HRRS-Nummer: HRRS 2019 Nr. 89
Bearbeiter: Holger Mann
Zitiervorschlag: HRRS 2019 Nr. 89, Rn. X

BVerfG 2 BvR 2377/16 (3. Kammer des Zweiten Senats) - Beschluss vom 20. Dezember 2018 (LG Stuttgart / AG Stuttgart)

Verpflichtung des Anbieters eines E-Mail-Dienstes zur Übermittlung von IP-Adressen (strafprozessuale Telekommunikationsüberwachung; Herausgabe der Inhalts- und Verkehrsdaten eines E-Mail-Accounts; Grundrecht der Berufsfreiheit des Dienstanbieters; Berufsausübungsfreiheit; verfassungsgemäße Einschränkung durch die gesetzlichen Mitwirkungs- und Vorhaltungsvorschriften für Telekommunikationsdienstanbieter; weiter Telekommunikationsbegriff; Bereitstellung der anfallenden IP-Adressen; „Vorhandensein" der externen IP-Adressen bei Verwendung eines NAT-Verfahrens; Erfordernis einer funktionstüchtigen Strafrechtspflege; erleichterte Zugriffsmöglichkeit auf Verkehrsdaten; Verhängung eines Ordnungsgeldes; präventive und repressive Funktion von Ordnungsmitteln).

Art. 10 GG; Art. 12 Abs. 1 Satz 2 GG; Art. 20 Abs. 3 GG; § 70 Abs. 1 StPO; § 95 Abs. 2 StPO; § 100a StPO; § 100b Abs. 3 Satz 1 StPO a. F.; § 100g Abs. 1 StPO; § 3 TKG; § 110 Abs. 1 Satz 1 Nr. 1 TKG; § 3 TKÜV; § 5 TKÜV; § 6 Abs. 1 TKÜV; § 7 Abs. 1 TKÜV

Leitsätze des Bearbeiters

1. Der Anbieter eines E-Mail-Dienstes ist verpflichtet, den Ermittlungsbehörden im Rahmen einer strafprozessualen Telekommunikationsüberwachung die IP-Adressen der auf ihren Account zugreifenden Kunden auch dann zu übermitteln, wenn er seinen Dienst aus Datenschutzgründen so organisiert hat, dass er diese nicht protokolliert (Hauptsacheentscheidung zur Ablehnung einer einstweiligen Anordnung vom 12. Dezember 2016 [= HRRS 2017 Nr. 133]).

2. Die Festsetzung eines Ordnungsgeldes gegen den Anbieter eines E-Mail-Dienstes, der sein internes Netzwerk mittels eines sogenannten NAT-Verfahrens (Network Adress Translation) vom Internet abtrennt und deshalb den Ermittlungsbehörden die - von ihm nicht geloggten - IP-Adressen der E-Mail-Nutzer nicht herausgibt, greift in die Berufsausübungsfreiheit des Anbieters ein, weil sie diesem technische und organisatorische Vorgaben für die Einrichtung seines Betriebes macht.

3. Eingriffe in die Berufsfreiheit sind nur auf der Grundlage einer gesetzlichen Regelung zulässig, die Umfang und Grenzen des Eingriffs erkennen lässt und mit welcher der Gesetzgeber - soweit möglich - alle wesentlichen Entscheidungen selbst trifft.

4. Nach den gesetzlichen Mitwirkungs- und Vorhaltungsvorschriften sind Telekommunikationsdienstanbieter verpflichtet, ihren Betrieb so zu gestalten, dass sie die im Rahmen einer rechtmäßig angeordneten Überwachung der Telekommunikation bei ihnen anfallenden IP-Adressen bereitstellen können.

5. Der Begriff der Telekommunikation im Sinne des § 100a StPO ist - orientiert am Schutzbereich des Art. 10 GG - weit auszulegen und umfasst nicht nur Kommunikationsinhalte, sondern auch die näheren Umstande der Telekommunikation. Zu den hiervon betroffenen Verkehrsdaten gehören auch und gerade die anfallenden (dynamischen oder statischen) IP-Adressen, mit denen die Kunden eines E-Mail-Dienstes mit ihren internetfähigen Endgeräten auf ihren E-Mail-Account zugreifen.

6. Diese externen IP-Adressen sind auch bei Verwendung eines NAT-Verfahrens zumindest für die Dauer der Verbindung bei dem Anbieter gespeichert und müssen daher von diesem auf Anforderung herausgegeben werden; denn die gesetzliche Verpflichtung zur Bereitstellung erstreckt sich auf alle Telekommunikationsdaten, die über die Anlage des Anbieters abgewickelt werden und die bei ihm - wenngleich möglicherweise nur vorübergehend - vorhanden sind. Der im Jahre 2017 neu eingefügten Regelung in § 7 Abs. 1 Satz 1 Nr. 9 TKÜV kommt insoweit eine rein klarstellende Funktion zu.

7. Wenngleich das Geschäftsmodell eines E-Mail-Anbieters, die IP-Adressen seiner Kunden aus Datenschutzgründen nicht zu protokollieren, unter dem Gesichtspunkt der Berufsfreiheit durchaus schützenswert erscheint, entbindet ihn dies nicht von der Einhaltung der gesetzlichen Vorgaben, die dem verfassungsrechtlichen Erfordernis einer funktionstüchtigen Strafrechtspflege Rechnung tragen. Dies gilt auch dann, wenn eine Systemumstellung ihm einen nicht unerheblichen technischen und finanziellen Aufwand abverlangt.

8. Die Vorschrift des § 100g Abs. 1 StPO schafft lediglich eine erleichterte Zugriffsmöglichkeit auf Verkehrsdaten und schränkt den Anwendungsbereich des § 100a StPO bei der (Echtzeit-)Überwachung künftiger Telekommunikation nicht ein.

9. Strafprozessualen Ordnungsmitteln kommt sowohl eine präventive als auch eine repressive Funktion zu. Der Verhängung eines Ordnungsgeldes gegen den Anbieter eines E-Mail-Dienstes steht daher nicht entgegen, dass dieser nach der von ihm gewählten Gestaltung seines Dienstes seine strafprozessualen Mitwirkungspflichten erst nach einem Umbau seines EDV-Systems erfüllen kann, bei dessen Abschluss die konkrete Überwachungsmaßnahme bereits überholt wäre.

Entscheidungstenor

Die Verfassungsbeschwerde wird nicht zur Entscheidung angenommen.

Gründe

I.

Die Verfassungsbeschwerde betrifft die Frage, ob der Anbieter eines E-Mail-Dienstes im Rahmen einer ordnungsgemäß angeordneten Telekommunikationsüberwachung verpflichtet ist, den Ermittlungsbehörden die Internetprotokolladressen (im Folgenden: IP-Adressen) der auf ihren Account zugreifenden Kunden auch dann zu übermitteln, wenn er seinen Dienst aus Datenschutzgründen so organisiert hat, dass er diese nicht protokolliert. 1

1. Der Beschwerdeführer betreibt seit 2009 als eingetragener Kaufmann den E-Mail-Dienst „XX…“. Der Dienst wirbt mit einem besonders effektiven Schutz der Kundendaten und sieht sich den Grundsätzen der Datensicherheit und der Datensparsamkeit verpflichtet. Er erhebt und speichert Daten nur dann, wenn dies aus technischen Gründen erforderlich oder - aus seiner Sicht - gesetzlich vorgesehen ist. 2

2. Die Staatsanwaltschaft Stuttgart führte ein Ermittlungsverfahren gegen den Nutzer des E-Mail-Accounts r…, von dem nur ein „Nickname“ bekannt war, wegen des Verdachts des unerlaubten Handeltreibens mit Betäubungsmitteln in nicht geringer Menge sowie eines Verstoßes gegen das Kriegswaffenkontrollgesetz. 3

3. Mit Beschluss vom 25. Juli 2016 ordnete das Amtsgericht Stuttgart auf Antrag der Staatsanwaltschaft gemäß §§ 100a, 100b StPO in der Fassung vor Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I S. 3202) die Sicherung, Spiegelung und Herausgabe aller Daten, die auf den Servern von „XX…“ bezüglich des betreffenden E-Mail-Accounts elektronisch gespeichert sind, „sowie sämtlicher bezüglich dieses Accounts künftig anfallender Daten (Inhalts- und Verkehrsdaten nebst IP-Adressen, insbesondere auch bei den zukünftigen Login-Vorgängen anfallender IP-Adressen)“ an. Die zunächst bis zum 24. September 2016 befristete Maßnahme wurde durch Beschluss des Amtsgerichts vom 19. September 2016 bis zum 24. November 2016 verlängert. 4

4. Am 28. Juli 2016 gab das Landeskriminalamt Baden-Württemberg dem Beschwerdeführer die angeordnete Überwachungsmaßnahme sowie den zu überwachenden Account bekannt. Noch am selben Tag richtete der Beschwerdeführer die Telekommunikationsüberwachung ein und unterrichtete das Landeskriminalamt hierüber. Der Beschwerdeführer wies jedoch darauf hin, dass Verkehrsdaten der Nutzer nicht „geloggt“ würden und solche Daten inklusive der IP-Adressen deshalb nicht zur Verfügung gestellt werden könnten. 5

Mit Schreiben vom 29. Juli 2016 wies die Staatsanwaltschaft den Beschwerdeführer darauf hin, dass er gesetzlich verpflichtet sei, für die Dauer der Überwachungsmaßnahme die Verkehrsdaten und insbesondere die IP-Adressen zu dem betreffenden Account zu „loggen“. Dem widersprach der nunmehr anwaltlich vertretene Beschwerdeführer mit Schriftsatz vom selben Tag. Die fraglichen IPAdressen würden von „XX…“ nicht erhoben und seien auch nicht vorhanden. Eine Pflicht, technische Vorkehrungen zur Erhebung von Daten zu treffen, die allein für Überwachungszwecke benötigt würden und während des üblichen Geschäftsbetriebes nicht anfielen, bestünde nicht. 6

Daraufhin drohte die Staatsanwaltschaft dem Beschwerdeführer mit Schreiben vom 1. August 2016 an, die Verhängung von Ordnungsmitteln zu beantragen. Die Ausführungen des Beschwerdeführers könnten allenfalls für die Vergangenheit gelten. Sie gingen jedoch für die Telekommunikationsüberwachung in Echtzeit fehl. Die Verpflichtung zur Mitwirkung an der Telekommunikationsüberwachung ergebe sich aus § 100b Abs. 3 Satz 1 StPO a.F. und werde durch § 110 des Telekommunikationsgesetzes (im Folgenden: TKG), die Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (im Folgenden: TKÜV) und die Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (im Folgenden: TR TKÜV) konkretisiert. Nach § 5 Abs. 1 und 2 TKÜV habe der Verpflichtete der berechtigten Stelle eine vollständige Kopie der Telekommunikation bereitzustellen, die über seine Anlage abgewickelt werde, einschließlich der 7

Daten über die näheren Umstände der Telekommunikation. Auch aus der TR TKÜV ergebe sich, dass die IP-Adressen als Teil der zugehörigen Ereignisdaten zusammen mit der vollständigen Kopie der zu überwachenden E-Mail übermittelt werden müssten. Dass die entsprechenden IP-Adressen zum Zeitpunkt des Abrufs oder Einstellens einer E-Mail oder eines sonstigen Zugriffs auf das Konto im Sinne von § 7 Abs. 1 Nr. 4 TKÜV vorhanden seien, sei unstreitig.

Der Annahme, die IP-Adressen seien „bei XX…“ vorhanden, widersprach der Beschwerdeführer mit Schriftsatz vom 2. August 2016 unter Darstellung seiner Systemstruktur. „XX…“ trenne sein internes Netz über ein sogenanntes NAT-Verfahren (Network Adress Translation), bei dem die Adressinformationen in Datenpaketen automatisiert durch andere ersetzt würden, aus Sicherheitsgründen strikt vom Internet ab. Die IP-Adressen der Kunden würden daher bereits an den Außengrenzen des Systems verworfen und seien dem Zugriff des Beschwerdeführers entzogen. Ebenfalls am 2. August 2016 hinterlegte der Beschwerdeführer beim Amtsgericht eine Schutzschrift, in der er mit im Wesentlichen gleichlautender Begründung einem Antrag auf Verhängung eines der in § 70 Abs. 1 StPO genannten Ordnungsmittel entgegen trat. 8

5. Mit angegriffenem Beschluss vom 9. August 2016 setze das Amtsgericht Stuttgart ein Ordnungsgeld in Höhe von 500 Euro, ersatzweise sieben Tage Ordnungshaft, gegen den Beschwerdeführer fest. Aufgrund des Beschlusses vom 25. Juli 2016 sei der Beschwerdeführer verpflichtet, zukünftig die Verkehrsdaten und insbesondere die IP-Adressen zu erheben. Seine Rechtsausführungen zur retrograden Erhebung von Verbindungsdaten gingen fehl. Der Beschwerdeführer sei aufgrund der gesetzlichen Vorgaben verpflichtet, seine technischen Einrichtungen so zu gestalten, dass die Erhebung der Daten gewährleistet sei. Insbesondere aufgrund der erheblichen Bedeutung des zugrundeliegenden Ermittlungsverfahrens erscheine die Höhe des Ordnungsgeldes und der hilfsweise festgesetzten Ordnungshaft sehr moderat. 9

6. Mit Schriftsatz vom 15. August 2016 legte der Beschwerdeführer Beschwerde gegen den Beschluss vom 9. August 2016 ein. Er machte im Wesentlichen geltend, dass sich das Amtsgericht nicht ausreichend mit seinen Argumenten auseinandergesetzt habe. Nach Übersendung der Antragsschrift der Staatsanwaltschaft, die ihm zuvor nicht zugeleitet worden war, begründete der Beschwerdeführer seine Beschwerde mit Schriftsatz vom 26. August 2016 ergänzend. Es komme für die rechtliche Bewertung allein auf § 100g StPO an, da diese Vorschrift sowohl für bereits angefallene als auch für zukünftig anfallende Verkehrsdaten gegenüber § 100a StPO lex specialis sei. Die IP-Adressen fielen hier indes nicht unter den Begriff der Verkehrsdaten, da sie von „XX…“ nicht erhoben, verarbeitet oder genutzt würden. Die Infrastrukturpflicht aus § 110 TKG normiere ebenfalls keine Rechtsgrundlage für die Datenerhebung. Letztlich sei der Ordnungsgeldbeschluss auch deshalb rechtswidrig, weil er den Beschwerdeführer zu etwas zwingen wolle, was dieser nicht erfüllen könne. Der Beschwerdeführer habe die verlangten Daten nicht und könne sie auch nicht kurzfristig, sondern nur durch eine aufwändige Neustrukturierung seines EDV-Systems erfassen. Etwaige Infrastrukturpflichten könnten aber nicht mithilfe eines Zwangsmittels der Strafprozessordnung durchgesetzt werden. 10

