Christian Koenig

Die Digitale Kopie von Briefsendungen

Postgeheimnis auf dem „Darkserver"?

Mit dem Produkt „Digitale Kopie" wird dem Empfänger zeitgleich zu einer physischen Briefsendung des geschäftlichen Versenders eine Kopie des physischen Briefes in sein digitales Postfach gelegt. Digitale Kopien von physischen Briefen werden in Form von PDF-Dateien jeweils streng inhalts- und datenakzessorisch zu einer konkreten physischen Postsendung verarbeitet, ausgewertet und elektronisch zugestellt. Es bedarf nicht viel Phantasie, sich Google-ähnliche Geschäftsmodelle vorzustellen, welche aufgrund einer Auswertung der Algorithmen der Verbindungsdaten und näheren Umstände des digitalisierten Postverkehrs den Datenschatz für das Werbegeschäft zu heben beabsichtigen. Der folgende Beitrag legt dar, dass es sich bei dem Produkt Digitale Kopie um einen dem Postgeheimnis nach § 39 PostG unterliegenden – in die physisch erbrachte Postdienstleistung integrierten – Paralleldienst handelt. Zumindest aber unterliegen die elektronischen Verarbeitungshandlungen des Postdienstleisters den Geboten und Verboten aus dem Postgeheimnis, da die Verarbeitungsagenten identische Inhalte und Daten in den Händen halten, welche aus parallel zugestellten physischen Briefsendungen generiert worden sind.

1 Digitale Kopie

Seit dem 1.1.2019 stellt ein großer Postdienstleister Geschäftskunden seine neue Produktplattform für die Digitale Kopie zur Verfügung. Bei diesem Produkt wird dem Empfänger zeitgleich zu einer physischen Briefsendung eines Geschäftskunden eine Kopie des physischen Briefes in sein digitales Postfach gelegt. Laut der Produktinformation des Postdienstleisters[1] soll der Vorteil darin bestehen, dass die Empfänger ihre Briefpost zusätzlich online erhalten und diese von überall elektronisch abrufen können. Für den absendenden Geschäftskunden soll der Vorteil darin bestehen, dass im Vergleich zu anderen elektronischen Versandverfahren die Digitale Kopie besser in die Regelprozesse zu integrieren sei. Der Einsatz von besonderen elektronischen Verschlüsselungstechniken biete darüber hinaus ein hohes Maß an Datensicherheit.

Digitale Kopien werden parallel zur Produktion und Einlieferung physischer Briefsendungen hergestellt. Nach einer Ankündigung der physischen Briefsendung durch den absendenden Geschäftskunden über das Auftragsmanagement-System des Postdienstleisters erfolgt aufgrund der zugeteilten Frankier-ID die Zuordnung der physischen Briefsendung zu der Digitalen Kopie. Geschäftskunden müssen die Druck- und Adressdaten ihrer Briefsendungen in die von dem Postdienstleister vorgegebenen elektronischen Formate umsetzen.[2] Der Herstellungsprozess der Digitalen Kopie lässt sich in den fünf folgenden Schritten zusammenfassen:

1. Der Postdienstleister erfasst vorab die Kontaktdaten des absendenden Geschäftskunden. Nach Prüfung dieser Kontaktdaten erhält der Geschäftskunde seine persönlichen Zugangsdaten.
2. Parallel zu den physischen Briefen erzeugen die Geschäftskunden ein Datenpaket, das sowohl allgemeine Auftrags- und Lieferinformationen als auch die einzelnen Briefe in elektronischer Form enthält. Dieses Datenpaket muss verschiedene Kriterien zur technischen Verarbeitung erfüllen.

1 Deutsche Post AG, Geschäftskundenleitfaden zur Digitalen Kopie, Einrichtung und Einlieferung (Stand 29.8.2018).

Univ.-Prof. Dr. iur. Christian Koenig LL.M. (LSE)

Direktor am Zentrum für Europäische Integrationsforschung (ZEI) der Universität Bonn

E-Mail: profkoenig@gmx.de

2 Geschäftskundenleitfaden zur Digitalen Kopie, Kapitel 4 „Abläufe und technische Spezifikationen".

3. Der Postdienstleister prüft die eingelieferten Datenpakete auf die Erfüllung der technischen Anforderungen sodann in einem Testlauf vor der tatsächlichen Produktion Digitaler Kopien. Auf der Testplattform legen die Geschäftskunden ein Datenpaket gemäß der technischen Spezifikation ab. Die Testdaten enthalten nur fiktive Inhalte und Empfänger, keine personenbezogenen Daten. Die Testdaten werden nach erfolgreicher Prüfung vollständig gelöscht. Der erfolgreiche Test ist Voraussetzung dafür, dass die Geschäftskunden die Freigabe für die Herstellung der Digitalen Kopie erhalten.[3]
4. Sind die Abnahmekriterien im Testlauf erfüllt worden, erhalten die Geschäftskunden die Produktionsfreigabe und ihre individuellen Zugangsdaten für das eigentliche Produktionssystem. Zuvor müssen die Geschäftskunden ihre elektronischen Schlüssel für das Produktionssystem des Postdienstleisters übermitteln. Die Datenpakete werden nun über eine asymmetrisch verschlüsselte Netzwerkverbindung vom digitalen Einlieferer auf die Server des Postdienstleisters übertragen. Zur Authentifizierung wird ein öffentlicher Schlüssel (mit 3072-bit-Schlüssellängen) verwendet, wobei die sichere Übertragung der verschlüsselten Datenpakete der Geschäftskunden den aktuellen Anforderungen der Europäischen Datenschutz-Grundverordnung (DS-GVO) entsprechen soll. Der gesicherte Zugang zum elektronischen Einlieferungsbereich wird durch ein Schlüsselpaar gewährleistet, das aus einem geheimen privaten Schlüssel und einem öffentlichen Schlüssel besteht. Der geheime Schlüssel verbleibt auf dem Rechner, von dem die Einlieferungen hochgeladen werden. Der öffentliche Schlüssel wird im Benutzerprofil des Geschäftskunden bei dem Postdienstleister hinterlegt.[4] Die Einlieferung des Datenpakets des Geschäftskunden erfolgt in dessen persönlichen, abgesicherten Einlieferungsbereich. Ein Gesamtpaket darf je Einlieferung 5 GB nicht überschreiten. Bei Überschreiten der Maximalgrößen wird die Einlieferung nicht verarbeitet und aus dem Verzeichnis „./upload' entfernt. Alle Dateneinlieferungen werden als ZIP-Archiv gepackt und anschließend verschlüsselt.
5. Nach dem Hochladen hat der Geschäftskunde die Datenpaket-Datei dahingehend umzubenennen, dass sie die Dateiendung „.zip.pgp' besitzt. Damit wird die Datei zur Verarbeitung freigegeben. Falls das nicht innerhalb von 24 Stunden geschieht, wird diese Datei aus dem Verzeichnis „./upload' gelöscht. Nachdem die Datei zur Weiterverarbeitung abgeholt wird, wird die Datei ebenfalls aus dem Verzeichnis „./upload' entfernt.

