Michael Knopp

Pseudonym – Grauzone zwischen Anonymisierung und Personenbezug

Pseudonyme sind lange als Instrument datenschutzfreundlicher Verfahrensgestaltung und als Mittel des Selbstdatenschutzes anerkannt. Diensteanbieter werden in verschiedenen Rechtsnormen wie dem TMG angehalten, pseudonyme Nutzungen zu ermöglichen. Datenverarbeitung wird jedoch zunehmend ausgelagert und spezialisiert, was Pseudonymen eine neue Funktion zukommen lässt. Pseudonymisierung soll dabei als Schutzmaßnahme für die Datenverarbeitung durch Dritte dienen und gegenüber dem Dienstleister den Personenbezug ausschließen. Die aktuelle Datenschutzgesetzgebung berücksichtigt diese Perspektive kaum. Was aber können und sollten Pseudonyme mit Blick auf Auftragsdatenverarbeitung, Outsourcing und Cloud-Computing aus Datenschutzsicht leisten?

1 Pseudonyme im Datenschutzrecht

Das Pseudonym hat erst relativ spät Einzug in das Bundesdatenschutzgesetz gehalten. Die Einführung einer Gesetzesdefinition von „Pseudonymisierung" war Teil der Novellierung vom 23.05.2001. Aufgegriffen wurde die Definition im Bundesdatenschutzgesetz, zunächst jedoch nur in § 3a BDSG als mögliche Maßnahme zur Gewährleistung von Datensparsamkeit.

Vorangegangen war dem bereits 1997 die deutlich konkretere Vorschrift, Nutzungsprofile zu Telediensten nur unter Verwendung von Pseudonymen zu bilden.[1] Daneben stand die Forderung nach dem Angebot pseudonymer Nutzungsmöglichkeiten von Telemediendiensten (damals Telediensten)[2] im damaligen Teledienstedatenschutzgesetz[3]. Während im Telemediendatenschutz jedoch die Ziele und die Funktion der Pseudonym-Verwendung leicht zu erschließen sind, fällt dies im Bundesdatenschutzgesetz deutlich schwerer.

Die Anforderung an Diensteanbieter, auch die pseudonyme Nutzung ihrer Angebote zu ermöglichen, dient dem Eigenschutz der Nutzer und deren Wahrnehmung ihrer informationellen Selbstbestimmung sowie ganz allgemein der Datensparsamkeit.[4] Die Nutzer können durch die Verwendung von Pseudonymen im Internet mit getrennten Identitäten agieren und in verschiedenen Rollen auftreten, ohne damit rechnen zu müssen, dass ihre verschiedenen Identitäten zusammengeführt werden. Es handelt sich also um einen Schutz gegen Profilbildung, gegen die dienstübergreifende Nachvollziehbarkeit des Nutzerverhaltens. In diesem Kontext ist es jedoch eine Maßnahme, die der Betroffene bzw. Nutzer ergreifen kann. Dasselbe Ziel wird mit § 5 Abs. 2 De-Mail-G und § 5 Abs. 3 SigG[5] verfolgt, die ebenfalls Pseudonyme zulassen bzw. als Option verfügbar machen.

Bei der Pflicht der Diensteanbieter, Nutzungsprofile ausschließlich pseudonym anzulegen und die Profile nicht mit Bestandsdaten zusammenzuführen, ist dagegen die verantwortliche Stelle Adressat und die Pseudonymisierung eine Schutzmaßnahme zugunsten der Nutzer ohne deren Beteiligung. Das Verwenden von Pseudonymen schränkt die Datenverarbeitung der Diensteanbieter ein, wobei diese selbst die faktische Möglichkeit haben, das Pseudonym aufzudecken und hieran lediglich rechtlich gehindert werden.

Das Konzept der Datensparsamkeit des Bundesdatenschutzgesetzes (§ 3a Satz 1 BDSG), dem die Definition der Pseudonymisierung dient, ist abstrakter. Personenbezogene Daten sollen immer dann pseudonymisiert oder anonymisiert werden (§ 3a Satz 2 BDSG), wenn der Verwendungszweck es erlaubt. Zum Schutz der Betroffenen soll von vornherein die personenbezogene Verarbeitung vermieden oder eingeschränkt werden. Pseudonyme haben den Vorteil, dass es möglich bleibt, Daten zusammenzuführen, die sich auf dieselbe pseudonyme Identität beziehen. Das

1 S. zunächst § 4 Abs. 4 TDDSG, dann § 6 Abs. 3 TDDSG, heute § 15 Abs. 3 TMG.
2 S. zunächst § 4 Abs. 1 TDDSG, dann § 4 Abs. 6 TDDSG, heute § 13 Abs. 6 TMG.
3 Das TDDSG ist zum 01.03.2007 durch das Telemediengesetz ersetzt worden.

Michael Knopp, Jurist

Berater bei der Secorvo Security Consulting GmbH. Schwerpunkte: Datenschutz und Rechtsfragen im Kontext der IT-Sicherheit.

E-Mail: michael.knopp@secorvo.de

4 Taeger/Gabel (Moos), BDSG, 2. Aufl. 2013, § 13 TMG Rn. 48; auch hier die Datensparsamkeit und das Ziel eines Netzes ohne personenbezogene Daten betonend Roßnagel (Jandt/Schaar/Schulz), Recht der Telemediendienste, 2013, § 13 TMG Rn. 127.
5 Roßnagel, s. Fn. 4, § 5 SigG Rn. 26 f.

Pseudonym als Instrument des Selbstdatenschutzes erlaubt auch rechtsgeschäftliches Handeln, da die Zuordnung des Handelns zu einer bestimmten Person möglich bleibt.

Neben der Funktion als Umsetzungsmittel der Datensparsamkeit, die jedoch in § 3a BDSG lediglich als nicht sanktionsbewehrte Zielvorgabe zu sehen ist,[6] wird die verantwortliche Stelle im Bundesdatenschutzgesetz in den §§ 30 Abs. 1 S. 1, 30a Abs. 3 S. 2 BDSG zur Pseudonymisierung als Vorstufe einer späteren Anonymisierung verpflichtet. Hier wird Pseudonymisierung als Schutzmechanismus gegen einen Missbrauch der Daten verwendet.[7]

Weitere Pflichten zur Pseudonymisierung, ebenfalls als Schutzmaßnahme, sehen bspw. § 299 Abs. 1 Nr. 1 SGB V für die Verwendung von Patientendaten zur Qualitätssicherung oder § 40 Abs. 2 des Arzneimittelgesetzes (AMG) bei der Datenweitergabe nach Durchführung klinischer Prüfungen vor.

Das Interesse an Pseudonymisierung hat sich zwischenzeitlich gewandelt. Für die verantwortlichen Stellen geht es vielfach nicht um Datensparsamkeit oder um eine datenschutzfreundliche Gestaltung. Stattdessen wollen sie Pseudonymisierung nutzen, um entstehende Interessenskonflikte – beispielsweise beim Einsatz von Cloud-Diensten oder allgemeiner im Kontext der Auslagerung von Datenverarbeitungen an Dritte und deren Unterauftragnehmer – zu lösen. Das Interesse, durch Pseudonyme Erleichterungen bei den die Datenverarbeitung begleitenden Maßnahmen zu gewinnen, ist neben die bisherige Ausrichtung getreten.

2 Datenschutzrechtliche Wirkung der Pseudonymisierung

Auch wenn Definition und verschiedenen Pflichten zur Anwendung von Pseudonymisierung durch das Bundesdatenschutzgesetz und das Telemediengesetz vorgegeben werden, fehlt es an einer Regelung zur datenschutzrechtlichen Wirkung der Pseudonymisierung.

Eine Auswirkung besteht für den Ausgang von Interessensabwägungen im Rahmen des § 28 Abs. 1 Nr. 2 BDSG oder § 32 Abs. 1 BDSG.[8] Ist der verantwortlichen Stelle eine pseudonymisierte Verarbeitung möglich, kann es sich negativ auf Abwägungsergebnisse auswirken, wenn sie dennoch nicht eingesetzt wird.

Im Weiteren ist nach Arten von Pseudonymen, Grundannahmen zum Personenbezug, dem Verwendungskontext und den verschiedenen Regelungskontexten zu unterscheiden. Wegen der immer wieder vorkommenden Vermengungen und Verwechslungen sollte zudem die Abgrenzung zur Anonymisierung und Verschlüsselung betrachtet werden.

Festzuhalten ist außerdem, dass Nummern, Codierungen oder ähnliches nicht per se Pseudonyme darstellen. Telefonnummern oder auch IP-Adressen dienen nicht dem Erschweren der Zuordnung, die Zuordnung unterliegt auch keinem besonderen Schutz. Die IP-Adresse bspw. kann nicht nur durch den Provider, sondern durch jeden, der ein Login unter Kenntnis der Personenzuordnung verlangt, für einen bestimmten Zeitraum zugeordnet werden. Es handelt sich um keine Verfahren, die auch nur die Erschwerung der Zuordnung zum Ziel haben.

2.1 Pseudonymisierungsformen

Unter dem Begriff Pseudonyme verbergen sich sehr viele verschiedene Formen und Verwendungskontexte, so dass eine einheitliche Behandlung im Grunde von vornherein ausscheidet.

Bereits ein Blick auf die Gesetzesdefinitionen bestätigt diese Annahme. Während § 3 Abs. 6a BDSG für den Prozess der Pseudonymisierung lediglich „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“ fordert, lautet § 2 Abs. 2 Nr. 7 des Landesdatenschutzgesetzes Schleswig-Holstein „Pseudonymisieren [ist] das Verändern personenbezogener Daten derart, dass die Einzelangaben […] ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“. Mit „wesentlich erschweren“ verlangt das BDSG, ob beabsichtigt oder nicht,[9] weniger als die an der Anonymisierungsdefinition orientierte zweite Definitionsvariante.

§ 30a BDSG wiederum beschreibt zwar eine Pseudonymisierung durch die Trennung von Identifizierungsmerkmalen von den Datensätzen, verwendet die Legaldefinition aber überhaupt nicht und sieht von einer Qualitätsanforderung völlig ab. Das deutet eine Unterscheidung bereits an: die Qualität der Pseudonymisierung. Ein Pseudonym kann gegenüber Dritten, die die Zuordnungsregel nicht kennen, die Qualität einer faktischen Anonymisierung besitzen. Es kann aber auch nur zu einer Erschwerung der Zuordnung führen, die für praktisch jeden überwindbar ist, dem es den Aufwand wert ist.

Neben der Qualität ergeben sich weitere Unterschiede, die zu beachten sind. Wesentliche Unterscheidungsmerkmale liegen darin, wer ein Pseudonym erstellt und wer die Zuordnungsfunktion verwaltet oder kennt. Das kann lediglich der Betroffene selbst, ebenso ein Treuhänder der verantwortlichen Stelle, ein vertrauenswürdiger Dritter oder die verantwortliche Stelle sein (etwa im Kontext von § 15 TMG).[10]

Zu unterscheiden sind auch Pseudonyme, unter denen der Betroffene auftritt, also eine Verwendung als Selbstschutzmechanismus, und solche, die als Schutzmechanismus durch eine verarbeitende Stelle völlig unabhängig und evtl. sogar in Unkenntnis des Betroffenen verwendet werden.

Die Frage nach der Wirkung stellt sich hier mit verschiedenen Bezügen. Bei nur dem Betroffenen bekannten Zuordnungen – ein heute eher theoretisches Konzept, da das Pseudonym so gut wie nie ohne weitere Identifizierungsmerkmale verwendet werden wird[11] – stellt sich für Verwender bereits die Frage, ob eine Erhebung personenbezogener Daten vorliegt. Bei der Verwendung als Schutzmechanismus stellt sich die Frage, ob für Dritte keine personenbezogenen Daten vorliegen (wobei die obigen Unterscheidungen weiter zum Tragen kommen) und ob hierdurch weitere oder andere Schutzmaßnahmen obsolet werden.

6 Gola/Schomerus, BDSG, 10.Aufl. 2010, § 3a Rn. 2.

7 Taeger/Gabel (Munz), s. Fn. 4, § 30a Rn. 22; BT-Drs. 16/13657, S. 20.

8 Taeger/Gabel (Taeger), s. Fn. 4, § 28 Rn. 59 (Auswirkung auf die Erforderlichkeitsbeurteilung); Möncke, DuD 98, 565.

9 Die Gesetzesbegründung gibt hier keine Hinweise, BT-Drs. 14/4329, S. 33.

10 So die Unterscheidungen nach Simitis (Dammann), BDSG, 8. Aufl. 2014, § 3 Rn. 220 ff; Roßnagel, Scholz, MMR 2000, 721 (725); Plath (Schreiber), BDSG, 2013, § 3 Rn. 63; Härting, NJW 2013, 2065.

11 Diese Voraussetzung für fehlenden Personenbezug für Dritte formulieren Roßnagel/Scholz, s. Fn. 10, 725.

2.2 Anonymisierung und Verschlüsselung

Häufig wird – wohl auch zur Vereinfachung – festgestellt, pseudonyme Daten seien, eine entsprechende Pseudonymisierungsqualität vorausgesetzt, für Dritte anonymen Daten gleichzusetzen. Angesichts dessen, dass mit der grundsätzlichen und beabsichtigten Zuordnungsmöglichkeit von Pseudonymen bereits definitionsgemäß ein Unterschied zwischen beiden Datenarten besteht, geht dieser Ansatz wenigstens teilweise fehl. Anonymisierte Daten sollte selbst die anonymisierende Stelle nicht wieder zuordnen können.[12] Gerade in Bezug auf die Verwendung eines relativen Verständnisses von Personenbezug sollte eine durchgängige, nicht relativierte Unterscheidung zwischen anonym und pseudonym aufrecht erhalten werden, allein schon um eine differenzierte Diskussion der Rechtswirkung zu ermöglichen. Begriffsfindungen wie anonyme Pseudonyme[13] greifen zwar bestehende Qualitätsunterschiede in Bezug auf Dritte auf, führen aber auch zu Verwirrung.

Anonymität stellt datenschutzrechtlich den Gegenpol zum Personenbezug dar und wird damit zur Anwendungsgrenze von Datenschutzrecht. Pseudonymisierung ist hierauf jedenfalls nicht angelegt. Selbst in der Hand von Dritten sind pseudonyme Daten immer noch dazu bestimmt, für mindestens eine Stelle in Besitz der Zuordnungsregel personenbezogen zu sein, wodurch Begriffe wie „irreversible Pseudonymisierung“[14] zum Widerspruch in sich werden.

Hinsichtlich der Verschlüsselung kann auf die diesbezüglichen Beiträge in diesem Heft verwiesen werden. Wird die Verschlüsselung zur Ersetzung der Identifizierungsmerkmale eingesetzt, ist sie schlicht ein Pseudonymisierungswerkzeug. Ansonsten schließt Verschlüsselung unberechtigte Dritte vom Zugriff aus, setzt aber gerade nicht bei der Zuordnung an. Bei verschlüsselten Dateien hält ein Dritter überhaupt keine verwendbaren Daten in den Händen, solange die Verschlüsselung hält und er die Daten nicht sehen kann. Bei pseudonymisierten Daten erhält ein Dritter dagegen verarbeitungsfähige Einzelangaben, er kann bloß den Betroffenen nicht bestimmen.

2.3 Personenbezug

Die Frage nach dem Personenbezug ist für die Einordnung von Pseudonymen entscheidend. Hier kommt die häufig zwischen vermeintlichen Extremen geführte Auseinandersetzung um ein absolutes oder relatives Verständnis des Personenbezuges zum Tragen. Das Meinungsspektrum ist hier tatsächlich sehr breit.[15] Für Anhänger eines objektiven oder absoluten Begriffs kommt es nicht darauf an, ob die betrachtete Stelle, die im Besitz von personenbezogenen Daten ist, tatsächlich selbst in der Lage ist, den Bezug herzustellen. Da der Personenbezug, ggf. durch Dritte mit den erforderlichen Mitteln oder dem notwendigen Zusatzwissen hergestellt werden kann, handelt es sich um personenbezogene Daten und auch die betrachtete Stelle muss im Umgang mit den Daten das Datenschutzrecht beachten.

Dagegen steht ein relatives Verständnis von Personenbezug, bei dem der Personenbezug von Daten aus Sicht der betrachteten Stelle zu beurteilen ist. Wenn der betrachteten Stelle eine Zuordnung nur mit unverhältnismäßigem Aufwand möglich wäre, sollen die Daten ihr gegenüber als anonym gelten.
Trotz vermittelnder Ansätze[16] ist eine rechtssichere Einordnung gerade auch von Pseudonymen hier fern.[17] Hinsichtlich des relativen Verständnisses wird letztlich das Entstehen von Schutzlücken mit Blick auf die Betroffenen befürchtet. Andererseits ist den Kritikern zuzustimmen, dass die generelle Zurechnung fremder Zuordnungsmöglichkeiten die aus dem Datenschutzrecht erwachsenden Pflichten unverhältnismäßig ausdehnt.[18]

Bei Pseudonymen ist definitionsgemäß klar, dass wenigstens eine Stelle die Zuordnungsmöglichkeit besitzt. Es liegt auch auf der Hand, dass eine Stelle, der die Zuordnung mit den ihr vernünftigerweise zur Verfügung stehenden Mitteln – so Erwägungsgrund 26 der Datenschutzrichtlinie[19] – nicht möglich ist, jedenfalls nicht sämtliche Pflichten einer datenschutzrechtlich verantwortlichen Stelle erfüllen kann. Wie sollte sie z. B. einem Anfragenden Auskunft erteilen oder abschätzen, ob, mangels fortdauernder Erforderlichkeit, im Einzelfall Daten zu löschen sind? Auf der anderen Seite kann aber auch nicht geleugnet werden, dass die definitionsgemäße Möglichkeit des wiederherstellbaren Personenbezugs zu einem ebenso fortdauernden Schutzbedarf der Betroffenen führt.

Weiter oben wurde bereits dargestellt, dass die verschiedenen Formen pseudonymisierter Daten sich nicht zuletzt hinsichtlich der Qualität der Pseudonymisierung und ihrer Beständigkeit gegenüber Dritten erheblich unterscheiden können. Selbst wenn man mit einem relativen Personenbezugsbegriff grundsätzlich bejaht, dass Pseudonymisierung den Personenbezug für Dritte ausschließen kann und diese dann bezüglich der pseudonymen Daten kein Datenschutzrecht mehr zu beachten haben, wäre dies für jeden Dritten und für die pseudonymisierten Daten im Einzelfall zu prüfen.[20]

2.4 Derzeitige Wirkung

Die aktuelle rechtliche Wirkung der Pseudonymisierung soll hier nur in Bezug auf die oben gestellte Frage, also mit Blick auf die Auslagerung und Weitergabe an Dienstleister, v. a. natürlich auch in die Cloud, betrachtet werden.

In diesem Fall muss der Auftraggeber oder der Cloudnutzer die von ihm ausgehende Weitergabe der Daten datenschutzrechtlich beurteilen, die datenschutzrechtliche Prüfung erfolgt also aus seiner Perspektive.

Wenn diese Stelle in der Lage ist, Dienstleistern lediglich pseudonymisierte Daten zur weiteren Verarbeitung zur Verfügung zu stellen, ergeben sich folgende Fragen: Bedarf die Weitergabe als Übermittlung einer Rechtsgrundlage? Kommt eine Einwilligung

12 Diese begriffliche Systematik wird allerdings in § 30 Abs. 1 BDSG bereits nicht durchgehalten.

13 S. z.B. Simitis (Scholz), s. Fn. 10, § 3 Rn. 218.

14 Plath (Schreiber), s. Fn. 10, § 3 Rn. 62.

15 Zur Diskussion, meist anhand der IP-Adresse als Beispiel, Brink/Eckhardt, ZD 2015, 205; Breyer, ZD 2014, 400; Soecht/Müller-Riemenschneider, ZD 2014, 71; aus dem Blickwinkel generell zunehmender Bezugsmöglichkeiten für eine Abkehr von der Konzentration auf den Personenbezug Karg, ZD 2012, 255.

16 S. bspw. Brink/Eckhardt, s. Fn. 15, die auf die Wahrscheinlichkeit abstellen, mit der eine Verwendung des Zuordnungswissens Dritter durch die verantwortliche Stelle zu erwarten ist.

17 Die Datenschutzaufsichtsbehörden tendieren zu einer weitreichenderen Zurechnung von Zuordnungsmöglichkeiten und bejahen ausdrücklich den Personenbezug für nach § Abs. 6a BDSG pseudonymisierte Daten, s. Düsseldorfer Kreis, Orientierungshilfe Cloud Computing, Version 2.0, 2014, S. 12.