7. Das Landgericht Stuttgart verwarf die Beschwerde mit Beschluss vom 1. September 2016 als unbegründet. Das Gericht teile die Auffassung der Staatsanwaltschaft. Allein der Einsatz der NAT-Technologie entbinde den Beschwerdeführer nicht von der Verpflichtung, eine vollständige Kopie der Telekommunikation inklusive der IP-Adressen zu übergeben. Die Verpflichtung ergebe sich aus § 100b Abs. 3 Satz 2 StPO a.F., § 110 TKG sowie aus §§ 3, 5 und 7 TKÜV „mit den dazu ergangenen Richtlinien“. Die zu überwachende Telekommunikation bestehe nach § 5 TKÜV aus dem Inhalt und den Daten über die näheren Umstände der Telekommunikation. Insoweit sei der Beschwerdeführer verpflichtet, der berechtigten Stelle eine vollständige Kopie der Telekommunikation bereit zu stellen. Aufgrund des Beschlusses vom 25. Juli 2016 sei der Beschwerdeführer dazu verpflichtet, gegebenenfalls die technischen Voraussetzungen zur Erfüllung seiner Mitwirkungspflicht zu schaffen und die IP-Adressen möglichst vollständig zur Auswertung zu übergeben. 11

8. Mit Schriftsatz vom 11. Oktober 2016 erhob der Beschwerdeführer „gemäß § 33a StPO Gegenvorstellung“ gegen den Beschluss vom 1. September 2016. Der Beschluss setze sich mit wesentlichem rechtlichen und tatsächlichen Vorbringen des Beschwerdeführers nicht auseinander und verletze dadurch den Anspruch auf rechtliches Gehör. Zudem verkenne das Landgericht den Aufwand und die zu erwartenden Folgen einer Schaffung der technischen Voraussetzungen zur Erhebung der IP-Adressen der Kunden des Beschwerdeführers. Auf Grundlage eines nach Bekanntgabe der Beschwerdeentscheidung eingeholten Kostenvoranschlags sei bei einer Projektlaufzeit von zwölf Monaten und bei zurückhaltender Berechnung von einem Kostenvolumen von mindestens 80.000 Euro auszugehen. 12

9. Das Landgericht legte den Schriftsatz als Gehörsrüge aus und wies diese mit Beschluss vom 28. Oktober 2016 zurück. Die Beschwerdekammer habe das ausführliche Vorbringen des Beschwerdeführers ihrer Entscheidung zugrunde gelegt. Damit scheide eine Anwendung des § 33a StPO aus, da im Rahmen einer Gehörsrüge nicht geltend gemacht werden könne, dass die Entscheidung inhaltlich falsch sei. 13

10. Am 18. November 2016 teilte das Landeskriminalamt dem Beschwerdeführer mit, dass die Überwachung des Anschlusses abgeschaltet werden könne. Das Ordnungsgeld wurde am 2. Januar 2017 bezahlt. 14

II.

Mit seiner Verfassungsbeschwerde wendet sich der Beschwerdeführer gegen den das Ordnungsgeld festsetzenden Beschluss des Amtsgerichts vom 9. August 2016 und die Beschwerdeentscheidung des Landgerichts vom 1. September 2016. Er rügt eine Verletzung seiner Berufsausübungsfreiheit (Art. 12 Abs. 1 Satz 2 GG) sowie seiner Grundrechte aus Art. 2 Abs. 1 GG (i.V.m. Art. 20 Abs. 3 GG), Art. 2 Abs. 2 Satz 2 GG und Art. 14 GG. 15

Der Eingriff in den Schutzbereich dieser Grundrechte sei nicht gerechtfertigt, weil es an einer einfachgesetzlichen Grundlage fehle. Mit der Verhängung des Ordnungsgeldes und der Androhung von Ordnungshaft solle etwas erzwungen werden, zu dem der Beschwerdeführer aus tatsächlichen Gründen nicht in der Lage (1.) und rechtlich nicht verpflichtet sei (2.). Im Übrigen sei die Festsetzung von Ordnungsgeld unverhältnismäßig (3.). 16

1. Aufgrund des verwendeten NAT-Systems verfüge der Beschwerdeführer nicht über die Daten, zu deren Herausgabe er gezwungen werden solle. Im gesamten Zugriffsbereich von „XX…“ lägen weder intern noch an den Außengrenzen IP-Adressen mit Nutzerbezug vor. Im Grenzbereich zwischen dem Internet und den abgesicherten „XX…“-Systemen träfen zahlreiche verschlüsselte und an die allgemeine IP-Adresse des Unternehmens gerichtete Zugriffsanfragen ein. Die Information, auf welches Postfach konkret zugegriffen werden solle, befinde sich innerhalb der verschlüsselten Zugriffsverbindung und könne von allen Komponenten im Grenz-/Übergangsbereich nicht aufgeschlossen werden. Nach Ausführung der gewünschten Aktion würden die Datenpakete wieder verschlüsselt und über dieselbe Verbindung wieder auf den Rückweg geschickt. An der Außengrenze des „XX…“-Systems werde die ursprüngliche Verbindung mit der öffentlichen IP-Adresse festgestellt und das verschlüsselte Datenpaket dem Kunden via Internet zugestellt. Der beschriebene Weiterleitungs- und Umwandlungsmechanismus sei weder dazu konzipiert noch in der Lage, die ihn durchlaufenden Inhalte zu filtern oder auszuwerten. „XX…“ müsste dafür seine Außengrenze zum Internet komplett neu konzipieren. 17

2. Eine Verpflichtung, die IP-Adressen an die Strafverfolgungsbehörden auszuleiten, bestehe nicht. 18

§ 100g StPO als allein einschlägige Norm erlaube den Strafverfolgungsbehörden unter bestimmten Voraussetzungen die Erhebung von Verkehrsdaten, so dass ein Rückgriff auf § 100a StPO nicht mehr erforderlich, aber auch nicht mehr zulässig sei. Bei den in Rede stehenden Daten handle es sich aber nicht um Verkehrsdaten im Sinne des § 100g StPO, da der Beschwerdeführer sie nicht erhebe und, da er sie für eigene Zwecke nicht benötige, nach § 96 TKG auch nicht erheben dürfe. Weder aus § 100g noch aus § 100b StPO a.F. könne daher eine Pflicht des Beschwerdeführers abgeleitet werden, die fraglichen IP-Adressen auszuleiten. 19

Dies gelte selbst dann, wenn der Gesetzgeber eine entsprechende Verpflichtung mit der Neuregelung des § 100g Abs. 1 StPO im Jahre 2007 hätte normieren wollen. Denn angesichts des entgegenstehenden Wortlauts der Norm würde es jedenfalls an einer normenklaren einfachrechtlichen Eingriffsgrundlage fehlen. Im Übrigen habe der Gesetzgeber ohnehin nur eine Echtzeitüberwachung der Verkehrsdaten nach dem Vorbild des § 100a StPO ermöglichen, nicht aber ein „Mehr“ an Datenerhebung durch die Telekommunikationsanbieter erreichen wollen. Dass der Gesetzgeber mit § 100g Abs. 1 StPO keine Pflicht des Telekommunikationsanbieters normieren wollte, Daten nur für Strafverfolgungszwecke zu erheben und zu speichern, ergebe sich schließlich auch aus der Gesetzesbegründung zu der im Jahre 2015 eingeführten modifizierten Form der Vorratsdatenspeicherung. Im Übrigen wäre eine Datenerhebungspflicht - dem sogenannten „Doppeltürenmodell“ des Bundesverfassungsgerichts folgend - gesondert und nicht in der Strafprozessordnung, sondern im Telekommunikationsgesetz zu regeln. 20

3. Die Festsetzung des Ordnungsgeldes sei nicht geeignet, um den damit verfolgten Zweck - die Ausleitung der IP-Adressen - zu erreichen. Der Beschwerdeführer könne die IP-Adressen nicht ausleiten. Der erforderliche Umbau des EDV-Systems würde etwa zwölf Monate dauern. Zu diesem Zeitpunkt sei die konkrete Überwachungsmaßnahme bereits abgelaufen. Der Beschluss sei aber auch unangemessen, weil der Umbau lange dauern, unverhältnismäßig hohe Kosten verursachen und die Sicherheitsstandards reduzieren würde. 21

III.

1. Zur Verfassungsbeschwerde haben der Generalbundesanwalt beim Bundesgerichtshof, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, das Bundesamt für Sicherheit in der Informationstechnik sowie die Bundesnetzagentur Stellung genommen. 22

a) Der Generalbundesanwalt beim Bundesgerichtshof hält die Verfassungsbeschwerde für nicht erfolgversprechend. 23

Die Verpflichtung zur Ausleitung der IP-Adressen bei laufender Telekommunikationsüberwachung finde ihre rechtliche Grundlage nicht in § 100g Abs. 1 StPO, sondern in § 100a Abs. 1 StPO. Die vom Beschwerdeführer vertretene gegenteilige Auffassung finde im Gesetz keine Stütze. Anders als bei § 100g StPO seien Maßnahmen nach § 100a 24

StPO nicht auf bestimmte Datengruppen (Verkehrsdaten, Inhaltsdaten) beschränkt, sondern erfassten die gesamte „Telekommunikation“. § 110 TKG verpflichte den Diensteanbieter, technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten, wobei die Anforderungen durch die TKÜV konkretisiert würden. Die „andere Adressierungsangabe“ im Sinne des § 7 Abs. 1 Satz 1 Nr. 4 TKÜV stelle bei E-Mail-Diensten, wie sie der Beschwerdeführer anbiete, die IP-Adresse dar, die dem internetfähigen Endgerät, mit der der Kunde auf sein Postfach zugreifen wolle, zugewiesen sei. Dementsprechend sehe die TR TKÜV die Übermittlung der IP-Adresse ausdrücklich vor.

Diese IP-Adresse sei bei dem Beschwerdeführer auch im Sinne von § 7 Abs. 1 Satz 1 Nr. 4 TKÜV vorhanden. Dass der Beschwerdeführer sie nicht für eigene Zwecke speichere, stehe dem nicht entgegen, denn für seine Dienstleistung sei er auf diese angewiesen und nutze sie. Ohne ihre Verarbeitung sei es dem Beschwerdeführer nicht möglich, die unter einer bestimmten E-Mail-Adresse abgewickelte Kommunikation dem richtigen Endgerät und damit dem Kunden zuzuordnen. 25

Die angegriffenen Ordnungsgeldbeschlüsse seien auf Grundlage rechtmäßiger Grundanordnungen zur Telekommunikationsüberwachung formell und materiell rechtmäßig ergangen. Die Festsetzung des moderat bemessenen Ordnungsgeldes sei auch nicht unverhältnismäßig. Dass der Beschwerdeführer eine Infrastruktur implementiert habe, die ihm derzeit die Ausleitung der verlangten Daten unmöglich mache, weil er sich selbst für sie gleichsam blind gemacht habe, entbinde ihn nicht von der gemäß § 100b Abs. 3 Satz 3 StPO a.F. in Verbindung mit § 95 Abs. 2 StPO mit Ordnungs- und Zwangsmitteln belegten Pflicht zur Ausleitung. 26

b) Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit äußerte mit Blick auf die „Überwachungs-Gesamtrechnung“ Bedenken, soweit Telekommunikationsanbieter verpflichtet werden sollten, ihre Datenverarbeitungsprozesse über das nach dem TKG erforderliche Maß hinaus umzugestalten. 27

c) Das Bundesamt für Sicherheit in der Informationstechnik äußerte sich zu den technischen Gegebenheiten des vom Beschwerdeführer verwendeten NAT-Systems. 28

d) Die Bundesnetzagentur äußerte die Auffassung, dass dem Beschwerdeführer die Ausleitung der IP-Adressen seiner Kunden tatsächlich und rechtlich möglich sei und seinerseits die Verpflichtung zu einer entsprechenden Umstrukturierung seiner Infrastruktur bestehe. 29

2. Der Beschwerdeführer hat auf die Stellungnahmen erwidert und dabei sein bisheriges Vorbringen wiederholt und vertieft. 30

3. Die Akten des Ausgangsverfahrens haben der Kammer vorgelegen. 31

IV.

Den zusammen mit der Verfassungsbeschwerde gestellten Antrag auf Erlass einer einstweiligen Anordnung hat die Kammer mit Beschluss vom 12. Dezember 2016 abgelehnt. 32

V.

Die Verfassungsbeschwerde wird nicht zur Entscheidung angenommen. Annahmegründe im Sinne des § 93a Abs. 2 BVerfGG liegen nicht vor, denn die Verfassungsbeschwerde ist zum Teil bereits unzulässig, im Übrigen jedenfalls unbegründet. 33

1. Soweit sich die Verfassungsbeschwerde gegen die Ausgangsentscheidung des Amtsgerichts vom 9. August 2016 richtet, ist sie unzulässig. Das Landgericht hatte als Beschwerdegericht eine eigene umfassende Sachprüfung vorzunehmen (vgl. § 308 Abs. 2, § 309 Abs. 2 StPO) und hat dies auch getan. Seine Entscheidung tritt daher an die Stelle der Entscheidung des Amtsgerichts; diese ist prozessual überholt (vgl. BVerfG, Beschlüsse der 3. Kammer des Zweiten Senats vom 17. April 2015 - 2 BvR 1986/14 -, juris, Rn. 10 und vom 8. November 2017 - 2 BvR 2129/16 -, juris, Rn. 11, beide m.w.N.). 34

2. Soweit sich die Verfassungsbeschwerde gegen die Beschwerdeentscheidung richtet, ist sie jedenfalls unbegründet. Zwar greift die Festsetzung des Ordnungsgeldes in die durch Art. 12 Abs. 1 Satz 2 GG geschützte Freiheit der Berufsausübung des Beschwerdeführers ein (a). Die Annahme des Landgerichts, der Eingriff sei durch § 70 Abs. 1 Satz 2, § 95 Abs. 2 StPO, § 100b Abs. 3 Satz 2 StPO a.F. in Verbindung mit § 110 Abs. 1 Satz 1 Nr. 1 TKG und den einschlägigen Vorschriften der TKÜV gerechtfertigt, ist jedoch von Verfassungs wegen nicht zu beanstanden (b). 35

a) Die Festsetzung des Ordnungsgeldes greift in die Berufsausübungsfreiheit ein. Den durch § 70 Abs. 1 Satz 2, § 95 Abs. 2 StPO in Verbindung mit § 100b Abs. 3 StPO a.F. sanktionierten Normen des TKG und der TKÜV kommt, soweit sie für Telekommunikationsdienstleister Vorhaltungspflichten statuieren, eine objektiv berufsregelnde Tendenz zu (vgl. zu diesem Erfordernis BVerfGE 95, 267 <302>; 97, 228 <253 f.>; 113, 29 <48>; 129, 208 <266 f.>; stRspr), da sie diesen technische und organisatorische Vorgaben für die Einrichtung ihres Betriebes machen (vgl. BGH, Beschluss vom 20. August 2015 - StB 7/15 -, juris, Rn. 7; Bär, in: KMR, StPO, § 100b Rn. 14a [Juni 2016]; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2492a; siehe auch Hermes, in: Dreier, GG, 3. Aufl. 2013, Art. 10 Rn. 28). Eine Berufswahlregelung liegt dagegen nicht vor; insbesondere wird dem Beschwerdeführer eine sinnvolle Ausübung seines Berufs nicht faktisch unmöglich gemacht (vgl. zu Anonymisierungsdiensten BVerfGE 125, 260 <359>). 36

b) Die Annahme des Landgerichts, der Eingriff in den Schutzbereich des Art. 12 Abs. 1 Satz 2 GG sei nach Maßgabe der einschlägigen gesetzlichen Vorschriften gerechtfertigt, begegnet keinen verfassungsrechtlichen Bedenken. 37

