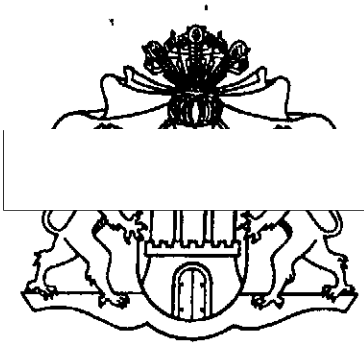

608 Qs 17/10
5000 Js 189/10
165 Gs 638/10

Landgericht Hamburg

Beschluss

In dem Ermittlungsverfahren

gegen

geboren am :

hat das Landgericht Hamburg, Große Strafkammer 8,

durch

den Vorsitzenden Richter am Landgericht
den Richter am Landgericht
den Richter am Landgericht

am 13.09.2010 beschlossen:

Auf die Beschwerde der Staatsanwaltschaft wird der Beschluss des Ermittlungsrichters des Amtsgerichts Hamburg vom 31. August 2010 wie folgt neugefasst:

Die Überwachung und Aufzeichnung der Telekommunikation, soweit sie durch Datenübertragung mittels IP-Protokolls (Voice-over-IP/VoIP) erfolgt, durch Ausleitung sämtlicher zur Versendung an einen Empfänger im Rahmen der Telekommunikation vorgesehenen Daten einschließlich Bild- und Videodaten, bevor das Programm „S" oder ein funktionsgleiches Fernkommunikationsprogramm die erzeugten Daten verschlüsselt, mittels Installation einer geeigneten Software auf den Laptops des Beschuldigten und mittels hierzu gegebenenfalls erforderlicher Maßnahmen der Fernsteuerung, betreffend die Laptops

Laptop A; Seriennummer
Laptop H P Seriennummer

bis zum Ablauf des 19.10.2010 wird angeordnet,

wobei von der Befugnis die Überwachung, Verarbeitung oder sonstige Manipulation sämtlicher nicht der Telekommunikation dienender Datenströme oder Datenverarbeitungsvorgänge ausgeschlossen ist.

Die Überwachung und Weiterleitung der Daten hat durch ein hierfür geeignetes Programm zu erfolgen, dessen Funktionsweise sicherstellt, dass die Überwachung oder Weiterleitung anderer als der von dieser Anordnung umfassten Daten ausgeschlossen ist.

Gründe:

I.

Die Staatsanwaltschaft Hamburg ermittelt in einem umfangreichen Verfahren wegen des Verdachts u.a. des organisierten Zigarettenschmuggels gegen den Beschuldigten. Die bisherigen Ermittlungen belegen, dass der Beschuldigte Laptops benutzt, um über diese mit einer sogenannten Webcam ausgestatten EDV-Geräte vermittels „Voice-over-IP" u.a. im S -Programm mit mutmaßlichen Mittätern konspirativ zu kommunizieren.

Auf Antrag der Staatsanwaltschaft ordnete der Ermittlungsrichter des Amtsgerichts Hamburg – gestützt auf § 100a StPO – die Überwachung und Aufzeichnung der Telekommunikation auch insoweit an, als sie durch Sprach- und Textübertragung mittels S oder funktionsgleicher Programme erfolge. Zu diesem Zweck gestattete er den Ermittlungsbehörden, eine geeignete Software auf den – aus anderen Gründen derzeit im Besitz der Ermittlungsbehörden befindlichen – Laptops zu installieren und ggf. mittels hierzu erforderlicher späterer Maßnahmen der Fernsteuerung der Software zu aktivieren (sogenannte „Quellen-TKÜ").

Ausgenommen von der ermittlungsrichterlichen Anordnung blieb ausdrücklich die Überwachung und Aufzeichnung desjenigen Teils der Voice-over-IP-Kommunikation, die über die Webcam eingefangenes Bilddatenmaterial liefere.

Die dagegen gerichtete, eine Erweiterung der Anordnung erstrebende Beschwerde der Staatsanwaltschaft hat Erfolg.

II.

Der Beschuldigte ist der ihm bisher vorgeworfenen Katalogstraftaten – gewerbsmäßige und bandenmäßige Hinterziehung von Einfuhrabgaben in drei Fällen (§ 373 Abs. 1, Abs. 2 Nr. 3 AO) – aufgrund der Ermittlungen des Zollfahndungsamtes in einer die Anordnung nach § 100a StPO tragenden Weise verdächtig.

Für das weitere Ermittlungsverfahren weist die Strafkammer jedoch auf Folgendes hin:

1. Die Einfuhrabgabenhinterziehung in den Fällen 1) und 2) (Hamburger „Freihafen-Fälle") dürfte bereits im unmittelbaren zeitlichen Zusammenhang mit der Abladung der im angefochtenen Beschluss näher bezeichneten Container vollendet gewesen sein. Dies folgt aus den nachstehenden Erwägungen.

Vor dem Verbringen in das Zollgebiet (vgl. Art. 36a Abs. 3 ZK) gibt der Reeder (oder ein Stellvertreter, Art. 36b Abs. 4 ZK) als Verbringer der Waren (Art. 36b Abs. 3 ZK) eine summarische Anmeldung bei

