Der Generalbundesanwalt
beim Bundesgerichtshof

Karlsruhe, den 29.10.2010

- [redacted] -

Nur für die Handakten!

Verfasser: [redacted]

Betrifft: Ermittlungsverfahren gegen [redacted]
wegen [redacted]

hier: Rechtliche Zulässigkeit der sogenannten „Quellen-TKÜ"

Vfg.:

1. Vermerk:

1. Zur Fragestellung:

Das BKA hat in dem vorgenannten Ermittlungsverfahren angeregt, einen Beschluss gemäß §§ 100a, 100b StPO zu erwirken, der „das Bundeskriminalamt ermächtigt, diejenigen Maßnahmen zu treffen, die erforderlich sind, um die Telekommunikation des Endgerätes (konkret die von der Beschuldigten genutzten „Personal Computer oder Laptops") in unverschlüsselter Form zu überwachen und aufzuzeichnen." Zur Begründung hat das Bundeskriminalamt ausgeführt, die Beschuldigte nutze unter anderem die verschlüsselnden Softwareprogramme Skype (zur Internettelefonie per Voice-over-IP) und MSN (zum Austausch von Textnachrichten in Echtzeit) sowie das Verschlüsselungsnetzwerk TOR.[1]

Unter einer Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) ist die Ausleitung von zum Zeitpunkt der Überwachung erzeugten Kommunikationsinhalten noch vor ihrer Verschlüsselung unmittelbar aus einem der beteiligten Zielrechner zu verstehen. Eine Mitwirkung des Diensteanbieters ist nicht erforderlich. Nach derzeitigem Stand der Technik ist für den Zugriff auf die zur Telekommunikationsübertragung bestimmten Daten vor der Verschlüsselung und Übertragung regelmäßig ein Softwareprogramm erforderlich, das - verdeckt - auf dem Zielcomputer installiert werden muss. Das Programm greift technisch auf den Datenfluss zu, bevor dieser im Ablauf des vom Benutzer verwendeten Telekommunikationsprogramms verschlüsselt wird, zum Beispiel am Mikrofon oder der Tastatur des Rechners.[2]

1 Vermerk des Bundeskriminalamtes vom 4. Oktober 2010
2 Henrichs, Kriminalistik 2008, 438

2. Zur rechtlichen Zulässigkeit der sogenannten Quellen-TKÜ:

Ein Antrag auf Anordnung einer sogenannten Quellen-Telekommunikationsüberwachung kommt aus Rechtsgründen nicht in Betracht. Es fehlt an der erforderlichen Rechtsgrundlage für einen Eingriff in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

Das BVerfG hat in seinem Urteil zur Online-Durchsuchung[3] entschieden, dass das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG - über seine bisher anerkannte Ausprägung hinaus - auch die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet.[4] Der Schutzbereich dieses Grundrechts erfasst sowohl das Interesse des Nutzer an der Vertraulichkeit der erzeugten, verarbeiteten und gespeicherten Daten als auch die Integrität des geschützten Systems gegen Zugriffe Dritter, durch die die Leistungen, Funktionen und Speicherinhalte des Systems genutzt werden können.[5] Nach der Entscheidung des BVerfG stellt die heimliche Infiltration eines informationstechnischen Systems mit einer forensischen Software einen Grundrechtseingriff von besonders hohem Gewicht dar. Ein Gesetz, das zu einem solchen Eingriff ermächtigt, muss daher besondere Anforderungen an den Eingriffsanlass vorsehen, Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen und die Maßnahme unter den Vorbehalt richterlicher Anordnung stellen.[6]

Eine Ermächtigung zur Infiltration eines informationstechnischen Systems, die diesen Anforderungen gerecht wird, enthält die Strafprozessordnung nicht.

2.1

Nach der genannten Entscheidung des BVerfG ist eine Ermächtigung dann allein an Art. 10I GG zu messen, wenn sie sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden. Danach kommt § 100a StPO als Eingriffsgrundlage einer Quellen-TKÜ in Betracht, wenn sichergestellt werden kann, dass ein weitergehender Eingriff in die Vertraulichkeit und die Integrität des geschützten Systems unter-

3 BVerfG Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - NJW 2008, 822, 827 - *Gegenstand war die Frage der Zulässigkeit der Regelung der Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen*

4 BVerfG aaO

5 BVerfG aaO, Rn. 204; Die Integrität des Systems ist bereits dann verletzt, wenn aufgrund der Infiltration nicht mehr zweifelsfrei zu klären ist, ob ein Berechtigter oder ein Dritter für einen gespeicherten Inhalt verantwortlich ist: Buermeyer/Bäcker in HRRS 2009, 433, 437.