aa) Art. 12 Abs. 1 Satz 2 GG erlaubt Eingriffe in die Berufsfreiheit nur auf Grundlage einer gesetzlichen Regelung, die Umfang und Grenzen des Eingriffs erkennen lässt. Dabei muss der Gesetzgeber selbst alle wesentlichen Entscheidungen treffen, soweit sie gesetzlicher Regelung zugänglich sind (vgl. BVerfGE 73, 280 <295>; 80, 1 <20>). Je stärker in grundrechtlich geschützte Bereiche eingegriffen wird, desto deutlicher muss das gesetzgeberische Wollen zum Ausdruck kommen (vgl. BVerfGE 87, 287 <317>; 98, 49 <60>). Dies bedeutet nicht, dass sich die Eingriffsvoraussetzungen ohne weiteres aus dem Wortlaut des Gesetzes ergeben müssten; es genügt, dass sie sich mit Hilfe allgemeiner Auslegungsgrundsätze erschließen lassen, insbesondere aus dem Zweck, dem Sinnzusammenhang und der Vorgeschichte der Regelung (vgl. BVerfGE 19, 17 <30>; 58, 257 <277>; 62, 203 <210>; 80, 1 <20 f.>; 82, 209 <224>; BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 22. April 2014 - 1 BvR 2160/11 -, juris, Rn. 20). 38

Die Auslegung und Anwendung des einfachen Rechts ist dabei Sache der dafür allgemein zuständigen Gerichte und einer Nachprüfung durch das Bundesverfassungsgericht grundsätzlich entzogen, soweit bei der zu treffenden Entscheidung nicht Willkür vorliegt oder spezifisches Verfassungsrecht verletzt ist (vgl. BVerfGE 18, 85 <92 f.>; 34, 369 <379>). Ein etwaiger Fehler der Fachgerichte muss gerade in der Nichtbeachtung von Grundrechten liegen. Das ist in der Regel erst dann der Fall, wenn ein Fehler sichtbar wird, der auf einer grundsätzlich unrichtigen Anschauung von der Bedeutung eines Grundrechts, insbesondere vom Umfang seines Schutzbereichs beruht, oder wenn eine fehlerhafte Rechtsanwendung bei verständiger Würdigung der das Grundgesetz beherrschenden Gedanken nicht mehr verständlich ist (vgl. BVerfGE 18, 85 <92 f.>; 62, 189 <192 f.>; 89, 1 <14>; 95, 96 <127 f.>). 39

bb) Danach ist ein Grundrechtsverstoß nicht ersichtlich. Die Fachgerichte haben die Vorschriften über die Mitwirkungs- und Vorhaltungspflichten von Telekommunikationsdienstanbietern (§ 100b Abs. 3 Satz 2 StPO a.F. i.V.m. § 110 Abs. 1 Satz 1 Nr. 1 TKG, § 3, § 5 Abs. 1 und 2, § 6 Abs. 1 sowie § 7 Abs. 1 TKÜV) in verfassungsrechtlich vertretbarer Weise ausgelegt; sie durften ohne Verfassungsverstoß davon ausgehen, dass der Beschwerdeführer gegen diese Pflichten verstoßen hat (1). Von der ihnen in diesen Fällen gemäß § 100b Abs. 3 Satz 3 StPO a.F. in Verbindung mit § 95 Abs. 2 Satz 1 StPO eingeräumten Möglichkeit, die in § 70 Abs. 1 Satz 2 StPO bezeichneten Ordnungsmittel festzusetzen, haben sie zudem in verfassungsrechtlich nicht zu beanstandender Weise Gebrauch gemacht (2). 40

(1) Die Fachgerichte durften ohne Verfassungsverstoß davon ausgehen, dass der Beschwerdeführer verpflichtet war, den Ermittlungsbehörden die am überwachten Account vom Zeitpunkt der Anordnung an anfallenden externen IP-Adressen zur Verfügung zu stellen, weil die Überwachung der Telekommunikation im Sinne von § 100a StPO nicht nur die Kommunikationsinhalte, sondern auch die näheren Umstände der Telekommunikation einschließlich der fraglichen IP-Adressen erfasst (a). Vor diesem Hintergrund ist gegen die Auffassung des Landgerichts, wonach der Beschwerdeführer gemäß § 110 Abs. 1 Satz 1 Nr. 1 TKG in Verbindung mit § 3, § 5 Abs. 1 und 2, § 6 Abs. 1 sowie § 7 Abs. 1 Satz 1 Nr. 4 TKÜV verpflichtet ist, seinen Betrieb so zu gestalten, dass er diese - bei ihm vorhandenen - IP-Adressen im Rahmen einer rechtmäßig angeordneten Überwachung der Telekommunikation bereitstellen kann, von Verfassungs wegen nichts zu erinnern (b). Aus § 100g StPO ergibt sich nichts anderes (c). 41

(a) Die - verfassungskonforme (vgl. BVerfGE 129, 208) - Vorschrift des § 100a StPO ermächtigt zur Überwachung und Aufzeichnung der Telekommunikation. Der Begriff der Telekommunikation wird von der herrschenden Meinung in Literatur und Rechtsprechung verfassungsrechtlich zulässig unter Rückgriff auf die Legaldefinition in § 3 Nr. 22 TKG bestimmt. „Telekommunikation“ ist danach der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (vgl. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 6. Juli 2016 - 2 BvR 1454/13 -, juris, Rn. 25 ff. m.w.N., auch zur Gegenansicht). Vor dem Hintergrund dieses „weiten“ Telekommunikationsbegriffs unterfällt der Zugriff auf E-Mail-Kommunikation, jedenfalls soweit es sich um die Übertragung der Nachricht vom Gerät des Absenders über dessen Mailserver auf den 42

Mailserver des E-Mail-Providers und um den späteren Abruf der Nachricht durch den Empfänger handelt, unstrittig dem Anwendungsbereich des § 100a StPO (vgl. Schmitt, in: Meyer-Goßner/Schmitt, StPO, 61. Aufl. 2018, § 100a Rn. 6b; Bruns, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 100a Rn. 16 ff.; Bär, in: KMR, StPO § 100a Rn. 28 [Juni 2016]; Graf, in: BeckOK, StPO, § 100a Rn. 54 [1. Januar 2018]; Wolter/Greco, in: SK-StPO, 5. Aufl. 2016, § 100a Rn. 36; Hauck, in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, § 100a Rn. 73; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2482a; Singelnstein, NStZ 2012, S. 593 <596>; zum Zugriff auf E-Mails, die auf dem Mailserver des Providers gespeichert sind, vgl. BVerfGE 124, 43).

Dabei ist zu beachten, dass sich die nähere Auslegung des Begriffs „Telekommunikation“ im Rahmen des § 100a StPO insbesondere auch an dem grundrechtlichen Schutz des von der Überwachung Betroffenen durch Art. 10 GG orientieren muss, denn das Fernmeldegeheimnis ist der verfassungsrechtliche Maßstab für die heimliche Überwachung flüchtiger Daten (vgl. BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 6. Juli 2016 - 2 BvR 1454/13 -, juris, Rn. 32 m.w.N.; vgl. auch BVerfGE 100, 313 <358 f.>; 113, 348 <364 ff.>; 129, 208 <240 ff.>; Bruns, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 100a Rn. 4; Bär, in: KMR, StPO § 100a Rn. 10 [Juni 2016]; kritisch Wolter/Greco, in: SK-StPO, 5. Aufl. 2016, § 100a Rn. 38 ff.). Vom Schutz des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG sind aber nicht nur die Kommunikationsinhalte, sondern auch die näheren Umstände der Telekommunikation erfasst (vgl. BVerfGE 129, 208 <240 f.>). Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (vgl. BVerfGE 67, 157 <172>; 85, 386 <396>; 107, 299 <312 f.>; 129, 208 <241>). Art. 10 Abs. 1 GG umfasst dabei sämtliche, mit Hilfe der Telekommunikationstechniken erfolgenden Übermittlungen von Informationen, unabhängig davon, wer Betreiber der Übertragungs- und Vermittlungseinrichtungen ist (vgl. BVerfGE 107, 299 <322>; 129, 208 <241>). 43

Aber auch unter Einbeziehung dieses Schutzinhalts in die Auslegung von § 100a StPO ist gegen die Auffassung, die Überwachung der Telekommunikation gemäß § 100a StPO betreffe auch die (früher als Verbindungsdaten bezeichneten) Verkehrsdaten im Sinne des § 3 Nr. 30 TKG, soweit diese im Rahmen der zu überwachenden Telekommunikation anfallen (vgl. Hauck, in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, § 100a Rn. 14, 57; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2482a; siehe auch BVerfGE 107, 299 <314 ff.>), verfassungsrechtlich nichts zu erinnern. Zu den Verkehrsdaten in diesem Sinne gehören auch und gerade die anfallenden IP-Adressen. Diese werden dementsprechend in § 96 Abs. 1 Satz 1 TKG - der die Verkehrsdaten, die vom Diensteanbieter zulässigerweise erhoben werden dürfen, abschließend bestimmt - als Nummern (vgl. § 3 Nr. 13 TKG) der beteiligten Anschlüsse oder Einrichtungen aufgeführt (vgl. BTDrucks 15/2316, S. 89 - zum damaligen § 94 TKG -; Braun, in: Beck’scher TKG-Kommentar, 4. Aufl. 2013, § 96 Rn. 7; Lutz, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 96 Rn. 6 f.; Klesczewski, in: Säcker, TKG, 3. Aufl. 2013, § 96 Rn. 5; zur Zuordnung von dynamischen IP-Adressen zu den Verkehrsdaten vgl. BVerfGE 130, 151 <181 ff.>; BGH, Urteil vom 13. Januar 2011 - III ZR 146/10 -, juris, Rn. 22 ff.). Dynamische oder statische IP-Adressen, mit denen die Kunden eines Anbieters von E-Mail-Diensten mit ihren internetfähigen Endgeräten auf ihren E-Mail-Account zugreifen wollen, unterfallen daher grundsätzlich dem Anwendungsbereich des § 100a StPO (vgl. auch BGH, Beschluss vom 20. August 2015 - StB 7/15 -, juris). 44

(b) Der Umstand, dass die Überwachung des E-Mail-Verkehrs im Rahmen einer Anordnung nach § 100a StPO auch die bezeichneten IP-Adressen umfasst, bedeutet allerdings nicht schon zwangsläufig, dass der Beschwerdeführer als Betreiber einer Telekommunikationsanlage verpflichtet ist, Vorkehrungen zu treffen, um den Ermittlungsbehörden auch und gerade diese IP-Adressen zur Verfügung zu stellen. § 100b Abs. 3 Satz 2 StPO a.F. verweist insoweit auf die Vorschriften des TKG und der TKÜV. 45

Nach § 110 Abs. 1 Satz 1 Nr. 1 TKG besteht für Betreiber von öffentlich zugänglichen Telekommunikationsdiensten die Verpflichtung, ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung der Telekommunikationsüberwachung vorzuhalten und die entsprechenden organisatorischen Vorkehrungen für deren unverzügliche Umsetzung zu treffen. Die grundlegenden technischen Anforderungen und organisatorischen Eckpunkte für die Umsetzung der Überwachungsmaßnahmen regelt dabei die auf Grundlage der Ermächtigung in § 110 Abs. 2 TKG erlassene TKÜV. Danach unterliegt auch der Beschwerdeführer der Vorhaltungsverpflichtung; dass die in § 3 Abs. 2 TKÜV vorgesehenen Ausnahmen für bestimmte Arten von Telekommunikationsanlagen eingreifen, ist weder vorgetragen noch ersichtlich. 46

Der Umfang der bereitzustellenden Daten bestimmt sich nach § 5 Abs. 1 und 2 in Verbindung mit § 7 Abs. 1 TKÜV. Gemäß § 5 Abs. 1 TKÜV besteht die zu überwachende Telekommunikation - dem weiten Telekommunikationsbegriff des § 100a StPO entsprechend - aus dem Inhalt und den Daten über die näheren Umstände der Telekommunikation. Nach Absatz 2 der Vorschrift hat der Verpflichtete eine vollständige Kopie der Telekommunikation bereitzustellen, die über seine Telekommunikationsanlage abgewickelt wird. Als Teil dieser Überwachungskopie hat der Verpflichtete gemäß § 7 Abs. 1 Satz 1 Nr. 2, 3 und 4 TKÜV schließlich auch die bei ihm vorhandenen Daten über eine gewählte Rufnummer oder eine andere Adressierungsangabe bereitzustellen. Nach dem Sprachgebrauch des TKG unterfallen die bei einer Telekommunikation anfallenden IP-Adressen dabei ohne weiteres dem Begriff „andere Adressierungsangabe“, denn sie dienen gerade der Adressierung, also der Erreichung oder dem Auffinden eines bestimmten Ziels im Internet. So unterfallen IP-Adressen - wie bereits dargelegt - der Legaldefinition des § 3 Nr. 13 47

TKG, wonach Nummern im Sinne des TKG Zeichenfolgen sind, die in Telekommunikationsnetzen Zwecken der Adressierung dienen (vgl. OVG NRW, Beschluss vom 26. Mai 2011 - 13 B 476/11 -, juris, Rn. 13 ff.; Lünenbürger/Stamm, in: Scheurle/Mayen, TKG, 3. Aufl. 2018, § 3 Rn. 35; Büning, in: Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 3 Nr. 49; Fetzer, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 3 Rn. 79; Säcker, in: Säcker, TKG, 3. Aufl. 2013, § 3 Rn. 38; vgl. auch BTDrucks 16/2581, S. 22).

Fraglich könnte vorliegend allenfalls sein, ob die IP-Adressen beim Beschwerdeführer im Sinne des § 7 Abs. 1 Satz 1 TKÜV vorhanden sind. Der Beschwerdeführer macht mit seiner Verfassungsbeschwerde unter Hinweis auf seine Systemstruktur geltend, er verfüge über die öffentlichen IP-Adressen seiner Kunden nicht. Im gesamten Zugriffsbereich von „XX…" lägen weder intern noch an den Außengrenzen (namentlich am NAT-Lastverteiler) IP-Adressen mit Nutzerbezug vor. Dies ist indes in dieser Allgemeinheit nicht zutreffend. Schon aus der von ihm beschriebenen Systemstruktur ergibt sich, dass der Beschwerdeführer die öffentlichen IP-Adressen seiner Kunden wenigstens für die Dauer der Kommunikation speichern muss, da er ansonsten die abgerufenen Datenpakete seinen Kunden gar nicht übersenden könnte. Dies steht im Einklang mit der Stellungnahme des Bundesamtes für Sicherheit in der Informationstechnik, wonach die Software auf dem NAT-Lastverteiler in der Lage sein müsse, für die Gesamtdauer einer Verbindung die internen Verbindungsdaten den externen Verbindungsdaten zuzuordnen, weil sonst eine erfolgreiche Kommunikation nicht möglich sei. Dementsprechend räumt der Beschwerdeführer in seiner Erwiderung auf die Stellungnahme des Bundesamts für Sicherheit in der Informationstechnik ein, dass die IP-Adressen in den programminternen Datenstrukturen gespeichert werden. Es kann dahinstehen, ob der Beschwerdeführer mit dieser seinen Angaben nach „flüchtigen" Speicherung die öffentlichen IP-Adressen gemäß § 3 Abs. 3 BDSG erhebt (vgl. hierzu Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 102 ff.). Jedenfalls fallen die Daten beim Zugriff auf den überwachten E-Mail-Account an, sind der Telekommunikationsanlage des Beschwerdeführers wenigstens zeitweise bekannt und werden von dieser auch zur Herstellung einer erfolgreichen Kommunikation mit dem anfragenden Kunden benutzt. Es ist daher jedenfalls verfassungsrechtlich vertretbar anzunehmen, die Daten seien beim Beschwerdeführer vorhanden und von diesem als Teil der vollständigen Kopie der überwachten, über seine Telekommunikationsanlage abgewickelten Telekommunikation bereitzustellen. 48

Dass der Beschwerdeführer auf die externen IP-Adressen - derzeit - nicht zugreifen kann, steht dem nicht entgegen. Denn dies liegt nicht daran, dass die Daten an sich nicht vorhanden wären, sondern allein daran, dass sich der Beschwerdeführer aus Datenschutzgründen dazu entschlossen hat, diese vor seinen internen Systemen zu verbergen und sie nicht zu protokollieren. Das Unterlassen einer entsprechenden Protokollierung ist indes nicht zwangsläufig mit dem Einsatz eines NAT-Lastverteilers verbunden, sondern allein dem vom Beschwerdeführer bewusst gewählten Geschäfts- und Systemmodell geschuldet. Dies wird nicht nur vom Bundesamt für Sicherheit in der Informationstechnik in seiner Stellungnahme bestätigt, welches eine entsprechende Protokollierung sogar empfiehlt, sondern wird zudem durch den Vortrag des Beschwerdeführers belegt, wonach er sein System, wenn auch mit nicht unerheblichem technischen und finanziellen Aufwand, entsprechend umgestalten könnte. 49

Das Bundesverfassungsgericht hat in diesem Zusammenhang nicht darüber zu befinden, welcher konkrete Systemaufbau unter Datenschutzaspekten vorzugswürdig erscheint. Es hat nur darüber zu entscheiden, ob die Auslegung der gesetzlichen Vorgaben durch die Fachgerichte Grundrechte des Beschwerdeführers verletzt. Die Rechtsauffassung des Landgerichts lässt nach den obigen Darlegungen jedoch weder einen Verstoß gegen das Willkürverbot noch gegen spezifisches Verfassungsrecht erkennen. Zwar erscheint das Anliegen des Beschwerdeführers, ein datenschutzoptimiertes und daher für viele Nutzer attraktives Geschäftsmodell anzubieten, auch unter dem Gesichtspunkt des Art. 12 Abs. 1 GG grundsätzlich durchaus schützenswert. Dies kann ihn jedoch nicht von den im Rahmen einer vertretbaren Auslegung gewonnenen Vorgaben des TKG und der TKÜV, die dem verfassungsrechtlichen Erfordernis einer funktionstüchtigen Strafrechtspflege Rechnung tragen (vgl. BVerfGE 133, 168 <199 Rn. 57>; stRspr), entbinden. 50

Diesem Ergebnis steht schließlich auch nicht entgegen, dass sich die bereitzustellenden Daten nach der im Rahmen der Neubekanntmachung der TKÜV vom 11. Juli 2017 neu eingefügten Regelung in § 7 Abs. 1 Satz 1 Nr. 9 TKÜV nunmehr ausdrücklich auch auf die der Telekommunikationsanlage des Verpflichteten bekannten öffentlichen IP-Adressen der beteiligten Nutzer erstrecken. Denn diese Neuregelung lässt jedenfalls keinen verfassungsrechtlich zwingenden Schluss darauf zu, dass die fraglichen IP-Adressen bislang aus dem Kreis der bereitzustellenden Daten ausgenommen gewesen wären. Vielmehr kommt dem neu eingefügten § 7 Abs. 1 Satz 1 Nr. 9 TKÜV ersichtlich eine klarstellende Funktion zu. Denn ausweislich der Entwurfsbegründung der Bundesregierung sollten damit die Festlegungen der TR TKÜV und die diesen Festlegungen zugrundeliegenden Standards des Europäischen Instituts für Telekommunikationsnormen (die sogenannten ETSI-Standards) für die Überwachung von internetbasierten Telekommunikationsdiensten „rechtlich abgesichert" werden. Diese sähen bereits jetzt vor, dass im Rahmen einer Überwachungsmaßnahme neben anderen Daten auch die jeweilige Internetprotokoll-Adresse mitzuteilen sei (vgl. hierzu die Anlagen F.1 und F.2.1 zur TR TKÜV). In der Praxis würden diese Anforderungen durch die betroffenen Telekommunikationsunternehmen bereits erfüllt (vgl. BRDrucks 243/17, S. 26). 51

(c) Entgegen der Auffassung des Beschwerdeführers verdrängt § 100g Abs. 1 StPO, soweit die (Echtzeit- 52

)Überwachung künftiger Telekommunikation betroffen ist, die Vorschrift des § 100a StPO nicht. Zwar hat der Gesetzgeber diese Vorschrift in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198) in Anlehnung an § 100a StPO als allgemeine und umfassende Befugnis zur Erhebung von Verkehrsdaten ausgestaltet (vgl. BTDrucks 16/5846, S. 50). Ziel war dabei allerdings, die bisherige Gleichbehandlung von Verkehrsdaten und Daten über den Inhalt einer Telekommunikation, deren Echtzeiterhebung nur unter den Voraussetzungen der §§ 100a, 100b StPO in der damaligen Fassung zulässig war, zu überwinden. Dies deshalb, weil eine mögliche Beschränkung der Echtzeiterhebung von Verkehrsdaten entsprechend § 100a StPO aufgrund der unterschiedlichen Eingriffsintensität nicht geboten sei (vgl. BTDrucks 16/5846 a.a.O.). Schon dies spricht dagegen, dass der Gesetzgeber mit der Neufassung des § 100g Abs. 1 StPO den Anwendungsbereich des § 100a StPO einschränken wollte. Vielmehr wollte er eine im Vergleich zu § 100a StPO mit seinen deutlich strengeren Eingriffsvoraussetzungen erleichterte Zugriffsmöglichkeit auf Verkehrsdaten schaffen. § 100g Abs. 1 StPO tritt daher für den Zugriff auf Verkehrsdaten, soweit es zukünftige Telekommunikation beziehungsweise deren Echtzeiterhebung betrifft, neben den weiter anwendbaren § 100a StPO (vgl. Bruns, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 100a Rn. 24; Hauck, in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, § 100a Rn. 59; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2482a; vgl. auch Eckhardt, CR 2007, S. 336 <341>). Aus der vom Beschwerdeführer zitierten Begründung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl I S. 2218) ergibt sich nichts anderes. Die angegebenen Fundstellen enthalten nur eine allgemeine Umschreibung des Anwendungsbereichs der Norm ohne dass erkennbar wäre, dass der Gesetzgeber mit der Neuregelung den Anwendungsbereich des § 100a StPO beschränken wollte (vgl. BTDrucks 18/5088, S. 27, 31).