Die Digitale Kopie wird mit der Erfassung der physischen Sendung im Produktionsprozess dem Empfänger parallel zugestellt. Die Zustellung erfolgt in den digitalen Briefkasten der Privatkunden (E-POST-App und -Portal). Bei Bedarf des Versenders erfolgt die Zustellung Ende-zu-Ende verschlüsselt; die Entschlüsselung erfolgt dann automatisiert im digitalen Briefkasten.

3 Geschäftskundenleitfaden zur Digitalen Kopie, Kapitel 5 „Technische Checkliste Einrichtung Digitale Kopie".

4 Geschäftskundenleitfaden zur Digitalen Kopie, Kapitel 6 „Anleitungen".

2 Einfachgesetzliche Ausgestaltung des Postgeheimnisses

Im Zuge der ganz überwiegenden Privatisierung des größten deutschen Postdienstleisters endete seine Qualifikation als unmittelbar auf die Wahrung der Grundrechte, insbesondere des Postgeheimnisses nach Art. 10 des Grundgesetzes, verpflichtete staatliche Einrichtung. Mithin vermag der Postdienstleister selbst keine staatlichen Grundrechtseingriffe mehr vorzunehmen.

Nunmehr soll § 39 PostG einen dem Art. 10 des Grundgesetzes entsprechenden Schutz des Postgeheimnisses auf einfachgesetzlicher Ebene gewährleisten. Nach der amtlichen Begründung zu § 39 PostG schützt das Postgeheimnis das Interesse des Bürgers, den Inhalt und die näheren Umstände seiner Kommunikation geheim zu halten. Dieses Geheimhaltungsinteresse besteht gegenüber staatlichen Stellen wie gegenüber privaten Dritten und vor allem den Erbringern der zur Kommunikation erforderlichen Transportdienste gleichermaßen.[5]

Demgegenüber beruht die Verpflichtung staatlicher Stellen zur Wahrung des Postgeheimnisses weiterhin unmittelbar auf Art. 10 des Grundgesetzes. Aufgrund der objektiven Grundrechtswirkungen als staatliche Schutzpflichten,[6] welche vom Bundesverfassungsgericht ausdrücklich für Art. 10 des Grundgesetzes hervorgehoben worden sind,[7] könnte insbesondere die Bundesnetzagentur gehalten sein, im Wege von geeigneten Anordnungen (§ 42 Abs. 1 und 2 PostG) zur Sicherstellung der Einhaltung der Pflichten zur Wahrung des Postgeheimnisses vorzugehen. Seit der Postprivatisierung begründet Art. 10 des Grundgesetzes in verstärktem Maße die Grundlage für staatliche Schutzpflichten,[8] welche nunmehr über § 42 Abs. 1 und 2 i. V. m. § 39 PostG konkretisiert und an die Bundesnetzagentur verpflichtend adressiert sind. Die objektive Grundrechtsentfaltung des Postgeheimnisses im Sinne staatlicher Schutzpflichten erfährt aufgrund der materiellen Nähe des Schutzbereiches von Art. 10 des Grundgesetzes zum allgemeinen Persönlichkeitsrecht nach Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 des Grundgesetzes, insbesondere dem Schutz personenbezogener Daten, eine weitere Verstärkung.[9]

Selbst wenn der größte deutsche Postdienstleister keine staatlichen Grundrechtseingriffe mehr vorzunehmen vermag, hat er auf der Produktplattform für die Digitale Kopie über die einfachgesetzliche Schutztransformation nach § 39 PostG einen dem Art. 10 des Grundgesetzes entsprechenden Gewährleistungsstandard des Postgeheimnisses auf einfachgesetzlicher Ebene sicherzustellen. Genügt er dem nicht, ist der Staat, vertreten durch die Bundesnetzagentur, durch geeignete Anordnungen nach § 42 Abs. 1 und 2 PostG – und zwar verfassungsrechtlich aufgrund der objektiven Grundrechtswirkungen als staatliche Schutzpflichten aus Art. 10 des Grundgesetzes auch gegenüber privat verursachten Gefährdungslagen – gehalten, die Einhaltung der Pflichten zur Wahrung des Postgeheimnisses sicherzustellen.

5 BT-Drucks. 13/7774, Seite 29.

6 *Herdegen*, in: Maunz/Dürig, Grundgesetz-Kommentar, 85. EL November 2018, Art. 1 Abs. 3 Rn. 20 ff.