18 Roßnagel/Scholz, s. Fn. 10, 726.

19 Ergänzend zum Verständnis Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP136, S. 17 ff.

20 Eine pauschale Aussage wird dementsprechend zumeist auch abgelehnt, bspw. Simitis (Scholz), s. Fn. 10, § 3 Rn. 218; Taeger/Gabel, s. Fn. 4, § 3 Rn. 48; anders (Personenbezug für Dritte ablehnend) Roßnagel/Banzhaf/Grimm, Datenschutz im Electronic Commerce, 2003, S. 151.

in Betracht? Ist ein Auftragsdatenverarbeitungsvertrag erforderlich (und möglich)?

Beispiele für die Relevanz gibt es zuhauf, darunter auch solche, die Berufsgeheimnisse umfassen. Etwa die Einschaltung von externen Hilfskräften (Schreibkräfte, IT-Dienstleister, Aktenentsorgung) durch Ärzte oder der Einsatz nachgelagerter Dienstleister durch Steuerberater. Auch einfache Beispiele, wie der selbständige ausführende Schneider eines Anbieters für Maßanzüge, sind betroffen.

Die Pseudonymisierung hat hier letztlich die Funktion einer Sicherheitsmaßnahme. Für die verantwortliche Stelle liegen, da sie die Zuordnung kennt, auch bei dem Dienstleister personenbezogene Daten vor. Der Dienstleister kann im Idealfall die Daten keiner bestimmten Person zuordnen, obwohl dies auch nicht immer auszuschließen ist: die Zahl der Personen mit einer Körpergröße von bspw. 2,10 m und einer bestimmten Schulterbreite im Beispiel des maßgeschneiderten Anzugs lässt sich vermutlich auch mit öffentlich zur Verfügung stehenden Mitteln sehr eng begrenzen. Welche Perspektive ist nun für die verantwortliche Stelle relevant? Der eigene Personenbezug oder der nach einem relativen Verständnis fehlende Personenbezug des Dienstleisters? Auch die Vertreter des relativen Personenbezuges bleiben hierauf in der Regel die Antwort schuldig.[21]

Da die verantwortliche Stelle vor allem angesichts der Haltung der Aufsichtsbehörden[22] – derzeit jedenfalls – nicht von einer Unanwendbarkeit des Datenschutzrechts ausgehen kann, bleibt ihr nur, weiter nach einer Rechtsgrundlage zu suchen oder einen Auftragsdatenverarbeitungsvertrag abzuschließen.[23]

In Betracht kommt bei Verwendung pseudonymisierter Daten in der Auftragsdatenverarbeitung allerdings, die Anforderungen an die technischen und organisatorischen Maßnahmen zu senken. Diese können jedoch nicht gänzlich entfallen, so dass diese Wirkung begrenzt bleibt.

Geht man von einer Übermittlung aus, kann die Pseudonymisierung als Abwägungskriterium bezüglich der Berücksichtigung der Betroffeneninteressen angeführt werden.

Zusammenfassend lässt sich festhalten, dass die derzeitige Wirkung der Pseudonymisierung eher gering bleibt, weil belastbare Regelungen fehlen. Hier steht die 2001 bereits vorgesehene grundlegende Reform des Datenschutzrechts weiter aus. Da Pseudonymisierung jedoch bislang auch in der geplanten Datenschutzgrundverordnung keine Rolle zu spielen scheint, muss hierauf wohl weiter gewartet werden.[24]

3 Mögliche Wirkungen

Eine andere Frage ist, ob Regelungen überhaupt geschaffen werden könnten oder sollten, die zu wesentlichen Erleichterungen in den aufgezeigten Fällen führen würden, also beispielsweise zum Entfallen der mit der Auftragsdatenverarbeitung verbundenen Pflichten.

Die gesetzlichen Regelungen haben – abgesehen von den Pseudonymisierungspflichten – die Verbreitung von Pseudonymisierung als datenschutzfördernde Technik[25] zum Ziel. Der Einsatz von Pseudonymisierung zur Begrenzung der Datenverbreitung durch Aufgabenteilung hat bislang nicht im Fokus gestanden.