(2) Gegen die Festsetzung des Ordnungsgeldes im konkreten Fall ist von Verfassungs wegen ebenfalls nichts zu erinnern. 53

(a) Die gesetzlichen Voraussetzungen für die Verhängung eines Ordnungsgeldes liegen vor. 54

Gemäß § 100b Abs. 3 Satz 3 StPO a.F. in Verbindung mit § 95 Abs. 2 StPO können gegen den Diensteanbieter im Falle der Weigerung, seinen Pflichten nachzukommen, die in § 70 StPO bestimmten Ordnungs- und Zwangsmittel, also insbesondere Ordnungsgeld und - ersatzweise - Ordnungshaft, festgesetzt werden. Aufgrund des Beschlusses des Amtsgerichts vom 25. Juli 2016 war der Beschwerdeführer verpflichtet, den Strafverfolgungsbehörden die angeordnete Telekommunikationsüberwachung zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Die von ihm für diesen Fall zu treffenden Vorkehrungen umfassten - wie dargelegt - auch die Übermittlung der beim Beschwerdeführer künftig auflaufenden IP-Adressen, mit denen auf die in der Anordnung bezeichnete Kennung zugegriffen wird. Diese waren vom Beschwerdeführer als Teil der vollständigen Kopie der von der Anordnung betroffenen Telekommunikation bereitzustellen, ohne dass dies von Verfassungs wegen zu beanstanden wäre. 55

Gegen diese Pflicht hat der Beschwerdeführer verstoßen. Anhaltspunkte für ein fehlendes Verschulden sind nicht erkennbar. Dass sich der Beschwerdeführer bei seinem Handeln in einem unverschuldeten Verbotsirrtum befunden hätte, was der Verhängung eines Ordnungsgeldes entgegenstehen könnte (vgl. Wohlers/Greco, in: SK-StPO, 5. Aufl. 2016, § 95 Rn. 31 m.w.N.), macht er nicht geltend. Insbesondere ist weder vorgetragen noch ersichtlich, dass der Beschwerdeführer bei Einrichtung seines Systems zu den gegenständlichen, sein Unternehmen unmittelbar und spezifisch betreffenden Rechtsfragen verlässlichen und sachkundigen Rechtsrat eingeholt und auf diesen vertraut hätte (vgl. hierzu etwa BGH, Beschluss vom 2. Februar 2000 - 1 StR 597/99 -, juris, Rn. 27; Urteil vom 16. Mai 2017 - VI ZR 266/16 -, juris, Rn. 28 ff.). Gegen ihn durfte daher im Rahmen des den Gerichten insoweit eingeräumten Ermessens ein Ordnungsgeld bis zu 1000 Euro, und für den Fall, dass dieses nicht beigebracht werden kann, Ordnungshaft festgesetzt werden (vgl. § 70 Abs. 1 Satz 2 StPO i.V.m. Art. 6 EGStGB). 56

(b) Die Festsetzung eines Ordnungsgeldes in Höhe von 500 Euro war auch nicht unverhältnismäßig. 57

(aa) Soweit der Beschwerdeführer darlegt, die Verhängung des Ordnungsgeldes sei nicht geeignet gewesen, den Zweck - die Ausleitung der IP-Adressen - zu erreichen, weil der erforderliche Umbau seines EDV-Systems etwa zwölf Monate gedauert hätte und zu diesem Zeitpunkt die konkrete Überwachungsmaßnahme bereits abgelaufen gewesen sei, verkennt er die Funktion von Ordnungsgeld und Ordnungshaft. Ordnungsmitteln kommt sowohl eine präventive als auch eine repressive Funktion zu: Sie dienen zwar einerseits dazu, den Betroffenen anzuhalten, seine verfahrensrechtlichen Mitwirkungspflichten zu erfüllen. Andererseits handelt es sich aber auch um strafähnliche Sanktionen, die an einen vorangegangenen Ordnungsverstoß anknüpfen (vgl. nur Ignor/Bertheau, in: Löwe-Rosenberg, StPO, 26. Aufl. 2008, Anhang zu § 51 Rn. 2 m.w.N.). Dementsprechend bleiben sie auch dann aufrechterhalten, wenn eine präventive Wirkung nicht mehr erreichbar ist, insbesondere, weil der Betroffene in den Fällen des § 95 StPO den Gegenstand nachträglich herausgibt (vgl. Schmitt, in: Meyer-Goßner/Schmitt, StPO, 61. Aufl. 2018, § 95 Rn. 9; Greven, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 95 Rn. 4; Wohlers/Greco, in: SK-StPO, 5. Aufl. 2016, § 95 Rn. 32 m.w.N.; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2328). Nichts anderes kann in den Fällen des § 100b Abs. 3 Satz 3 StPO a.F. in Verbindung mit § 95 Abs. 2 StPO gelten. 58

(bb) Die Festsetzung der bezeichneten Ordnungsmittel war angesichts der Weigerung des Beschwerdeführers, seinen gesetzlichen Pflichten nachzukommen, auch erforderlich. Dass die Bundesnetzagentur zur Durchsetzung der sich aus § 110 Abs. 2 TKG in Verbindung mit der TKÜV ergebenden Verpflichtungen nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder bis zu einer Höhe von 500.000 Euro festsetzen kann (vgl. § 115 Abs. 2 Satz 1 Nr. 1 TKG), steht dem nicht entgegen. Denn die Festsetzung von Zwangsgeldern dient allein der Durchsetzung der gesetzlichen Vorhaltungsverpflichtungen und betrifft die gesetzeswidrige Einrichtung des Betriebs im Allgemeinen, während durch die Festsetzung eines Ordnungsgeldes gemäß § 100b Abs. 3 Satz 3 StPO a.F. in Verbindung mit § 95 Abs. 2 StPO - wie dargelegt - jedenfalls auch ein Pflichtverstoß im konkreten Strafverfahren sanktioniert werden soll. Die Vorschriften dienen daher unterschiedlichen Zwecken und stehen nebeneinander. Insbesondere kann der Umstand, dass ein Diensteanbieter seinen Betrieb von vornherein nicht den gesetzlichen Vorschriften entsprechend einrichtet, ihn nicht von der Verhängung strafprozessualer Ordnungsmittel befreien. 59

(cc) Die Verhängung des Ordnungsgeldes war schließlich verhältnismäßig im engeren Sinn. Gemäß dem Übermaßverbot darf die Schwere des Eingriffs nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen (vgl. BVerfGE 90, 145 <173>; 109, 279 <349 ff.>; 118, 168 <195 f.>; stRspr). Bei der gebotenen Gesamtabwägung muss die Grenze der Zumutbarkeit für den Adressaten der Maßnahme gewahrt sein (vgl. BVerfGE 90, 145 <173>; 120, 224 <241>). 60

Eine unzumutbare Belastung für den Beschwerdeführer ist hier nicht erkennbar. Das festgesetzte Ordnungsgeld selbst war mit 500 Euro nicht übermäßig hoch bemessen und gefährdet den Beschwerdeführer nach eigenen Angaben in wirtschaftlicher Hinsicht nicht. Allerdings wird dadurch ein Pflichtverstoß sanktioniert, den der Beschwerdeführer nur durch erhebliche, zeit- und kostenintensive Umbauarbeiten hätte vermeiden können und für die Zukunft vermeiden kann. Dies ist aber lediglich eine Folge der vom Beschwerdeführer bewusst gewählten Systemstruktur, die verhindert, dass er seinen Mitwirkungspflichten als Telekommunikationsanbieter nachkommen kann. Diese haben die Fachgerichte - wie dargelegt (vgl. oben V.2.b)) - in verfassungsrechtlich nicht zu beanstandender Weise den gesetzlichen Vorschriften entnommen. Allein die Wahl eines datenschutzoptimierten Geschäftsmodells kann den Beschwerdeführer nicht von der Einhaltung dieser Pflichten suspendieren. Es ist verfassungsrechtlich nicht zu beanstanden, wenn die Unternehmen die hierfür anfallenden Kosten grundsätzlich zu tragen haben (vgl. BVerfGE 125, 260 <359 ff.>). Dass die damit verbundenen Kostenlasten erdrosselnde Wirkung hätten, ist weder vorgetragen noch ersichtlich. 61

3. Von einer weiteren Begründung wird gemäß § 93d Abs. 1 Satz 3 BVerfGG abgesehen. 62

Diese Entscheidung ist unanfechtbar. 63