7 BVerfG, Beschluss vom 20. Juni 1984, BVerfGE 67, 157 (185).

8 *Durner*, in: Maunz/Dürig, Grundgesetz-Kommentar, Art. 10 Rn. 76.

9 *Stern*, in: Beck'scher PostG-Kommentar, 2. Auflage 2004, § 39 Rn. 6.

3 Schutzbereich des Postgeheimnisses

3.1 Umstände des Postverkehrs sowie Inhalt von Postsendungen

Gemäß § 39 Abs. 1 PostG unterliegen dem Postgeheimnis die „näheren Umstände des Postverkehrs" sowie der „Inhalt von Postsendungen".

Welche Gegenstände als Postsendungen zu qualifizieren sind, ergibt sich aus § 4 Nr. 1 lit. a) – c), Nr. 5 PostG. Der Postverkehr erfasst sämtliche Vorgänge, die der Postbeförderung dienen. Damit werden durch den Schutz der näheren Umstände des Postverkehrs auch nicht-inhaltsbezogene Verbindungsdaten dem Postgeheimnis unterworfen. Geschützt wird nicht nur der Kommunikationsinhalt, sondern auch der gesamte Kommunikationsvorgang.[10] Erfasst sind damit alle Umstände, die mit der konkreten Benutzung eines Postdienstleisters zusammenhängen, insbesondere Absender und Empfänger, Ort und Zeit der Aufgabe einer Sendung sowie die Art und Weise der Inanspruchnahme der Postdienstleistung.[11] Das Postgeheimnis schützt damit auch vor der Offenbarung, Übermittlung oder Weitergabe von Verbindungsdaten, die unabhängig von ihrem Inhalt erkennen lassen, *wer mit wem, wann und auf welche Art und Weise* Briefe oder sonstige Postsendungen austauscht.[12]

Die Geschäftskunden übertragen PDF-Dateien mit Kopien von zu versendenden physischen Briefen, die anschließend für die Bereitstellung der Dienstleistung Digitale Kopie verwendet werden, über eine asymmetrisch verschlüsselte Netzwerkverbindung auf die Server des Postdienstleisters. PDF-Dateien gelten bei isolierter Betrachtung nach § 4 Nr. 1 lit. a) – c) PostG nicht als Postsendungen im Sinne von § 39 PostG. Auch die elektronische Übermittlung der PDF-Dateien unterfällt nicht dem sachlichen Schutzbereich des Postgeheimnisses, da sie nicht der Postbeförderung dient und es sich damit um keinen Postverkehr handelt.

Indes werden von dem Postdienstleister Digitale Kopien von physischen Briefen in Form von PDF-Dateien jeweils streng inhalts- und datenakzessorisch zu einer konkreten physischen Postsendung verarbeitet, ausgewertet und elektronisch zugestellt. Im Gegensatz zu der elektronischen Einlieferung der Sendungsdateien eines Geschäftskunden ist die Verarbeitung und Auswertung der PDF-Dateien durch den Postdienstleister nicht eine bloß postvorbereitende Tätigkeit, sondern ein Vorgang, der als Bestandteil des Empfängerservices der parallelen physischen Postbeförderung selbst dient. Mithin handelt es sich bei dem Produkt Digitale Kopie um einen dem Postgeheimnis nach § 39 PostG unterliegenden – in die physisch erbrachte Postdienstleistung integrierten – Paralleldienst. Zumindest aber unterliegen die elektronischen Verarbeitungshandlungen den Geboten und Verboten aus dem Postgeheimnis. Denn die Verarbeitungsprozesse beschränken sich nicht auf die digitale Daten-, Medien- und Übertragungswelt. Vielmehr halten die Verarbeitungsagenten identische Inhalte und Daten in den Händen, welche aus parallel zugestellten physischen Briefsendungen generiert worden sind.

10 BVerfGE 85, 386 (396); 100, 313 (358).

11 *Stern*, in: Beck'scher PostG-Kommentar, § 39 Rn. 10.

12 *Durner*, in: Maunz/Dürig, Grundgesetz-Kommentar, Art. 10 Rn. 77.

3.2 Verpflichtungs- und Verbotsadressat

Nach § 39 Abs. 2 PostG ist zur Wahrung des Postgeheimnisses verpflichtet, wer geschäftsmäßig Postdienstleistungen im Sinne von § 4 Nr. 1 PostG erbringt oder daran mitwirkt.

§ 4 Nr. 4 PostG definiert die geschäftsmäßige Erbringung von Postdiensten als *„das nachhaltige Betreiben der Beförderung von Postsendungen für andere mit oder ohne Gewinnerzielungsabsicht"*. Bei dem Produkt Digitale Kopie handelt es sich um einen dem Postgeheimnis nach § 39 PostG unterliegenden – in die physisch erbrachte Postdienstleistung integrierten – Paralleldienst. Zumindest aber unterliegen die elektronischen Verarbeitungshandlungen, welche geschäftsmäßig im Rahmen einer postalischen Dienstleistung gemäß § 39 Abs. 2 PostG erbracht werden, den Geboten und Verboten aus dem Postgeheimnis.

Darüber hinaus sind solche Dienstleister verpflichtet, welche an der Herstellung des – in die physisch erbrachte Postdienstleistung integrierten – Paralleldienstes Digitale Kopie *„mitwirken"*. Zu den Mitwirkenden zählen auch Erfüllungs- und Verrichtungsgehilfen sowie Subunternehmer.[13] Es ist davon auszugehen, dass an den Herstellungsschritten der Digitalen Kopie neben den Providern der elektronischen Kommunikationswege auch IT-Dienstleister an den digitalen Verarbeitungsprozessen beteiligt sind. Auch sie sind, indem sie an der Erbringung des Produkts Digitale Kopie mitwirken, nach Maßgabe von § 39 Abs. 2 PostG zur Wahrung des Postgeheimnisses verpflichtet.