6 BVerfG aaO, Leitsatz 3 sowie Rn. 242 ff. und 257 ff.

bleibt.[7] Eine solche **Beschränkung** des Eingriffs kann jedoch derzeit **technisch nicht gewährleistet** werden. Vielmehr ist für die Durchführung der Quellen-TKÜ die verdeckte Installation einer Software (sogenannter „Trojaner") auf dem Endgerät des Betroffenen erforderlich, um die Inhalte vor der Kommunikationsschnittstelle abzufangen und auszuleiten. Wird jedoch Fremd-Software auf einem System installiert, so bewirkt bereits diese Infiltration einen Eingriff in die Integrität des Systems. Das BVerfG hat in diesem Zusammenhang ausgeführt:

> *„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." „... es könne (ferner) nicht ausgeschlossen werden, dass der Zugriff selbst bereits Schäden auf dem Rechner verursacht. So könnten Wechselwirkungen mit dem Betriebssystem zu Datenverlusten führen... Zudem ist zu beachten, dass es einen rein lesenden Zugriff infolge der Infiltration nicht gibt. Sowohl die zugreifende Stelle als auch Dritte, die eventuell das Zugriffsprogramm missbrauchen, können auf Grund der Infiltration des Zugriffsrechners Datenbestände versehentlich oder sogar durch gezielte Manipulationen löschen, verändern oder neu anlegen."* [8]

Da zudem mit der Infiltration, die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems bereits genommen ist,[9] sind - zumindest nach derzeitigem Stand der Technik - die bestehenden Eingriffsermächtigungen in der Strafprozessordnung nicht nur am Grundrecht aus Art. 10 GG, sondern stets auch an dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme zu messen.

2.2

Hinzu tritt, dass das BVerfG in seiner Entscheidung neben technischen Vorkehrungen zur Beschränkung der Quellen-TKÜ ausdrücklich auch entsprechende „rechtliche Vorgaben" fordert[10]

Dem entspricht es, dass der Gesetzgeber für den präventiv-polizeilichen Bereich in dem Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das BKA vom 25. Dezember 2008 (BGBl. I S. 3083) neben der Befugnis zur Überwachung und Aufzeichnung der Telekommunikation (§ 20l Abs. 1 BKAG) eine eigenständige Rechtsgrundlage für die

---

7 BVerfG aaO, Leitsatz 4
8 BVerfG aaO Rn. 189 und 240
9 BVerfG aaO Rn. 204
10 BVerfG aaO Rn. 190

Quellen-TKÜ (§ 20l Abs. 2 BKAG) geschaffen hat. Aus der Gesetzesbegründung, wonach § 20l Abs. 2 Satz 1 BKAG eine Rechtsgrundlage *für den heimlichen, technischen Eingriff in ein informationstechnisches System* schafft, ergibt sich, dass auch der Gesetzgeber von der Notwendigkeit einer ausdrücklichen gesetzlichen Ermächtigung für die Quellen-TKÜ ausgeht.[11]

2.3

Schließlich ist die Durchführung einer Quellen-TKÜ bei verfassungskonformer Auslegung auch nicht als eine **Annexkompetenz** zu § 100a StPO zulässig, wenn zur Überwachung Software auf dem betroffenen Endgerät installiert werden muss.[12] In diesem Fall ist zwischen der eigentlichen Telekommunikationsüberwachung als Primärmaßnahme und der zur Umsetzung notwendigen Installation der entsprechenden Software und damit der Infiltration des Zielcomputers als Vorbereitungs- und Begleitmaßnahme der Überwachung (Sekündärmaßnahme) zu unterscheiden.[13] Nach der Rechtsprechung des Bundesgerichtshofs ist zwar grundsätzlich davon auszugehen, dass der Gesetzgeber mit der Primärbefugnis zu eingriffsrechtlichen Maßnahmen stillschweigend auch eine Ermächtigung für Vorbereitungs- und Begleitmaßnahmen geschaffen hat (sogenannte Annexkompetenz). Dies gilt allerdings nur, sofern diese mit einer solchen Maßnahme typischerweise unerlässlich verbunden sind, lediglich geringfügig in den Rechtskreis des Betroffenen eingreifen oder zumindest unter Beachtung des Verhältnismäßigkeitsgrundsatzes eine notwendige Begleitmaßnahme darstellen, für die kein milderes Mittel in Betracht kommt.[14]

Dies kann vorliegend angesichts des Gewichts des Grundrechtseingriffs, der mit einer Infiltration des Zielcomputers des Beschuldigten verbunden ist, nicht angenommen werden. Das BVerfG hat in diesem Zusammenhang ausgeführt.[15]

> *„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. ...*

---

11 BT-Drucksache 16/9588, S. 29

12 so auch AG Hamburg, Beschluss vom 28. August 2009, StraFo 2009, 512 ff.; Buermeyer/Bäcker, HRRS 2009, 433 ff; a. A. Meyer-Goßner StPO § 100a Rn. 7 m.w.N.; Graf in BeckOK StPO Edition 7 (Stand 1. August 2010) § 100a Rn. 114, 115; Nack in KK StPO § 100a Rn. 27; Bär in KMR § 100a Rn. 31; LG Hamburg, Beschluss vom 13. September 2010 (608 Qs 17/10); AG Bayreuth, MMR 2010, 266; