solche Mitwirkung an der beruflichen Tätigkeit soll nur dann gegeben sein, wenn die mitwirkende Person unmittelbar mit der beruflichen Tätigkeit der schweigepflichtigen Person, ihrer Vorbereitung, Durchführung, Auswertung und Verwaltung befasst ist. Der Mandant ist nicht in solch einer Weise mit der Tätigkeit des Rechtsanwalts befasst. Werden beispielsweise Strafakten an den Mandanten weitergegeben, die persönliche Daten von Zeugen beinhalten, so besteht weiterhin ein Strafbarkeitsrisiko des Berufsgeheimnisträgers (hier: Strafverteidiger) nach § 203 StGB, da ihm diese Geheimnisse seitens der Justiz anvertraut worden sind. Diesem Problem kann allerdings mit der Anonymisierung der persönlichen Daten Dritten praktikabel und zumutbar entgegengewirkt werden (s.u.E).

Praktisch liegt das Problem natürlich darin, dass der Betroffene „Ross + Reiter“ kennen muss, um den Strafverteidiger bei der Vorbereitung der Verteidigung durch Darstellung des Sachverhaltes aus seiner Sicht zu unterstützen. Denn sofern der Mandant tatsächlich etwas mit der ihm vorgeworfenen Tat zu tun hat, kann primär er Unzulänglichkeiten in Darstellung des Sachverhalts in der Ermittlungsakte erkennen, etwa wenn ein Zeuge bei dem Treffen, auf das sich seine Aussage (auch) bezieht, gar nicht zugegen war. Dann aber ist der Betroffene bzw. der Mandant faktisch an der „Vorbereitung, Durchführung, Auswertung und Verwaltung“ der Strafverteidigung beteiligt und wäre dann wohl „mitwirkende Person“ i.S.v. § 203 Abs. 3 Satz 2 StGB-E. Insoweit wäre die Betrachtungsperspektive des § 53a StPO durch die oben dargelegte funktionsbezogene Differenzierung zu ersetzen.

C. § 43e BRAO-E

Für Rechtsanwälte soll die bislang nur satzungsrechtlich bestehende Verpflichtung, Personal und mitwirkende Personen zur Verschwiegenheit zu verpflichten, nunmehr ins Gesetz übernommen werden, § 43 Buchst. e Abs. 2 BRAO-E. Sofern der Berufsgeheimnisträger dritte Personen an seiner Berufsausübung mitwirken lässt, ist er im Interesse des Geheimnisschutzes dazu verpflichtet, diese Dritten als Dienstleister im Hinblick auf ihre Vertrauenswürdigkeit sorgfältig auszuwählen, zu überwachen und sie zur Geheimhaltung zu verpflichten.

Daraus ergibt sich zugleich, dass über die o.g. und vom Entwurf zu § 203 StGB in Bezug genommene Belehrung hinaus, jedenfalls in den Bereichen

spezifischen Berufsrechts mehr zu verlangen ist: Belehrung + Überwachung.

Beide Normen müssten m.E. insoweit aufeinander abgestimmt werden.

Eine solche Formulierung ist als *Compliance* Vorschrift zu werten, bzw. als gesetzlicher Auftrag, entsprechende Compliance-Strukturen zu schaffen. Derartige Compliance-Strukturen bzw. prognostischen Prüfungen verlangt in der Sache bereits die Datenschutz Grundverordnung (siehe Datenschutz-Folgenabschätzung; Art. 35 DSGVO).[25]

---

[25] **Artikel 35 DSGVO - Datenschutz-Folgenabschätzung**

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.
(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

1. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
2. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
3. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.
(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.
(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.
(7) Die Folgenabschätzung enthält zumindest Folgendes:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der

Da hier bislang nur bereichsspezifische Anforderungen durch den Gesetzgeber ausformuliert bzw. angedeutet wurden (bspw. §§ 130, 30 OWiG; 93 AktG, „Business Judgement Rule"), wäre eine Konkretisierung zumindest hilfreich und wünschenswert im Sinne einer einheitlichen Anwendung des Strafrechts.