3.3 Verbot der Kenntnisnahme

§ 39 Abs. 3 PostG untersagt es den nach Absatz 2 Verpflichteten, sich oder anderen über das für die Erbringung der Postdienste erforderliche Maß hinaus Kenntnis vom Inhalt von Postsendungen oder den näheren Umständen des Postverkehrs zu verschaffen. Damit wird in Bezug auf sämtliche Tatsachen, die dem objektiven Schutzbereich des Postgeheimnisses nach Absatz 1 unterfallen, ein generelles Verbot der Kenntnisverschaffung ausgesprochen.[14]

Die Kenntnisverschaffung übersteigt die bloße Kenntnisnahme. Über die passive Entgegennahme von Informationen hinausgehend ist die aktive Beschaffung von Daten aus einem konkreten Kommunikationsvorgang erfasst.[15]

Im Rahmen der Digitalen Kopieprozesse werden von den Geschäftskunden zur Verfügung gestellte PDF-Dateien von dem Postdienstleister verarbeitet, ausgewertet und elektronisch zugestellt. Diese PDF-Dateien enthalten digitale Kopien von physischen Briefen. Dabei ist die Gleichheit von den Daten und Inhalten der PDF-Dateien und der physischen Briefsendungen der Digitalen Kopie produktimmanent. Folglich werden durch die unmittelbare Bereitstellung der PDF-Dateien an die eigenen Mitarbeiter des Postdienstleisters und seine dritten Dienstleister Informationen über die physischen Briefsendungen vermittelt. Bei der Verarbeitung und Auswertung der PDF-Dateien werden Informationen über die Inhalte von Postsendungen bzw. die näheren Umstände des die Postsendungen betreffenden Postverkehrs insofern preisgegeben, als die Verarbeitungsagenten identische

13 BT-Drucks. 147/97, S. 46.

14 *Stern*, in: Beck'scher PostG-Kommentar, § 39 Rn. 21.

15 *Mayen*, in: Scheurle/Mayen, TKG, 3. Auflage 2018, § 88 Rn. 71. Für die Auslegung des Begriffs der Kenntnisverschaffung im Sinne von § 39 PostG ist aufgrund der strukturellen Parallelen zwischen dem Postgeheimnis und dem Fernmeldegeheimnis ein Rückgriff auf das Wortverständnis des § 88 TKG möglich.

Inhalte und Daten in den Händen halten, welche aus parallel zugestellten physischen Briefsendungen generiert worden sind.

Eine nach § 39 Absatz 3 PostG untersagte Kenntnisverschaffung setzt indes voraus, dass die eigenen Mitarbeiter des Postdienstleisters („sich verschaffen") bzw. ihre dritten Dienstleister („anderen verschaffen") erkennen, dass die übertragenen Datenpakete elektronisch erstellte Kopien der Inhalte und Verbindungsdaten physischer Postsendungen enthalten.

In Bezug auf die eigenen Mitarbeiter des Postdienstleisters ist hiervon bei lebensnaher Betrachtung der Verarbeitungsprozesse der Digitalen Kopien *prima facie* auszugehen. Die Mitarbeiter wissen offensichtlich, dass sie mit den Verarbeitungsprozessen des Produkts Digitale Kopie betraut sind. Bei der Verarbeitung der PDF-Dateien können sie Einblick in die elektronisch kopierten Inhalte und nicht-inhaltsbezogenen Verbindungsdaten der parallel versandten physischen Briefsendungen nehmen. Auch bei den von dem Postdienstleister eingebundenen IT-Drittdienstleistern liegt die Annahme nahe, dass ihnen die Parallelität zwischen den Daten und Inhalten der PDF-Dateien und denen der physischen Briefsendungen bekannt ist. Dass sich Inhalte und Verbindungsdaten mit denen der parallelen physischen Briefsendungen decken, ist zwingendes Merkmal des Produkts Digitale Kopie. Zwecks elektronischer Verarbeitung zur Digitalen Kopie, welche zumindest eine aktive Auswertung der Verbindungsdaten in Bezug auf die parallel versandten physischen Briefsendungen erfordert, liegt prima facie auch eine nach § 39 Abs. 3 PostG unzulässige Kenntnisverschaffung vor.

3.4 Anforderungen an einen Verzicht

Auf die Wahrung des Postgeheimnisses kann im Einzelfall nach allgemeiner Auffassung durch Einwilligung verzichtet werden.[16]

Ratione materiae setzt ein Verzicht auf die Wahrung des Postgeheimnisses voraus, dass diesem der wirksam erklärte Einverständniswille des Verzichtenden zugrunde liegt, dem Postdienstleister und ggf. weiteren bei der Herstellung von Digitalen Kopien *„mitwirkenden"* Drittdienstleistern *„über das für die Erbringung der Postdienste erforderliche Maß hinaus Kenntnis vom Inhalt von Postsendungen oder den näheren Umständen des Postverkehrs zu verschaffen"* (§ 39 Abs. 3 PostG).

Da das Rechtsinstitut des Verzichtes auf dem allgemeinen Rechtsgrundsatz *volenti non fit iniuria* (dem Einwilligenden geschieht kein Unrecht)[17] beruht, sind die diesen allgemeinen Rechtsgrundsatz tragenden Säulen des Verzichtsbewusstseins sowie der Freiwilligkeit des Verzichtes näher zu beleuchten. Denn nur eine Person, die freiwillig und bewusst in die Handlungen eines anderen einwilligt, ist in der Lage über das Rechtsgut, auf das verzichtet werden soll, wirksam zu disponieren.

Ratione personae wird demgegenüber in Rechtsprechung und Literatur die umstrittene Frage unterschiedlich beantwortet, ob der Verzicht nur eines der Kommunikationspartner, also des Absenders oder des Empfängers, ausreicht, um eine Verletzung des Postgeheimnisses auszuschließen, oder ob beide den Verzicht erklären müssen.

Stern geht im Beck'schen Kommentar zum PostG davon aus, dass die Erklärung entweder des Absenders oder des Empfängers genüge, um eine Verletzung des Postgeheimnisses auszuschließen.[18] Zur Begründung wird angeführt, dass die beiden Kommunikationspartner im Verhältnis zueinander keinen Anspruch auf Wahrung des Postgeheimnisses hätten.

Indes findet der einfachgesetzliche Schutz des Postgeheimnisses nach § 39 PostG in Art. 10 des Grundgesetzes seine verfassungsrechtliche Verankerung. Art. 10 des Grundgesetzes wird seit der überwiegenden Privatisierung des größten deutschen Postdienstleisters und seinem damit einhergehenden Ausschluss aus dem Kreis der unmittelbar Grundrechtsverpflichteten ein staatliches Schutzgebot entnommen. Daraus erwächst der gesetzgeberische Auftrag, die Anbieter von Postdienstleistungen einfachgesetzlich zur Einhaltung des Postgeheimnisses umfassend zu verpflichten.[19] § 39 PostG soll der amtlichen Begründung zufolge einen dem Art. 10 des Grundgesetzes entsprechenden Schutz auf einfachgesetzlicher Ebene gewährleisten,[20] sodass die Vorschrift auch den objektivrechtlichen Gehalt des Postgeheimnisses konkretisiert.[21] Angesichts dieser Einordnung sind Erkenntnisse aus der Rechtsprechung zu Art. 10 des Grundgesetzes auf § 39 PostG übertragbar.

In seiner Fangschaltungsentscheidung[22] führte das Bundesverfassungsgericht aus, dass entgegen der in der postrechtlichen Literatur vertretenen Ansicht ein Fernsprechteilnehmer gegenüber der (seinerzeitigen) Deutschen Bundespost nicht mit Wirkung für den anderen auf die Wahrung des nach Art. 10 des Grundgesetzes geschützten Fernmeldegeheimnisses verzichten könne. Zweck des Fernmeldegeheimnisses sei die Abschirmung von Kommunikationsvorgängen und -inhalten gegenüber staatlichen Eingriffen. Angesichts dieses Schutzziels sei jegliche staatliche Intervention, die nicht im Einverständnis mit sämtlichen Kommunikationspartnern erfolgt, als Grundrechtseingriff zu qualifizieren.[23]

Dass sich der Beschluss des Bundesverfassungsgerichts auf das Fernmeldegeheimnis bezieht, ist unerheblich. Die drei Einzelgewährleistungen des Art. 10 des Grundgesetzes (Post-, Brief- und Fernmeldegeheimnis) bezwecken den einheitlich geltenden umfassenden Schutz des durch Kommunikationsmittel ermöglichten Ferninformationsaustauschs. Angesichts der identischen Schutzrichtung ist auch eine einheitliche Handhabung angezeigt.[24] Dies gebietet die Übertragung von Maßstäben, die für eines der drei Grundrechte durch das Bundesverfassungsgericht entwickelt worden sind, auf die jeweils anderen Gewährleistungen.[25] Die in dem Bundesverfassungsgerichtsbeschluss getroffene Feststellung, der Verzicht auf das Fernmeldegeheimnis müsse kumulativ durch alle Kommunikationspartner erfolgen, ist damit auf das Postgeheimnis übertragbar.

Die Argumentation, dass der Verzicht eines der am Kommunikationsvorgang Beteiligten genüge, weil die Kommunikationspartner untereinander keinen Anspruch auf Wahrung des Postgeheimnisses hätten, überzeugt nicht. Die Ansicht verkennt, dass Art. 10 des Grundgesetzes und dementsprechend auch § 39 PostG die Vertraulichkeit des Übertragungsmediums vor externen Ein-

16 *Stern*, in: Beck'scher PostG-Kommentar, § 39 Rn. 13.

17 Zum allgemeinen Rechtsgrundsatz *volenti non fit iniuria* vgl. Kindler, in: Münchener Kommentar zum BGB, Teil 10 (Internationales Handels- und Gesellschaftsrecht), 7. Auflage 2018, Rn. 384 f.

18 *Stern*, in: Beck'scher PostG-Kommentar, § 39 Rn. 13 m. w. N.

19 *Lampe*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 222. EL Dezember 2018, PostG, § 39 Rn. 1.

20 BT-Drucks. 13/7774, S. 29.

21 *Stern*, in: Beck'scher PostG-Kommentar, § 39 Rn. 7 f.

22 BVerfG, Beschluss vom 25. März 1992 – 1 BvR 1430/88 –, BVerfGE 85, 386-405.

23 BVerfG, Beschluss v. 25.3.1992 – 1 BvR 1430/88 –, BVerfGE 85, 386 (399).

24 *Durner*, in: Maunz/Düring, Grundgesetz-Kommentar, Art. 10 Rn. 45.

25 *Durner*, in: Maunz/Düring, Grundgesetz-Kommentar, Art. 10 Rn. 48.

griffen schützt, nicht aber das Kommunikationsverhalten der beteiligten Partner untereinander adressiert.[26] Würde der einseitige Verzicht als ausreichend erachtet, bliebe die in einer Kommunikationsbeobachtung liegende Grundrechtsverletzung des *anderen* Gesprächspartners außer Betracht. Hierdurch würden Bedeutung und Tragweite von Art. 10 des Grundgesetzes verkürzt.[27] Der nach Art. 10 des Grundgesetzes gebotene Gewährleistungsgleichlauf gegenüber Anrufer und Angerufenen wie gegenüber Versender und Empfänger liefe ins Leere, wenn einer der Kommunikationspartner zu Lasten des anderen darüber entscheiden könnte, ob die Inhalte, Verbindungsdaten und sonstigen Umstände ihrer Kommunikation vertraulich bleiben.

Eine Verletzung des Postgeheimnisses entfällt damit erst, wenn sowohl Versender als auch Empfänger unmissverständlich auf den Schutz verzichten.

4 Zuordnung der Verarbeitungsprozesse

Bei isolierter Betrachtung der seitens des Postdienstleisters von den Versendern (Geschäftskunden) erhaltenen PDF-Dateien, welche Kopien von physischen Briefsendungen abbilden, ist festzustellen, dass die PDF-Dateien selbst nicht als Postsendungen und die elektronische Übermittlung von PDF-Dateien nicht als Beförderung von Postsendungen zu qualifizieren sind (vgl. § 4 Nr. 1 bis 3 PostG).

Demgegenüber könnten die seitens des Postdienstleisters beherrschten Verarbeitungsprozesse bis zur Zustellung der Digitalen Kopie in den elektronischen Briefkasten der Privatkunden (via E-POST-App und -Portal) – und zwar parallel im Produktionsprozess mit der Erfassung und Zustellung der physischen Briefsendung – sehr wohl in das Postgeheimnis eingreifen.

Ein Eingriff in das Postgeheimnis könnte insbesondere im Rahmen der Verarbeitung und Auswertung der PDF-Dateien erfolgen. Darüber hinaus wäre das Postgeheimnis verletzt, wenn der Postdienstleister dritten Dienstleistern, etwa Providern der elektronischen Kommunikationswege oder Dienstleistern, die mit der Auswertung der PDF-Dateien beauftragt sind, Informationen über die Inhalte der kopierten physischen Briefsendungen und/oder die näheren Umstände des die Briefsendungen betreffenden Postverkehrs preisgibt.

Dies setzt voraus, dass die eigenen Mitarbeiter des Postdienstleisters („sich verschaffen") bzw. seine dritten Dienstleister („anderen verschaffen") erkennen, dass die über eine asymmetrisch verschlüsselte Netzwerkverbindung vom digitalen Einlieferer (dem absendenden Geschäftskunden) auf die Server des Postdienstleisters übertragenen Datenpakete elektronisch erstellte Kopien der Inhalte und Verbindungsdaten physischer Postsendungen enthalten.

Hiervon ist bei lebensnaher Betrachtung der Verarbeitungsprozesse der Digitalen Kopien zunächst bei den eigenen Mitarbeitern des Postdienstleisters („sich verschaffen") *prima facie* auszugehen. Diese wissen offensichtlich, dass sie mit den Verarbeitungsprozessen der Digitalen Kopien befasst sind, welche in Bezug auf die elektronisch kopierten Inhalte sowie die nicht-inhaltsbezogenen Verbindungsdaten streng inhalts- und datenakzessorisch zu den parallel versandten physischen Briefsendungen hergestellt und zugestellt werden. Zumindest der Einblick von Mitarbeitern des Postdienstleisters in die geschützten Gegenstände des Postgeheimnisses ist den Verarbeitungsprozessen der Digitalen Kopie evident produktimmanent.

Aber auch eine Preisgabe (zumindest) der Verbindungsdaten der digital kopierten physischen Briefsendungen gegenüber den eingebundenen Drittdienstleistern (Providern der elektronischen Kommunikationswege und/oder mit den digitalen Verarbeitungsprozessen befassten Dienstleistern) liegt bei lebensnaher Betrachtung der Verarbeitungsprozesse der Digitalen Kopie *prima facie* nahe.

Auffällig ist, dass die – zwar den Datenschutz fokussierenden – umfassenden Anleitungen zur Digitalen Kopie[28] keinerlei den Schutz des Postgeheimnisses betreffende Vorkehrungen erwähnen. Während die Anleitungen zur Digitalen Kopie ausführliche Beschreibungen der Datenschutzvorkehrungen im Sinne der EU-DSGVO enthalten, etwa zur sicheren Übertragung der verschlüsselten Datenpakete der Geschäftskunden auf die Server des Postdienstleisters sowie zum durch ein Schlüsselpaar besonders gesicherten elektronischen Einlieferungsbereich,[29] fehlen jedwede Hinweise auf das Postgeheimnis betreffende Schutzvorkehrungen, um in die Verarbeitungsprozesse eingebundene Mitarbeiter sowie Drittdienstleister von einer verbotenen Kenntnisnahme im Sinne von § 39 Abs. 3 PostG abzuschirmen.

Angesichts der bisherigen Intransparenz der nach der Dateiübergabe im elektronischen Einlieferungsbereich von dem Postdienstleister beherrschten Verarbeitungsprozesse der Digitalen Kopien ist zumindest bis zum Antritt eines substantiierten Gegennachweises *prima facie*[30] von einer nach § 39 Abs. 3 PostG verbotenen Kenntnisnahme auszugehen, da die Parallelität der Briefsendungen mit den PDF-Dateien für die Digitale Kopie produktimmanent ist. Ohne solche, bisher offensichtlich nicht getroffenen wirksamen Abschirmungsmaßnahmen muss aufgrund der engen Inhalts-, Daten- und Verarbeitungsakzessorietät zwischen physischen Briefsendungen und Digitalen Kopien darauf geschlossen werden, dass die eigenen Mitarbeiter des Postdienstleisters bzw. seine Drittdienstleister sowohl erkennen, dass die vom absendenden Geschäftskunden auf die Server übertragenen Datenpakete elektronisch erstellte Kopien der Inhalte und Verbindungsdaten physischer Postsendungen enthalten, als auch hiervon entgegen dem Verbot nach § 39 Abs. 3 PostG Kenntnis nehmen.