den zuständigen Zollbehörden ab. Bei der Verbringung in eine Freizone folgt die Pflicht zur summarischen Anmeldung für Waren, die von außerhalb des Zollgebietes kommen, aus Art. 176 Abs. 2 ZK. Die Meldung erfolgt in Deutschland über das Zoll-EDV-System ATLAS. Inhaltlich meldet der Reeder dabei die Daten des Schiffsmanifests, d.h. Menge, Art und Beschaffenheit der Ware. Zudem wird auch der Bestimmungsort (Freizone oder Seezollhafen) angegeben. Über das EDV-System wird dann eine Registriernummer (ATA-Nr. bei Freizone, ATB-Nr. bei Seezollhafen) erstellt. Währenddessen fährt das Schiff unter Benutzung des von den Zollbehörden bezeichneten Verkehrsweges (Art. 38 Abs. 1 ZK) zu der von den Zollbehörden bezeichneten Zollstelle oder in eine Freizone (Art. 166 ff ZK). In der Regel bei der Löschung der Fracht, d.h. beim Abladen der Waren iSv Art. 46 ZK, werden die Container anhand ihrer Container-Nr. durch den Hafenanlagenbetreiber computermäßig erfasst. Diese Datensätze, d.h. die Löschung eines bestimmten Containers mit einem ausweislich der summarischen Anmeldung bestimmten Inhalts, wird sodann in das ATLAS-System des Zolls eingepflegt. Hierbei handelt es sich um die „Mitteilung an die Zollbehörden in der vorgeschriebenen Form, dass sich die Ware bei der Zollstelle oder an einem anderen von den Zollbehörden bezeichneten oder zugelassenen Ort befindet", d.h. um die Gestellung der Ware nach Art. 40 ZK. Die Pflicht zur Gestellung folgt bei der Verbringung von Nichtgemeinschaftswaren unmittelbar in eine Freizone nunmehr (seit 1. Juli 2009) aus Art. 170 Abs. 2 Buchst. d) ZK (s. zum früheren Rechtszustand vor dem 01.07.2009 BGH NJW 03, 3068).

Wird bei der Wareneinfuhr in die EU auf das unter der Ladung versteckte oder durch besondere Vorrichtungen verheimlichte Schmuggelgut nicht hingewiesen oder werden in der summarischen Anmeldung nur Angaben zur Tarnware und damit falsche Angaben über die Warenart gemacht und damit nur Tarnware gestellt, entsteht die Einfuhrzollschuld wegen vorschriftswidrigen Verbringens in das Zollgebiet der EU nach Art. 202 Abs. 1 Buchst. a), Art 40, Art 4 Nr. 19 ZK. Da die vorschriftswidrig verbrachte Ware entgegen Art 217 Abs. 1 ZK nicht im Zeitpunkt der Zollschuldentstehung buchmäßig erfasst und dem Zollschuldner nach Art 221 Abs. 1 ZK mitgeteilt werden kann, wird die Zollschuld durch die Falscherklärung nicht oder nicht rechtzeitig iSv § 370 Abs. 4 S 1 AO festgesetzt. Mit Blick auf die in Art 218 Abs. 1 ZK vorgesehene Frist für die buchmäßige Erfassung wird es mithin spätestens am zweiten Tag nach der Zollschuldentstehung zur Vollendung der Steuerstraftat kommen.

Für die sogenannten „Freihafenfälle" gilt seit dem 01.07.2009 nichts anderes (vgl. zum früheren Rechtszustand BGH wistra 03, 389 und F/G/J/Jäger § 373 AO Rn. 39). Die Verpflichtung zur Gestellung und summarischen Anmeldung der Ware beim Verbringen in die Freizone führt – soweit statt der eigentlichen Ware nur die Tarnware (summarisch) angemeldet und gestellt wird – zur Zollschuldentstehung nach Art. 202 ZK, die wiederum nicht buchmäßig erfasst und nicht iSv Art. 221 Abs. 1 ZK mitgeteilt werden kann. Damit tritt spätestens zwei Tage nach Löschen der Ware im Freihafen (vgl. wiederum Art. 218 Abs. 1 ZK) Vollendung des Steuerdelikts ein.

Diese Rechtsfolge scheint sich auf den ersten Blick nicht mit dem Wesen des „Freihafens" zu vertragen, weil dort die Nichtgemeinschaftswaren gerade für die Erhebung der Einfuhrabgaben und Anwendung der handelspolitischen Maßnahmen nach Art. 166 Buchst. a) ZK bei der Einfuhr als nicht im Zollgebiet der Gemeinschaft befindlich angesehen werden. Mithin würden bei einer inhaltlich zutreffenden summarischen Anmeldung und Gestellung keine Einfuhrabgaben anfallen. Sie führt auch dazu, dass einer bei der späteren „Ausfuhr" aus dem „Freihafen" (typischerweise lagern Schmuggler Container mit Schmuggelgut in der Freizone zunächst zwischen) abgegebenen inhaltlich unzutreffenden Zollanmeldung wegen der Einmaligkeit der Zollschuldentstehung keine weitere zoll- oder zollstrafrechtliche Bedeutung zukommt. Die hier vorgenommene Betrachtung ist gleichwohl zwingend:

„Freihäfen" existieren nur noch in der historisierenden Terminologie des deutschen Zollrechts. Sie sind nach dem Zollkodex Freizonen nach Art. 166 ZK und damit Teile des Zollgebiets der Gemeinschaft. Es handelt sich bei ihnen um ein Zollverfahren im weiteren Sinne, nämlich um eine zollrechtliche Bestimmung iSv Art. 4 Nr. 15 ZK (Witte/Witte Art 202 ZK Rn. 30). Die dort lediglich fingierte Drittlandssituation erlangt Nichtgemeinschaftsware erst dadurch, dass sie ordnungsgemäß in dieses „Zollverfahren" überführt wird. Ordnungsgemäß kann sie aber nur dann in eine Freizone „überführt" werden, wenn sie mit zutreffender summarischer Anmeldung gestellt wird. Geschieht dies nicht, entsteht schon keine Drittlandsfiktion; vielmehr wird die Nichtgemeinschaftsware vorschriftswidrig iSv Art. 202 ZK mit allen zoll- und zollstrafrechtlichen Folgen verbracht.

Soweit diejenigen Personen, die die inhaltlich unzutreffende summarische Anmeldung abgegeben haben, in die mutmaßliche Tat eingeweiht sind, lässt sich ihr Tatbeitrag den übrigen Mittätern, mutmaßlich damit auch dem Beschuldigten, über § 25 Abs. 2 StGB zurechnen. Sind die Erklärenden hingegen gutgläubig, erfolgt die Zurechnung nach den Grundsätzen der mittelbaren Täterschaft.

Bei der vorschriftswidrigen Verbringung der Zigaretten in den „Hamburger Freihafen" werden Zoll-EU, (deutsche) Einfuhrumsatzsteuer und (deutsche) Tabaksteuer (vgl. § 21 Abs. 1 TabStG) in noch genau zu ermittelnder – hier aber prognostisch gesichert erheblicher – Höhe hinterzogen.

2. Der Beschuldigte ist auch im Fall 3) einer täterschaftlich begangenen vollendeten gewerbsmäßigen und bandenmäßigen Hinterziehung von Einfuhrabgaben verdächtig.

Soweit der die Zigaretten enthaltene Container bei der erstmaligen Einfuhr in die EU unter Abgabe einer lediglich die Tarnware umfassenden summarischen Anmeldung an der zuständigen EU-Außenzollstelle gestellt wurde, liegt wiederum iSd Art. 202 ZK ein vorschriftwidriges Verbringen vor, das zur Entstehung der Einfuhrabgaben führt. Die strafrechtliche Haftung von Mittätern oder Hintermännern, die nicht selbst an der Abgabe der falschen summarischen Mitteilung oder der mit ihr verknüpften Gestellung mitgewirkt haben, bereitet keine Probleme. Ihnen wird – soweit die unmittelbar Handelnden dolos sind – der Tatbeitrag der Erklärenden nach § 25 Abs. 2 StGB zugerechnet. Handeln die unmittelbar Erklärenden – etwa ausnahmsweise nicht eingeweihte Lkw-Fahrer – undolos, so bedienen sich die Hintermänner dieser Personen iSv § 25 Abs. 1 Var. 2 StGB als Tatmittler und handeln danach selbst als mittelbare Täter.

Beim hier ebenfalls in Betracht kommenden Schmuggel über die „Grüne Grenze" gilt Folgendes: Da in diesen Fällen gerade keine Gestellung oder eine mit ihr verknüpfte summarische Anmeldung stattfindet, weil die Täter an der Zollbehörde vorbei einführen, liegen regelmäßig Fälle des pflichtwidrigen Unterlassens einer Steuererklärung nach § 370 Abs. 1 Nr. 2 AO vor.

Bei dieser Steuerhinterziehung durch Unterlassen ist – jedenfalls nach der hergebrachten Dogmatik des § 370 Abs. 1 Nr. 2 AO – die Frage zu klären, wer von den an der Tat Beteiligten verpflichtet war, eine entsprechende Erklärung abzugeben, namentlich geht es darum, ob auch organisierende Hintermänner iSv § 370 Abs. 1 Nr. 2 AO erklärungspflichtig sein können. Der Bundesgerichtshof hat sich dieser Problematik über den Begriff des Verbringers genähert und dabei an die Rechtsprechung des Gerichtshofs der Europäischen Union in der Rechtssache *Viluckas und Jonusas* (Rs C-238/02 und C-246/02, wistra 04, 376; AW-Prax 04, 309) angeknüpft (BGH wistra 07, 224; NJW 07, 1294 mit abl. Anm. Witte/Harksen, AW-Prax 07, 378; s. auch F/G/J/Jäger § 370 AO Rn. 224b ff.; abl. Witte/Witte Art. 202 ZK Rn. 36). Danach verbringen bei der Einfuhr mit einem Kraftfahrzeug diejenigen Personen die Nichtgemeinschaftsware in das Zollgebiet der Gemeinschaft, die die Herrschaft über das Fahrzeug

im Zeitpunkt der Verbringung haben, nämlich u.a. die Fahrer, und zwar derjenige der das Fahrzeug lenkt, und sein Beifahrer oder Ersatzmann, sofern er sich im Fahrzeug befindet. Ferner sei auch eine andere im Fahrzeug befindliche Person Verbringer, wenn nachgewiesen ist, dass sie hinsichtlich der Verbringung der Waren Verantwortung trägt. Mit Blick darauf, dass es nach der EuGH-Entscheidung auf die Herrschaft über das Fahrzeug bei der Einfuhr ankomme, hat der BGH gefolgert, dass nicht nur der Fahrer, sondern kraft ihrer Weisungsbefugnis auch diejenigen Organisatoren des Transports, die beherrschenden Einfluss auf den Fahrzeugführer haben, indem sie die Entscheidungen zur Durchführung des Transports treffen und die Einzelheiten der Fahrt bestimmen, als Verbringer – und mithin als Gestellungspflichtige iSv Art 40 ZK – anzusehen seien (BGH aaO; s auch F/G/J/Jäger aaO). Strafbarkeitslücken blieben demnach allenfalls in dem unwahrscheinlichen, aus Tätersicht wegen des jederzeitigen Entdeckungsrisikos unvernünftigen Fall, in dem sich Hintermänner für das Verbringen in das Gemeinschaftsgebiet vorsatzloser Fahrer bedienen, dabei selbst aber keine unmittelbare Kontrolle über das Fahrzeug ausüben (s. F/G/J/Jäger § 370 AO Rn. 224c).

Bei der Bestimmung des mutmaßlichen Steuerschadens ist allerdings zu beachten, dass die Katalogtat des § 373 AO lediglich Einfuhrabgaben – allerdings auch solche ausländischer Staaten – umfasst. Bei einer Einfuhr in einen anderen Mitgliedstaat der EU handelt es sich dabei um Zoll-EU und – soweit nach innerstaatlichem Recht als Einfuhrabgabe ausgestaltet – die dortige Einfuhrumsatzsteuer und die dortige Verbrauchsteuer.

Soweit die Schmuggeltat an der Außengrenze eines anderen Mitgliedstaates begonnen wurde, aber – weil die Ware noch nicht endgültig zur Ruhe gekommen war und die Schmuggeltat somit noch nicht beendet wurde (vgl. BGH wistra 00, 425; NJW 07, 1294) – noch in andere Mitgliedstaaten „weitergeschmuggelt" wurde, können die in anderen Mitgliedstaaten anfallenden Verbrauchsteuern deshalb nicht Gegenstand eines deutschen Urteils sein, weil beim „Weiterschmuggeln" die weiteren ausländischen Verbrauchsteuern nicht mehr als Einfuhrabgabe anfallen (BGH NJW 07, 1294) und § 373 Abs. 4 AO nur die Einfuhrabgaben, derzeit nicht aber ausländische Verbrauchsteuern und ausländische Umsatzsteuer (vgl. § 370 Abs. 6 S 4 AO) unter deutschen Strafrechtsschutz stellt (vgl. Leplow, PStR 07, 180). Soweit der im Ausland begonnene Einfuhrschmuggel aber ohne Beendigung nach Deutschland fortgesetzt wird, kommt tateinheitlich – neben der Verkürzung der ausländischen bei der Einfuhr anfallenden Verbrauchsteuern und des Zolls – eine Steuerhinterziehung bezüglich der deutschen Verbrauchsteuern nach § 370 Abs. 1 Nr. 2 AO in Betracht.

Allerdings ist in Fällen dieser Art im Blick zu behalten, dass das gemeinschaftsrechtliche Verbrauchsteuersystem – jedenfalls für den Fall normgemäßen Verhaltens – davon ausgeht, dass verbrauchsteuerpflichtige Waren im Ergebnis grundsätzlich nicht mit den Verbrauchsteuern mehrerer Mitgliedstaaten belastet sein sollen. Das Gemeinschaftsrecht sieht deshalb die Möglichkeit der Erstattung von in anderen Mitgliedstaaten entstandenen und auch erhobenen Verbrauchsteuern vor. Vor diesem Hintergrund wird es nahe liegen, in vergleichbaren Fällen der Steuerhehlerei, des Schmuggels oder der Steuerhinterziehung die Strafverfolgung hinsichtlich der verkürzten Abgaben gemäß §§ 154, 154a StPO auf die bei der Einfuhr in einen anderen Mitgliedstaat hinterzogene Einfuhrabgabe Zoll sowie die bei dem Verbringen in das deutsche Verbrauchsteuergebiet hinterzogene deutsche Tabaksteuer zu beschränken. Es bedarf dann auch nicht der sonst erforderlichen Feststellung und Anwendung der tabaksteuerrechtlichen und umsatzsteuerrechtlichen Vorschriften anderer Mitgliedstaaten sowie der zuweilen schwierigen Berechnung und Darstellung der in anderen Mitgliedstaaten hinterzogenen Tabaksteuer (BGH Urt. vom 2. Februar 2010 – 1 StR 635/09; vgl. insoweit auch BGH NStZ 07,

595; siehe auch Jäger, NStZ 08, 21, 24). Auch bei einer etwaigen Inblicknahme nur der Hinterziehung von deutscher Tabaksteuer läge – wegen § 100a Abs. 2 Nr. 2 a) – eine Katalogtat vor.

III.

Die Voraussetzungen der Anordnung der beantragten Überwachungsmaßnahme liegen vor, insbesondere ist entgegen der Auffassung des Ermittlungsrichters auch die Überwachung und Aufzeichnung sämtlicher zur Kommunikation vorgesehener Daten einschließlich solcher, die Bild- oder Videoaufzeichnungen betreffen, zulässig.

Die beantragte sog. „Quellen-Telekommunikationsüberwachung", bei der Daten, die im Rahmen eines Telekommunikationsvorgangs entstehen und für die Versendung an einen Kommunikationsteilnehmer vorgesehen sind, durch ein hierzu eingerichtetes und auf dem für die Durchführung des Kommunikationsvorgangs genutzten Gerät aufgespieltes Computerprogramm an die Ermittlungsbehörden weitergeleitet werden, ist vom Anwendungsbereich des § 100a StPO grundsätzlich umfasst (vgl. Meyer-Goßner, StPO, 53. Auflage 2010, § 100a, Rdnr. 7a m. w. Nachw.).

Dabei ist im Hinblick auf die für den Eingriff erforderliche Rechtsgrundlage grundsätzlich zwischen dem Primäreingriff – der in der Weiterleitung der Kommunikationsdaten an die Ermittlungsbehörden liegt (dazu sogleich Ziff. 1) – und dem zur Durchführung dieser Maßnahme erforderlichen sekundären Eingriff – der im Aufspielen und in der Aktivität des die Kommunikationsdaten an die Ermittlungsbehörden versendenden Computerprogramms besteht (dazu sogleich Ziff. 2) – zu differenzieren. Beide Eingriffe sind im Rahmen der geltenden Vorschriften der Strafprozessordnung zulässig.

1. Die Überwachung und Aufzeichnung der vom Beschuldigten im Rahmen von Telekommunikationsvorgängen zum Zwecke dieser Kommunikation produzierten und für die Weiterleitung an den Kommunikationspartner vorgesehenen Daten ist in ihrer Gesamtheit von § 100a StPO erfasst. Der Begriff der – der Überwachung und Aufzeichnung zugänglichen – Telekommunikation gem. § 100a Abs. 1 StPO umfasst sämtliche technischen Vorgänge 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. Meyer-Goßner, StPO, 53. Aufl. 2010, § 100a, Rdnr. 6 unter Hinweis auf § 3 Nr. 22 und 23 TKG).

Insbesondere ergeben sich aus der Vorschrift – entgegen der im angefochtenen Beschluss vertretenen Auffassung – keine Anhaltspunkte dafür, dass bestimmte Dateninhalte wie etwa Bild- und Videodaten von der Überwachung und Aufzeichnung auszunehmen wären. Soweit durch die Übertragung visueller Inhalte eine Tangierung des Kernbereichs privater Lebensgestaltung des oder der Betroffenen gegenüber einer reinen Gesprächsüberwachung insbesondere dann ansteigt, wenn dieser in seiner Wohnung audiovisuelle Inhalte aufnimmt und versendet, steht dies der Anordnung der Überwachungsmaßnahme nicht entgegen. Vielmehr ist diesem erhöhten Schutzbedürfnis durch strikte Befolgung der Durchführungsvorschriften des § 100a Abs. 4 StPO Rechnung zu tragen, wonach Erkenntnisse aus dem Kernbereich privater Lebensgestaltung im Strafverfahren nicht verwertbar und die zugrundeliegenden Daten unverzüglich zu löschen sind.

2. Der „sekundäre Eingriff", der in der Durchführung der „Quellen-Telekommunikationsüberwachung" mittels eines heimlich in das informationstechnische System des überwachten Kommunikationsteilnehmers eingespielten, die Daten kopierenden und an die Ermittlungsbehörden über das Internet versendenden Computerprogramms besteht, ist ebenfalls zulässig. Zwar fehlt es für diese Maßnahme an einer ausdrücklichen gesetzlichen Regelung, sie ist jedoch als typische und in die Rechte des Betroffenen nur unwesentlich eingreifende Begleitmaßnahme der Telekommunikationsüberwachung als sogenannte „Annexkompetenz" von § 100a StPO gedeckt.

a) Die Annahme von „Annexkompetenzen" für nicht ausdrücklich gesetzlich geregelte Eingriffe in Rechte des Beschuldigten oder Dritter im Rahmen der Durchführung einer im Übrigen zulässigen strafprozessualen Maßnahme beruht auf der Überlegung, dass der Gesetzgeber bei der Schaffung der strafprozessualen Eingriffstatbestände nicht sämtliche weniger bedeutsamen Einzelheiten der – insbesondere technischen – Durchführung zulässiger Eingriffe in Rechte Betroffener ausdrücklich regeln kann und will und deshalb solche mit der Durchführung der zulässigen Maßnahme typischerweise verbundenen weiteren Eingriffe als ebenfalls zulässig vorausgesetzt hat, die erforderlich sind, um die gesetzlich geregelte Maßnahme nicht ganz oder in wesentlichen Teilen ihres Anwendungsbereiches ins Leere laufen zu lassen (vgl. zur Annexkompetenz im allgemeinen: BGH Ermittlungsrichter, Beschl. v. 20.3.2003, Az.: 1 BGS 107/03, Rdnr. 6 ff., zitiert nach juris; zur Annexkompetenz im Rahmen des § 100c StPO: BGH, Urteil v. 24.1.2001, Az.: 3 StR 324/00, Rdnr. 18, zitiert nach juris).

Hiervon ausgehend setzt die Annahme einer „Annexkompetenz" zunächst voraus, dass es sich bei dem in Rede stehenden, gesetzlich nicht ausdrücklich geregelten Eingriff um eine mit der gesetzlich geregelten Maßnahme *typischerweise verbundene* und *zu ihrer Durchführung erforderliche Begleitmaßnahme* handelt, da andernfalls nicht davon auszugehen ist, dass der Gesetzgeber die Möglichkeit einer solchen ergänzenden Maßnahme zumindest in Form eines „sachgedanklichen Mitbewusstseins" in Betracht gezogen und gebilligt hat.

Darüber hinaus darf von der Begleitmaßnahme lediglich eine *verhältnismäßig geringfügige Beeinträchtigung* grundrechtlich geschützter Interessen ausgehen, da andernfalls der grundgesetzliche – im vorliegenden Zusammenhang aus Art. 10 Abs. 2 Satz 1 GG folgende – Gesetzesvorbehalt umgangen würde. Insbesondere muss die Intensität des Begleiteingriffs in jedem Fall hinter dem Gewicht des primären Eingriffs zurückbleiben.

Beispielhaft zeigt sich die Notwendigkeit der Annahme solcher „Annexkompetenzen" in der gesetzlichen Regelung zur Wohnraumüberwachung gem. §§ 100c, 100d StPO. Die technische Durchführung der Wohnraumüberwachung wird in aller Regel ein heimliches und unbefugtes Eindringen der Ermittlungsbehörden in die Wohnung eines Betroffenen erfordern, um die für die Überwachung erforderlichen technischen Geräte zu installieren. Obwohl es sich hierbei um einen Grundrechtseingriff von erheblichem Gewicht handelt und das Gesetz in § 100b StPO auch umfangreiche Verfahrensvorschriften für die Durchführung der Maßnahme enthält, hat der Gesetzgeber die Schaffung einer ausdrücklichen Ermächtigungsgrundlage für das typischerweise erforderliche Eindringen in die Wohnung des Betroffenen nicht für erforderlich gehalten, sondern die Zulässigkeit dieser Begleitmaßnahme stillschweigend vorausgesetzt, da die Wohnraumüberwachung anders kaum oder gar nicht durchgeführt werden kann.

Das Beispiel der Wohnraumüberwachung gibt aufgrund der erheblichen Eingriffsintensität der vorausgesetzten Begleitmaßnahmen sogar Anlass, das aufgestellte Kriterium der *verhältnismäßig geringfügigen Eingriffsintensität* für die Annahme einer Annexkompetenz in Frage zu stellen. Vorliegend

soll dennoch von dieser Voraussetzung ausgegangen werden, da andernfalls die von Verfassungs wegen gebotene Begrenzung der Annahme von Annexkompetenzen nicht möglich erscheint.

b) Die Voraussetzungen der *Typizität* und der *Erforderlichkeit* der Begleitmaßnahme sind vorliegend erfüllt.

Für das Erfordernis der Typizität ist es im Rahmen des § 100a StPO aufgrund des umfassenden und technisch vielfältigen Charakters der überwachungsfähigen Telekommunikationsvorgänge ausreichend, wenn die Überwachung in einem wesentlichen Teil des Anwendungsbereiches der Vorschrift ohne das heimliche Einspielen eines Computerprogramms in das informationstechnische System des Überwachten undurchführbar wäre. Das ist vorliegend der Fall.

aa) Die sogenannte „Internet-Telefonie" in ihren verschiedenen technischen Ausformungen stellt eine wesentliche Fallgruppe innerhalb des Anwendungsbereiches des § 100a StPO dar. Sie kommt seit Jahren in der Praxis häufig vor, insbesondere da die hierfür notwendigen technischen Geräte und Vorkehrungen (Computer, Mikrofon-Ohrhörer-Kombination (sog. „Headset"), Internetanschluss mit schneller Datenübertragung) sehr verbreitet und preisgünstig zu erwerben sind, die hierfür erforderliche Software in verschiedenen Spielarten gratis im Internet verfügbar ist und zudem die Internet-Telefonie eine besonders preisgünstige Fernkommunikationsmethode darstellt.

Dafür, dass der Gesetzgeber diesen Anwendungsbereich des § 100a StPO trotz seiner erheblichen Verbreitung übersehen haben könnte (so AG Hamburg, Beschl. v. 28. 8. 2009, 160 Gs 301/09, Rdnr. 22, zitiert nach juris), bestehen insbesondere vor dem Hintergrund, dass durch die Verwendung des inhaltlich weitreichenden Begriffs der „Telekommunikation" in § 100a Abs. 1 StPO eine möglichst umfassende und von den technischen Einzelheiten ihrer Durchführung losgelöste Überwachung ermöglicht werden soll, keine Anhaltspunkte.

bb) Für die unbemerkte Überwachung dieser Kommunikationsform ist das heimliche Einspielen eines Programms in das informationstechnische System des Überwachten (regelmäßig ein handelsüblicher Computer) erforderlich. Die Überwachung eines im Rahmen der Internet-Telefonie (z. B. mit Hilfe des Programms „S ") durchgeführten Telekommunikationsvorgangs lässt es aus technischen Gründen nicht zu, die aufzuzeichnenden Daten erst nach ihrer Versendung aus dem informationstechnischen System des Überwachten zu kopieren und aufzuzeichnen, wie dies z. B. wie im Falle des Abhörens von Mobiltelefonen durch einen Zugriff des jeweiligen Netzbetreibers auf die in seinem Netz durchlaufenden Kommunikationsdaten und deren Weiterleitung an die Ermittlungsbehörden der Regelfall ist (vgl. § 100b Abs. 3 StPO).

In technischer Hinsicht werden die Kommunikationsdaten zunächst vom Kommunikationsteilnehmer erzeugt, indem reale Kommunikationshandlungen und -inhalte wie Sprache oder Bilder mit Hilfe technischer Geräte wie Mikrofon mit angeschlossenem Analog-Digital-Wandler („Soundkarte") und Digitalkamera („Webcam") aufgezeichnet und in digitale Daten umgewandelt werden. Diese Daten werden sodann innerhalb des Nutzercomputers an das den Telekommunikationsvorgang betreibende Programm (z. B. „S ") weitergeleitet, von diesem verschlüsselt und in verschlüsselter Form in das Fernkommunikationsnetz (Internet) eingespeist. Im Computer des Kommunikationsempfängers findet nach Eingang der verschlüsselten Daten ein umgekehrter Vorgang statt, d. h. die Daten werden zunächst entschlüsselt, anschließend wird der Nachrichteninhalt auf geeigneten Geräten (Monitor, Soundkarte mit Lautsprecher oder Kopfhörer) abgespielt.

Da die im Internet versandten verschlüsselten Daten – entsprechend dem Zweck der Verschlüsselung – selbst mit hohem technischem Aufwand nicht oder jedenfalls nicht zeitnah entschlüsselt werden können, erfordert die Überwachung dieser Art des Nachrichtenverkehrs einen Zugriff auf die Kommunikationsdaten innerhalb eines der beteiligten technischen Systeme (Computer), bevor diese vom jeweiligen Kommunikationsprogramm verschlüsselt oder nachdem sie beim Empfänger entschlüsselt worden sind, durch ein hierzu geeignetes, dem Überwachungszweck entsprechend heimlich in das informationstechnische System eines Nutzers eingebrachtes Programm.

Da die Internet-Telefonie nach alledem in der Praxis seit Jahren verbreitet ist und zudem das heimliche Einspielen eines die unverschlüsselten Kommunikationsdaten weiterleitenden Programms für die Überwachung dieser Kommunikationsform zwingend erfordert, sind die Kriterien der Typizität und der Erforderlichkeit vorliegend erfüllt.

c) Das heimliche Einspielen eines die Überwachung und Weiterleitung des Datenstroms durchführenden Computerprogramms bewirkt auch nur einen verhältnismäßig geringfügigen Eingriff in die Rechte des Betroffenen.

aa) In technischer Hinsicht bewirkt die Begleitmaßnahme eine geringfügige Belastung der Rechen- und Speicherkapazität des betroffenen Computers sowie eine je nach Datenmenge und Übertragungsgeschwindigkeit unterschiedlich ausfallende Verlangsamung der Internet-Datenverbindung aufgrund der durch das Überwachungsprogramm zusätzlich versandten Datenkopie. Diese Beeinträchtigungen betreffen im Wesentlichen den Bedienungskomfort des genutzten Computers und bewegen sich regelmäßig in einer für den Nutzer kaum wahrnehmbaren Größenordnung.

bb) Soweit teilweise der im heimlichen Aufspielen eines Überwachungsprogramms liegende Eingriff in ein privates informationstechnisches System als solcher bereits im Sinne einer „gravierenden Grenzverletzung zwischen Staat und Einzelnem" als schwerwiegend angesehen wird (vgl. AG Hamburg, aaO, Rdnr. 24 f.), vermag die Kammer dieser Ansicht nicht zu folgen.

Sie würde, da die tatsächlichen Aktivitäten des heimlich eingespielten Überwachungsprogramms sich auf die zulässige Weiterleitung der nach § 100a StPO zu überwachenden und aufzuzeichnenden Daten und die unter lit. aa) dargestellten geringfügigen Nutzungsbeeinträchtigungen beschränken, voraussetzen, dass das Aufspielen und die Existenz des Programms bereits eine schwerwiegende Gefährdung der Rechte des Betroffenen darstellen.

Als Gegenstand dieser Grundrechtsverletzung käme zwar das in der Rechtsprechung des Bundesverfassungsgerichts als Ausfluss des allgemeinen Persönlichkeitsrechts entwickelte besondere Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in Betracht (vgl. BVerfGE, Urteil vom 27. 2. 2008, 1 BvR 370/07, 1 BvR 595/07, Rdnr. 180 ff., zitiert nach juris). In der zitierten Entscheidung stellt das Bundesverfassungsgericht jedoch zugleich klar, dass eine gesetzliche Ermächtigung, die sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, *allein* an Art 10 Abs. 1 GG zu messen ist, wobei der Schutzbereich dieses Grundrechts unabhängig davon betroffen ist, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt. Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt (vgl. BVerfG, aaO, Leitsatz 4 und Rdnr. 166).

Demgegenüber erstreckt sich der Grundrechtsschutz des Art. 10 Abs. 1 GG nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort (BVerfG, aaO, Rdnr. 167).

Das Bundesverfassungsgericht führt (aaO) weiter aus:

> (Rdnr. 170) „Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert ("Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder - soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert - das Verhalten in der eigenen Wohnung."
>
> (Rdnr. 171) „Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen - anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung - stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden."
>
> (Rdnr. 172) „Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer 'Quellen-Telekommunikationsüberwachung', wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."

Zu der im vorliegenden Zusammenhang entscheidenden Frage, ob die „rechtlichen Vorgaben" für eine Quellen-Telekommunikationsüberwachung durch die bestehenden Vorschriften der Strafprozessordnung bereits gegeben sind, äußert sich das Bundesverfassungsgericht aufgrund des anderen Sachzusammenhangs der dortigen Entscheidung nicht. Dies ist nach Auffassung der Kammer der Fall, da § 100a StPO allein die Überwachung der „Telekommunikation", nicht aber sonstiger Daten für zulässig erklärt. Der von der Vorschrift gestattete Überwachungsrahmen ist damit hinreichend deutlich abgegrenzt, ein Zugriff auf andere Datenbestände als diejenigen aus laufender Telekommunikation – und damit eine den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betreffende Gefährdung – sind nach dem Wortlaut der Vorschrift ausgeschlossen.

Soweit das Bundesverfassungsgericht darüber hinaus die Sicherstellung der Beschränkung des überwachten Datenverkehrs auf laufende Telekommunikationsvorgänge fordert, betrifft dies im Ergebnis allein die Frage, ob die Ermittlungsbehörden zu einer strengen und rechtmäßigen Umsetzung einer Anordnung der „Quellen-Telekommunikationsüberwachung" in der Lage sind. Die Funktion des hierbei von den Ermittlungsbehörden eingesetzten Computerprogramms hat sich anordnungsgemäß auf die Überwachung und Weiterleitung der von der gerichtlichen Anordnung nach § 100a StPO erfassten Telekommunikationsdaten zu beschränken, mithin dürfen von der eingesetzten Software allein diejenigen Daten überwacht und aufgezeichnet werden, die für die Versendung in das Fernkommunikationsnetz vorgesehen sind und auf die dort zugegriffen werden könnte, wenn ihre Auswertung nicht aufgrund der Verschlüsselung praktisch unmöglich wäre.

Die entsprechenden Beschränkungen in der Funktion der eingesetzten Software sind durch zweckentsprechende Programmierung sicherzustellen. Die Ermittlungsbehörden dürfen daher die Überwachung auch nicht mit Computerprogrammen durchführen, deren Funktionsweise ihnen nicht so vollständig bekannt ist, dass die Übermittlung anderer als von der Anordnung nach § 100a StPO erfasster Daten oder sonstige unzulässige Datenmanipulationen nicht sicher ausgeschlossen werden können. Regelmäßig wird es daher für die Ermittlungsbehörden erforderlich sein, die genutzte Software entweder selbst fachkundig zu erstellen oder sie bei Ankauf von einem privaten Hersteller aus eigener technischer Sachkunde auf die Richtigkeit der Funktionsweise hin zu überprüfen.

Ist die Sicherstellung einer solchen Funktionsweise der eingesetzten Software nicht möglich, hat die Überwachung insgesamt zu unterbleiben. Wie bereits ausgeführt, handelt es sich aber insoweit nur um eine besondere Ausprägung des Grundsatzes, dass die Ermittlungsbehörden eine richterlich angeordnete strafprozessuale Maßnahme sorgfältig, rechtstreu und unter Beachtung der inhaltlichen Grenzen der Anordnung durchzuführen haben.

Der Umstand, dass die Überwachung durch ein heimlich in das informationstechnische System eingespieltes Programm erfolgt, stellt daher bei der als selbstverständlich vorauszusetzenden rechtstreuen Umsetzung der Maßnahme durch die Ermittlungsbehörden keinen durch § 100a StPO nicht abgedeckten Grundrechtseingriff dar, der über die oben lit. aa) genannten, geringfügigen Nutzungsbeeinträchtigungen hinausginge.

d) Der Annahme einer Annexkompetenz im vorstehend dargestellten Sinne stehen schließlich auch keine gesetzessystematischen Hindernisse entgegen.

aa) Der „Quellen"-Zugriff auf Kommunikationsinhalte auf dem informationstechnischen System eines Betroffenen steht nicht im Widerspruch zur gesetzlichen Ausgestaltung der Telekommunikationsüberwachung in §§ 100a, 100b StPO.

Insbesondere ergibt sich aus der gesetzlichen Regelung in § 100b Abs. 3 StPO, wonach jeder Anbieter von Telekommunikationsdiensten gegenüber dem Gericht und den Ermittlungsbehörden die Maßnahmen nach § 100a StPO zu ermöglichen und die hierfür erforderlichen Auskünfte zu erteilen hat, nach Auffassung der Kammer nicht schon, dass die Anordnung nach § 100a StPO sich ausschließlich an den Telekommunikationsanbieter („Netzbetreiber") richtet und mithin der Zugriff auf die Telekommunikationsdaten ausschließlich auf dem Leitungsweg im Herrschaftsbereich dieses Netzbetreibers erfolgen dürfte (so LG Hamburg, Beschl. v. 1.10.2007, Az.: 629 Qs 29/07, Rdnr. 34, zitiert nach juris; wohl auch Nack in Karlsruher Kommentar zur StPO, 6. Auf. 2008, § 100a, Rdnr. 5, der aber

gleichwohl die auf § 100a StPO gestützte „Quellen-TKÜ" für einen Übergangszeitraum bis zu einer gesetzlichen Regelung für zulässig hält (aaO, Rdnr. 27)).

Zwar wird in aller Regel die Überwachung im Wege des Zugriffs auf beim Netzbetreiber vorhandene Daten den zweckmäßigsten Weg der Telekommunikationsüberwachung darstellen, da auf diese Weise sowohl die Heimlichkeit der Überwachung als auch ihre Beschränkung auf reine Telekommunikationsdaten sichergestellt werden kann. Dass aber die Ermittlungsbehörden auf diese Möglichkeit nicht beschränkt sind, folgt bereits daraus, dass es auch von § 100a StPO erfasste Telekommunikationsformen gibt, bei denen kein Anbieter tätig wird, wie z. B. bestimmte Formen des analogen Funkverkehrs. Im Übrigen lässt sich eine solche Beschränkung aber der gesetzlichen Regelung, die allein den Netzbetreiber zur Unterstützung verpflichtet, seine Inanspruchnahme aber nicht vorschreibt, nicht entnehmen.

Auch unter dem Gesichtspunkt der Eingriffsintensität spricht im Übrigen die Regelung des § 100b Abs. 3 StPO nicht gegen die hier angenommene Annexkompetenz. Mit der dort vorgesehenen Möglichkeit einer Einbeziehung des Netzbetreibers in den Überwachungsvorgang hat der Gesetzgeber eine für den Betroffenen besonders belastende Durchführungsmaßnahme, durch die nämlich Mitarbeiter des Netzbetreibers als private Dritte auf seine Verwicklung in ein strafrechtliches Ermittlungsverfahren aufmerksam gemacht werden, für zulässig erklärt. In dieser Hinsicht stellt das Installieren einer Überwachungssoftware – von dem allein die Ermittlungsbehörden Kenntnis haben – für den Überwachten einen Eingriff von erheblich geringerer Intensität dar.

bb) Der Anordnung steht auch nicht entgegen, dass die Ermittlungsbehörden in §§ 100a, 100b StPO anders als z. B. in § 100c Abs. 1 StPO nicht ausdrücklich zum „Einsatz technischer Mittel" ermächtigt werden (vgl. hierzu LG Hamburg, aaO, Rdnr. 35 im Zusammenhang mit der Typizität des Einsatzes technischer Mittel bei der Telekommunikationsüberwachung). Dass die Überwachung jeglichen elektrischen oder elektronischen, digitalen oder mittels analoger Signale durchgeführten Kommunikationsverkehrs den Einsatz technischer Mittel erfordert, kann als dem Gesetzgeber bei der Schaffung der Vorschrift sicher bekannt und damit von der hier angenommenen Annexkompetenz abgedeckt betrachtet werden. Im Übrigen setzt ersichtlich auch der in § 100b Abs. 3 StPO vorgesehene Datenzugriff durch einen Telekommunikationsanbieter den Einsatz besonderer technischer Vorkehrungen voraus, da eine Datenüberwachung in dessen normalem Geschäftsgang nicht vorkommt. Dass aber zwar der private Netzbetreiber zum Einsatz technischer Überwachungsmittel befugt sein soll, die den Vorgang beauftragenden Ermittlungsbehörden selbst jedoch nicht, liegt erkennbar nicht in der Absicht des Gesetzgebers.

cc) Die Quellen-Telekommunikationsüberwachung greift auch nicht – in durch die Ermächtigungsgrundlage des § 100a StPO nicht gerechtfertigter Weise – in Rechte des Betroffenen aus Art. 13 GG ein, auch wenn sich das für die Telekommunikation genutzte Gerät in der Wohnung eines Betroffenen befindet.

Für die Abgrenzung zwischen im vorliegenden strafprozessualen Zusammenhang durch § 100a StPO geregelte Eingriffe in das Grundrecht aus Art. 10 GG einerseits und durch § 100c StPO regulierte Eingriffe in das Grundrecht aus Art. 13 GG andererseits kommt es nicht entscheidend auf den Standort des Kommunikationsgerätes an. Dies ist beispielsweise für die Überwachung des Mobilfunkverkehrs insofern allgemein anerkannt, als eine Überwachungsmaßnahme nach § 100a StPO nicht deshalb unzulässig wird oder abgebrochen werden muss, weil ein überwachtes Gespräch von einem der Beteiligten aus seiner Wohnung heraus geführt wird.

Demgegenüber beruht die Abgrenzung der Schutzbereiche vorrangig auf der vom Betroffenen selbst bestimmten Zielrichtung seiner Kommunikation. Richtet diese sich im Wege einer Fernkommunikation nach außen, ist regelmäßig der Schutzbereich des Fernmeldegeheimnisses betroffen, wohingegen die „nichtöffentliche" (vgl. § 100c Abs. 1 StPO) Kommunikation innerhalb privater Räume dem Schutzbereich des Art. 13 GG unterfällt. Im Hinblick auf den Schutz informationstechnischer Systeme ist zur Abgrenzung namentlich von Bedeutung, dass der sein System an ein Fernkommunikationsnetz anschließende Betroffene sich insoweit freiwillig eines Teils seiner durch Art. 13 GG geschützten Privatsphäre begibt. Das Bundesverfassungsgericht (aaO) führt hierzu aus:

> (Randnummer 175) „Darüber hinaus kann eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13 Abs. 1 GG zu messen sein, so beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG ist die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera dazu genutzt werden."
>
> (Randnummer 176) „Art. 13 Abs. 1 GG vermittelt dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet (vgl. etwa Beulke/Meininghaus, StV 2007, S. 63 <64>; Gercke, CR 2007, S. 245 <250>; Schlegel, GA 2007, S. 648 <654 ff.>; a.A. etwa Buermeyer, HRRS 2007, S. 392 <395 ff.>; Rux, JZ 2007, S. 285 <292 ff.>; Schaar/Landwehr, K&R 2007, S. 202 <204>). Denn der Eingriff kann unabhängig vom Standort erfolgen, so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone."

Im vorliegenden Zusammenhang ist nach diesen Ausführungen weder durch das Übertragen von Telekommunikationsdaten aus Wohnungen, noch durch das Einspielen eines Telekommunikations-Überwachungsprogramms auf den vom Beschuldigten genutzten mobilen Computern (Laptops) ein durch § 100a StPO nicht gerechtfertigter Eingriff in das Grundrecht aus Art. 13 GG anzunehmen.

Landgericht Hamburg

Ausgefertigt:

Urkundsbeamtin
der Geschäftsstelle