Gerade angesichts fortschreitender Aufgabenteilung und Verteilung von Datenverarbeitungen sollte hierauf jedoch mehr Aufmerksamkeit verwendet werden. Die Auftragsdatenverarbeitung ist als Instrument vielfach überfordert, den Betroffenenschutz realistisch zu gewährleisten. Selbst bei einer weiteren Verbreitung von Auftragnehmerzertifizierungen und einer Vereinheitlichung der Zertifizierungsanforderungen auf einem hohen Niveau kann Auftragsdatenverarbeitung dem Kontrollverlust gerade im Bereich des Cloud Computing nur begrenzt entgegenwirken. Man betrachte nur entstehende Vertragsketten beim Einsatz von Unterauftragnehmern, die Problematik der Verarbeitung außerhalb Europas und die bestehenden Supportzugriffe von Unterauftragnehmern oder verbundenen Unternehmen. Eine rein normative Lösung erfordert hier schon Optimismus.

Eine Pseudonymisierung vor der Weitergabe kann hier Risiken mindern und wäre daher zu fördern. Ein Verzicht auf datenschutzrechtliche Vorgaben ist dennoch nicht angebracht. Pseudonymisierung sollte auch gegenüber Dritten nicht mit Anonymität gleichgesetzt werden. Auch den Empfänger pseudonymer Daten sollten weiter datenschutzrechtliche Pflichten treffen. Es bestehen zu viele Risiken der Zuordnung, sei es durch Bekanntwerden der Zuordnungsregel, durch nicht ausreichend entfernte oder veränderte Identifikationsmerkmale oder durch Zusatzwissen der Empfänger, um nur einige Beispiele zu nennen. Der Empfänger sollte daran gehindert bleiben, die pseudonymen Daten uneingeschränkt weiterzugeben und weiter verpflichtet sein, die Daten gegen einen unbefugten Gebrauch zu schützen. Eine generelle Erlaubnis zur Weitergabe für die verantwortliche Stelle, den Auftraggeber, würde angesichts dessen ebenfalls zu weit gehen.

Eine Erlaubnis zum Dienstleistereinsatz unter Verzicht auf eine Auftragsdatenverarbeitung käme nur im Gegenzug zur Regelung weiterer Pflichten und Anforderungen bei der Pseudonymisierung in Betracht. Dann aber könnte Pseudonymisierung zu einem wichtigen Instrument bei der Aufgabenteilung und dem Dienstleistereinsatz werden.

4 Fazit

Die Pseudonymisierung ist ein unvollständig und lückenhaft geregeltes Instrument des Datenschutzrechts. Gerade in Bezug auf Auslagerung und v. a. auch beim Cloud Computing könnte der Pseudonymisierung eine wichtige Rolle im Ausgleich zwischen den bestehenden Kontrollverlusten und den Betroffeneninteressen sowie als Korrektiv zu der sehr verpflichtungsorientierten Auftragsdatenverarbeitung zukommen. Hierzu sind aber ergänzende Regelungen nötig, die einerseits die Pflichten pseudonymisierender verantwortlicher Stellen regeln, andererseits aber die Verarbeitung pseudonymisierter Daten erleichtern.

21 Am weitesten in der Betrachtung gehen hier Roßnagel/Scholz, s. Fn.10, allerdings weitgehend aus der Perspektive der Erhebung und des nachträglichen Aufdeckungsrisikos. Im Ergebnis werden hier ausgehend vom nicht gegebenen Personenbezug pseudonymer Daten ergänzende Regelungen gefordert. Unter einer Betonung von auszuweitenden Verboten der Identifizierung kommt Härting, NJW 2013, 2065, zu dem Ergebnis, dass das „Verbot mit Erlaubnisvorbehalt" auf pseudonymisierte Daten für die verantwortliche Stelle anwendbar ist. In Konsequenz wird gefordert, dass genau dies zu ändern sei, weil es den Anreiz minimiere, Pseudonyme zu verwenden.

22 S. oben Fn. 17 (OH-Cloud).

23 Die Einwilligung dürfte in diesem Kontext eine eher geringe Rolle spielen. Der Verweis von Härting, s. Fn. 21, 2068, zur Vorsicht auf eine Einwilligung zu setzen, dürfte wenigstens in dem hier besprochenen Kontext fehlgehen.

24 S. Karg in diesem Heft.

25 Zur Einordnung als datenschutzfreundliche Technik im Bereich Kommunikation Danesis u.a., Privacy and data protection by design, 2014, S. 29.