5 Wirksamer Verzicht der Versender und Adressaten?

Aufgrund dieses Befundes eines möglichen Eingriffs in das Postgeheimnis stellt sich nun die Frage, ob sowohl die Versender als auch die Adressaten insoweit auf die Wahrung des Postgeheimnisses verzichten, also ob beide Seiten des Postverkehrs darin ein-

26 BVerfGE 131, 151 (189); *Guckelberger*, in: Schmidt-Bleibtreu/Hormann/Henneke, Grundgesetz-Kommentar, 14. Auflage 2017, Art. 10 Rn. 11.

27 BVerfG, Beschluss v. 25.3 1992 – 1 BvR 1430/88 –, BVerfGE 85, 386 (399).

28 Geschäftskundenleitfaden zur Digitalen Kopie.

29 Geschäftskundenleitfaden zur Digitalen Kopie, Kapitel 6 „Anleitungen".

30 Erschüttert wird der *prima facie*-Beweis (Anscheinsbeweis), indem der Beweisgegner die konkrete und ernsthafte Möglichkeit eines anderen als des erfahrungsgemäßen Geschehensablaufs darlegt und nachweist. Eine bloß abstrakte Möglichkeit eines anderen Geschehensablaufs vermag den *prima facie*-Beweis nicht zu erschüttern, da dieser gerade auf der erfahrungssatzmäßigen Typizität des mit ihm bewiesenen Geschehensablaufs konstitutiv beruht. Vgl. *Doukoff*, Grundlagen des Anscheinsbeweises, SVR 2015, S. 245 (252).

willigen, dass der Postdienstleister sich oder Dritten Kenntnis von den Inhalten der kopierten physischen Briefsendungen und/oder von den näheren Umständen des die Briefsendungen betreffenden Postverkehrs verschafft.

5.1 Verzicht der Versender?

Grundsätzlich könnte ein solcher Verzicht im Verhältnis der Versender zum Postdienstleister in den Verträgen über die Digitale Kopie erklärt sein. Allerdings setzt ein wirksamer Verzicht der Versender voraus, dass der Verzicht sich auf sämtliche Maßnahmen des Postdienstleisters erstreckt, die ohne wirksamen Verzicht zu einer Verletzung des Postgeheimnisses führen. Schon das erforderliche Verzichtsbewusstsein der Versender verlangt danach deren umfassende Aufklärung, insbesondere eine Offenlegung der wesentlichen – eine Kenntnisnahme im Sinne von § 39 Abs. 3 PostG ermöglichenden – Schritte in den Verarbeitungsprozessen und zwar von der Dateiübergabe im elektronischen Einlieferungsbereich bis zur Zustellung der Digitalen Kopien.

Die Anleitungen zur Digitalen Kopie[31] lassen jedenfalls weder die für einen wirksamen Verzicht gebotene Aufklärung noch eine Offenlegung der für das Postgeheimnis relevanten Verarbeitungsmaßnahmen erkennen. Ohne dass dem Verfasser die Verträge mit den Versendern bekannt sind, steht zu befürchten, dass auch diese Verträge bzw. ihre Anlagen bisher keine für einen wirksamen Verzicht gebotene Aufklärung und Offenlegung enthalten. Damit wären die einzelnen in das Postgeheimnis eingreifenden Verarbeitungsmaßnahmen einem rechtfertigenden Verzicht gar nicht zugänglich. Diese Verarbeitungsmaßnahmen verletzen dann das Postgeheimnis schon auf Seite des Versenders.

5.2 Verzicht der Adressaten?

Auf der Adressatenseite ist kein Einverständnis mit der Offenbarung von Inhalten oder vom Postgeheimnis geschützten näheren Umständen des Postverkehrs erkennbar, zumal regelmäßig keine Postbeförderungsverträge zwischen dem Postdienstleister und den Adressaten geschlossen werden.

Ein Einverständnis der Adressaten könnte zwar grundsätzlich auch in Verträgen zwischen den Versendern und den Adressaten vereinbart werden.

Da auch ein wirksamer Verzicht der Adressaten deren belastbares Verzichtsbewusstsein und damit eine umfassende Aufklärung aufgrund der Offenlegung der wesentlichen – eine Kenntnisnahme im Sinne von § 39 Abs. 3 PostG ermöglichenden – Verarbeitungsschritte der Digitalen Kopien voraussetzt, sind überhaupt keine Anhaltspunkte für eine Einwilligung in Eingriffe in das Postgeheimnis auf der Adressatenseite erkennbar.

Die in der Literatur angesprochene Möglichkeit einer mutmaßlichen Einwilligung in Eingriffe in das Postgeheimnis *„innerhalb enger Grenzen"*[32] dürfte praktisch ausgeschlossen sein. Denn einem mutmaßlich konkludierten Verzicht der Adressaten auf ihr

31 Geschäftskundenleitfaden zur Digitalen Kopie.

32 *Stern*, in: Beck'scher PostG-Kommentar, § 39 Rn. 13.

Postgeheimnis wird gerade das erforderliche – nur bei entsprechender Aufklärung und Offenlegung belastbare –Verzichtsbewusstsein fehlen. Auch hier zeigt sich die Nähe des Postgeheimnisses zum Schutz personenbezogener Daten aufgrund des allgemeinen Persönlichkeitsrechts nach Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 des Grundgesetzes, welches – umgesetzt in den Datenschutzgesetzen und -verordnungen – nur bewusste (explizite) Einwilligungen in die private Verarbeitung personenbezogener Daten zulässt.