Dabei ist die in § 43e BRAO-E genannte Prüfungs- und Sorgfaltspflicht gegenüber „Dienstleister" anzuwenden, wohingegen § 203 StGB-E diese auf „sonstige mitwirkende Personen" als tatsächlich tätige natürliche Personen bezieht.

Der weitere Inhalt von § 43 Buchst. e Abs. 2 BRAO-E erscheint rein deklaratorisch. Eigentlich versteht sich von selbst, dass das Vertragsverhältnis zu beenden ist, wenn die gesetzlichen Vorgaben nicht eingehalten werden können.

Denkbar wäre es, analog zu entsprechenden Verfahrensweisen im Compliance-Sektor, auf eine Zertifizierung des Diensteanbieters abzustellen, welche u.a. eine regelmäßige Schulung der Mitarbeiter nachweisen.[26] Allerdings müssten entsprechende verbindliche Standards geschaffen werden

---

Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.
(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.
(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.
(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

[26] Entsprechende Angebote, wie etwa „Trusted Cloud – Datenschutzprofil für Cloud-Dienste" (http://www.tcdp.de/index.php) bestehen. Jedoch müssten die Zertifizierungen allgemeine Verbindlichkeit beanspruchen können, um strafrechtliche Wirkung zu entfalten.

und im Einklang mit datenschutzrechtlichen Anforderungen stehen.[27] Denkbar wäre auch eine einzelvertragliche Ausgestaltung i.S. § 43e Abs. 3 Nr. 3 BRAO-E. Problematisch daran ist, dass diese die vertraglichen oder nichtvertraglichen Auftragsverhältnisse mit Arbeitnehmern oder Dritten auf Seiten des Dienstleisters nicht umfänglich erfassen kann.[28] Mit Blick auf eine strafrechtlich einheitliche Handhabung erscheint jedenfalls eine weitergehende Konkretisierung unabhängig vom Einzelfall erstrebenswert.[29]

Nicht unproblematisch ist auch die aktuelle Regelung des § 43e Abs. 4 BRAO d.E.[30] Hier wird sich der Rechtsanwalt i.d.R. nur auf die Angaben des Dienstleisters verlassen können, dass (1) die Dienstleistung nicht im *Ausland* erbracht wird, d.h. das Speichermedium der Cloud nicht im Ausland platziert ist oder (2) ein vergleichbarer Geheimnisschutz gewährleistet ist. Eine eigene Überprüfung wird dem Rechtsanwalt häufig nicht möglich sein. Ob damit bspw. ein Unterlassen (§ 13 StGB) ausgeschlossen werden kann, erscheint klärungsbedürftig. Ggf. müsste von staatlicher Seite (bspw. BSI) eine entsprechende Liste als sicher geltender Staaten veröffentlicht werden.[31] Für den Datenverkehr in nicht EU-Staaten sind entsprechende Listen vorhanden, auf denen sich – bspw. in Form eines Verweises – aufbauen ließe.[32]

Zutreffend ist der Hinweis in der Stellungnahme des Bundesrats, dass dieser sehr weitreichende Geheimnisschutz nicht nur dort gewährleistet werden kann, wo ein entsprechendes Berufsausübungsrecht besteht.[33]

Nach Abs. 5 darf der Rechtsanwalt bei der Inanspruchnahme von Dienstleistungen, die unmittelbar einem einzelnen Mandanten dienen, dem Dienstleister den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der Mandant darin eingewilligt hat. Gerade hier zeigt sich erneut das Problem

---

[27] Vgl. Preuß, a.a.0. (Fn.4), S. 804.
[28] Zu § 53a StPO s.u. D.
[29] Zu Großprojekten unter Einbindung externer Dritter zweifelnd Reschke, a.a.O. (Fn.3), S. 580.
[30] BT-Drs 18/11936, S. 8.
[31] Ob die Vorschläge der Begründung ausreichend sind, erscheint fraglich, BT-Drs- 18/11936, S. 34 f.
[32] European Commission, Justice, Data protection, International transfer: http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm und insbesondere: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[33] BT-Drs- 18/11936, S. 43.

der Drittgeheimnisse. Der Mandant kann nur in die Weitergabe seiner eigenen Geheimnisse einwilligen, nicht jedoch in die von beispielsweise Familienmitgliedern oder sonstigen Zeugen, die in der Akte auftauchen. Es muss also weiterhin der Schutz personenbezogener Daten Dritter gewährleistet werden. Des Weiteren wird bei den Dienstleistern nach Tätigkeiten unterschieden. Nur solche Tätigkeiten, die konkret einem einzelnen Mandanten dienen (Detektiv, Übersetzer) sollen nur bei Einwilligung weitergegeben werden dürfen.

Zu Absatz 6 s.u. E II

D. Strafprozessrecht

§ 53a StPO gewährleistet für das Verhältnis zwischen Mandant und Rechtsanwalt ein gewisses Maß an Schutzstandards. Im Bereich des thematisierten Datenoutsourcings wird dies in den Fällen relevant, in denen sowohl strafrechtlich gegen den Mandanten ermittelt wird, als auch die vom Mandanten beauftragte Kanzlei, die für das Zivilverfahren mandatiert wurde, Rechtsdienstleistungen auslagert. Es wäre fatal, wenn die mandatsbezogenen Privilegien beim Datenoutsourcing nicht greifen würden. Diese Situation wird unter anderem durch das Zeugnisverweigerungsrecht nach §§ 53, 53a StPO reguliert. Der Wortlaut des § 53 StPO bezieht sich auf Strafverteidiger, Rechtsanwälte und Steuerberater. § 53a StPO erweitert diesen umfassenden Schutz für Gehilfen, die an der berufsmäßigen Tätigkeit des geschützten Personenkreises teilnehmen („Berufshelfer“). Insoweit stellt sich die Frage, ob der Gehilfenbegriff des § 203 StGB-E und der des § 53a StPO gleichzusetzen sind. Um in Genuss des durch § 53a StPO intendierten Schutzes des Vertrauensverhältnisses zu gelangen, fordert die Rechtsprechung, dass zwischen der Tätigkeit des Berufsträgers (Auftraggeber) und der Hilfsperson (Auftragnehmer) ein *innerer funktionaler Zusammenhang* bestehen muss.[34] Dieser umfasst dann ebenfalls die vom § 203 StGB-E umfassten Gehilfen, jedoch nicht unbedingt Dritte (externe Diensteanbieter), die selbständige Einzelaufträge ausführen, wie Cloud-Anbieter. Denn diese Personengruppe unterfällt nicht dem bisherigen Wortlautverständnis des § 53a StPO. Im Zusammenhang des Datenoutsourcings im Hinblick auf § 203 StGB-E muss daher auch die Reichweite des Gehilfenbegriffs aus

[34] BGH 7.4.2005 – 1 StR 326/04, BGHSt 50, 64 = NJW 2005, 2406; MüKo-StPO/Percic, § 53 a Rn. 2 m.w. N.

§ 53a StPO neu diskutiert werden, um einen umfassenden Schutz zu gewährleisten. Sollte ein funktionsbezogener Interpretationsansatz bei Gehilfen maßgeblich sein, könnte dem Abhilfe geschaffen werden. Danach ist Gehilfe jede Person, die vom Hauptberufsträger für die in § 53 Abs. 1 Nr. 1 bis 4 StPO bezeichneten Tätigkeiten herangezogen wird und umfasst jede Wahrnehmung, die dem Berufshelfer in dieser Eigenschaft anvertraut oder bekannt wird.[35] Danach wäre der selbständig auftretende Cloud-Anbieter Gehilfe im Sinne des § 53a StPO, sowie eine „sonstige mitwirkende Person" nach § 203 StGB-E. Angesichts der bisherigen Handhabung des § 53a StPO folgt dieses erweiterte funktionsbezogene Verständnis jedoch nicht aus der Änderung des § 203 StGB. Zudem müsste klargestellt werden, dass (bzw. unter welchen Voraussetzungen) insoweit auch Mandanten funktionsbezogen Kenntnis erlangen können.