6 Anordnungen der Bundesnetzagentur

Angesichts der intransparenten Verarbeitungsprozesse der Digitalen Kopie nach der Dateiübergabe im elektronischen Einlieferungsbereich und der Übertragung der Datenpakete auf die Server des Postdienstleisters liegt ein Sachverhalt vor, der prima facie eine nach § 39 Abs. 3 PostG verbotene Kenntnisnahme zumindest nahelegt. Aufgrund der engen Inhalts-, Daten- und Verarbeitungsakzessorietät zwischen physischen Briefsendungen und Digitalen Kopien kann darauf geschlossen werden, dass die eigenen Mitarbeiter des Postdienstleisters bzw. seine Drittdienstleister sowohl erkennen, dass die vom absendenden Geschäftskunden auf die Server übertragenen Datenpakete elektronisch erstellte Kopien der Inhalte und Verbindungsdaten physischer Postsendungen enthalten, als auch hiervon entgegen dem Verbot nach § 39 Abs. 3 PostG Kenntnis nehmen.

Aufgrund dieses Sachverhaltes ist die Bundesnetzagentur nach § 42 Abs. 1 PostG gehalten, im Wege der gebotenen Amtsermittlung die erforderlichen Auskünfte von dem nach § 39 PostG verpflichteten Postdienstleister einzufordern und dessen Betriebseinrichtungen ggf. zu überprüfen. Denn es bestehen prima facie Anhaltspunkte, dass der Postdienstleister auf seiner Produktplattform für die Digitale Kopie einen dem Art. 10 des Grundgesetzes entsprechenden Gewährleistungsstandard des Postgeheimnisses nach § 39 PostG nicht ausreichend sicherstellt. Damit ist die Bundesnetzagentur gerade aufgrund der staatlichen Schutzpflichten aus Art. 10 des Grundgesetzes (objektive Grundrechtswirkung) gegenüber diesen privatwirtschaftlich verursachten Gefährdungslagen verpflichtet, die Einhaltung der Pflichten zur Wahrung des Postgeheimnisses im Wege von geeigneten Anordnungen nach § 42 Abs. 1 und 2 PostG sicherzustellen.

Nach § 42 Abs. 1 PostG kann die Bundesnetzagentur zunächst im Wege der gebotenen Amtsermittlung die erforderlichen Auskünfte von dem nach § 39 PostG Verpflichteten einfordern und dessen technische Betriebseinrichtungen und Geschäftsräume überprüfen. Da belastbare prima facie Anhaltspunkte vorliegen, dass auf der Produktplattform für die Digitale Kopie kein ausreichender Gewährleistungsstandard des Postgeheimnisses nach § 39 PostG sichergestellt ist, wird zumindest das Aufgreifermessen der Bundesnetzagentur in Richtung einer hier ausnahmsweise zwingend gebotenen Amtsermittlung nach § 42 Abs. 1 PostG aufgrund der staatlichen Schutzpflichten aus Art. 10 des Grundgesetzes auf Null reduziert.[33]

Sollten die Ermittlungen der Bundesnetzagentur eine Verletzung des Postgeheimnisses auf der Produktplattform für die Digitale Kopie ergeben, stellt sie nach § 42 Abs. 2 PostG fest, dass auf dieser Produktplattform die Pflichten zur Wahrung des Postgeheimnisses gemäß § 39 PostG nicht eingehalten werden, und kann geeignete Anordnungen zur Beendigung der Verstöße erlassen.

Das von der Bundesnetzagentur verhältnismäßig auszuübende Auswahlermessen erlaubt nach § 42 Abs. 2 PostG Anordnungen, die das weitere geschäftsmäßige Erbringen von Postdiensten ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen. Verhältnismäßige ultima ratio wäre hier eine Suspendierungsanordnung, den Betrieb der Produktplattform für die Digitale Kopie solange einstweilen einzustellen, bis der Postdienstleister wirksame Abschirmungsmaßnahmen umsetzt, die sicherstellen, dass weder seine eigenen Mitarbeiter noch Drittdienstleister Kenntnis von den (aus den parallelen physischen Postsendungen) elektronisch kopierten Inhalten und Verbindungsdaten nehmen (können).

7 Fazit

1. Prima facie bestehen belastbare Anhaltspunkte, dass auf der Produktplattform für die Digitale Kopie ein dem Art. 10 des Grundgesetzes entsprechender Gewährleistungsstandard des Postgeheimnisses nach § 39 PostG nicht ausreichend sicherstellt wird.
2. Aufgrund dieses Befundes wird zumindest das Aufgreifermessen der Bundesnetzagentur in Richtung einer hier ausnahmsweise zwingend gebotenen Amtsermittlung nach § 42 Abs. 1 PostG nach Maßgabe der staatlichen Schutzpflichten aus Art. 10 des Grundgesetzes auf Null reduziert.
3. Sollten die Ermittlungen der Bundesnetzagentur eine Verletzung des Postgeheimnisses auf dieser Produktplattform ergeben, könnte sie nach § 42 Abs. 2 PostG insbesondere anordnen, den Betrieb der Produktplattform solange einstweilen einzustellen, bis wirksame Abschirmungsmaßnahmen zum Schutz des Postgeheimnisses umgesetzt wurden.

33 Zur Ermessensreduzierung auf Null vgl. *Wolff*, in: Sodan/Ziekow, Verwaltungsgerichtsordnung, 5. Auflage 2018, § 114 Rn. 129 ff.; Rennert, in: Eyermann, Verwaltungsgerichtsordnung, 15. Auflage 2019, § 114 Rn. 32.