Aus Sicht der Mandanten, der Berufsgeheimnisträger und Dritter involvierter Personen bedarf es daher insgesamt einer einheitlichen und in sich konsistenten Regelung der §§ 53, 53a StPO und § 203 StGB.

E. Alternativen

I. Anonymisierung und Pseudonymisierung

Um das hohe Strafbarkeitsrisiko zu senken, das im Prinzip allein dadurch entsteht, dass dritte, außerhalb der eigenen Sphäre stehende Personen zu Hilfstätigkeiten der Berufsgeheimnisträger herangezogen werden, könnte auch daran gedacht werden, bei *Anonymisierung* personenbezogener Daten die Strafbarkeit zu begrenzen.[36] Sodass es für niemanden oder nur mit einem unverhältnismäßig großen Aufwand möglich ist, die Daten einer Person zuzuordnen. Eventuell könnte dazu auch eine bloße *Pseudonymisierung* (Ersetzung von Identifikationsmerkmalen durch Kennzeichen, wobei es über eine Zuordnungsregel möglich ist, den Personenbezug für eine bestimmbare Person herzustellen) ausreichen.[37] Für letztere müsste der Zugangsschlüssel beim Berufsgeheimnisträger verbleiben, um den Schutz zu

---

[35] Näher Tsambikakis, Strafprozessuale Zeugnisverweigerungsrechte aus beruflichen Gründen, 20111, S. 117.
[36] Vgl. Preuß, a.a.O. (Fn.4), S. 805.
[37] Ausf. Cornelius, a.a.O. (Fn.9), S. 383 ff.

gewährleisten. Geht es um Privatgeheimnisse kann diese alternative Lösung in Betracht gezogen werden, sie hilft jedoch nicht weiter, wenn es um Unternehmensgeheimnisse geht. Des Weiteren ist die Praktikabilität mandatsbezogener Informationen in anonymisierter oder pseudonymisierter Form nicht alltagstauglich und mit höherem Aufwand verbunden. Eine gewisse Bedeutung könnte sie daher wohl v.a. im mit erfassten Bereich der Ausbildung erhalten und im Falle der Weitergabe der Strafakte an den eigenen Mandanten, soweit es um Geheimnisse Dritter geht (dazu oben S. 6). Beachtet werden muss auch, dass es durchaus unvermeidbar sein bzw. nicht ausgeschlossen werden kann, dass externe Dienstleister personenbezogene Daten einsehen (s.o. § 43e BRAO).

II. Einwilligungslösung

Ein Ansatz der Vermeidung einer Strafbarkeit nach § 203 StGB wird in der Einholung einer Einwilligung der Betroffenen Personen gesehen. Dann wäre ein Offenbaren jedenfalls nicht mehr unbefugt. Voraussetzung ist aber, dass die Einwilligung ausdrücklich erklärt wurde und der Betroffene zuvor über die Datenübermittlung ausreichend *informiert* wurde. Problematisch ist dabei, dass eine Einwilligung nur für die *Zukunft* gilt, kann also eine einmal eingetretene Strafbarkeit nicht beseitigen. Insoweit würde auch eine nachträgliche Genehmigung das Problem des Handlungsunrechts nicht lösen.[38]

Würde sie auch für Daten, die in der Vergangenheit erhoben und gespeichert wurden, eingeholt werden können, wäre an eine Lösung im Sinne der „tätigen Reue“ zu denken. Ob hierfür eine Notwendigkeit besteht, ist indes zu bezweifeln.

Des Weiteren kann eine Einwilligung nur insoweit die Strafbarkeit ausschließen, als das die betroffenen Personen über das jeweilige Geheimnis verfügungsberechtigt sind. Dies kann bei *Drittgeheimnissen* fraglich sein.[39]

Das Problem der personenbezogenen Daten Dritter, die sich bspw. in einer elektronischen Akte oder einem Sitzungsprotokoll befinden, ist aus strafprozessualer Sicht bekannt. Üblicherweise geht man davon aus, dass diese Rechte durch das Recht auf Verteidigung (§§ 136 Abs. 1, 137 StPO, Art 6 Abs. 3 EMRK) überlagert werden, soweit dies für eine effektive Verteidigung

---

[38] Vgl. Preuß, a.a.O. (Fn.4), S. 807.
[39] Diese Gesetzesbegründung geht davon aus, dass grds. der Mandant „Herr des Geheimnisses“ sei; vgl. BT-Ds- 18/11936, S. 35 zu § 43e Abs. 6 BRAO-E.

notwendig ist. Wenn es aber bereits insoweit einer Abwägung bedarf, welche Daten einem Mandanten zugänglich gemacht werden können, so bedeutet dies, dass eine Einwilligung des Mandanten insoweit unerheblich wäre. Außerhalb des strafprozessualen Bereichs dürfte sich das Problem noch verschärft stellen, da es insoweit kein „Recht auf effektive Verteidigung" gibt.

Zudem müssten die Betroffenen im Vorhinein genau darüber aufgeklärt werden (umfassend), in welchem Umfang und an wen eine eventuelle Datenauslagerung oder Weitergabe erfolgt. Dass eine solche schlüssig und rechtswirksam erklärt werden wird, kann auch angesichts des heute vermehrten Einsatzes von externen Experten, nicht generell vermutet werden.

Zudem müsste eine Einwilligung wohl vollständig wiederholt werden, wenn bspw. der Cloud-Anbieter gewechselt würde, da i.d.R. dann andere personelle Strukturen, Speicherorte usw. vorliegen werden. Ob eine pauschale Einwilligung, welche diese Eventualitäten mit abdeckt, strafrechtlich wirksam wäre, erscheint angesichts der an Einwilligungen zu stellenden Konkretisierungserfordernisse, zumindest zweifelhaft.[40] Die Schwierigkeit liegt hier insbesondere in der Komplexität des Sachverhalts, welcher dem Mandanten in seinen wesentlichen Grundzügen bewusst sein muss, damit die Einwilligung wirksam ist.[41]

Auch der Gedanke einer konkludenten Einwilligung der Berechtigten kann ebenso wenig zu ausreichender Rechtssicherheit führen. Es dürfte zwar vielfach offensichtlich sein, dass sich die aufgesuchten Berufsgeheimnisträger zeitgemäßer EDV-Anlagen (Ausstattung) bedienen, die üblicherweise von externem Fachpersonal eingereicht und gewartet werden müssen, jedoch darf dies nicht zu Lasten des Betroffenen gehen. Behält man die vom Gesetzgeber vorgeschlagene Differenzierung zwischen den berufsmäßig tätigen Gehilfen und den Personen, die bei dem Geheimnisträger zur Vorbereitung auf den Beruf tätig sind einerseits (§ 203 Abs. 3 Satz 1 StGB-E) und den sonstigen mitwirkenden Personen (§ 203 Abs. 3 Satz 2 StGB-E) andererseits im Hinterkopf, so lässt sich die Annahme einer konkludenten Einwilligung allenfalls bei den „berufsmäßig tätigen Gehilfen" annehmen. Weil diese im Gegensatz zu den „sonst mitwirkenden Personen" in der Sphäre des Berufsgeheimnisträgers eingegliedert sind.

---

[40] Vgl. nur Roxin, Strafrecht AT 1, § 13, Rn. 51 ff., so auch Cornelius, a.a.O. (Fn.9), S. 384 f.
[41] Preuß, a.a.O. (Fn.4), S. 807.

Letztlich erscheint die Einholung einer wirksamen Einwilligung aller potenziell betroffenen Personen zur vollständigen rechtlichen Absicherung des Vorgangs in der Praxis zumindest in vielen Fällen nicht praktikabel (und zumutbar). Es verbleibt ein erhebliches Strafbarkeitsrisiko.

Prof. Dr. Carsten Momsen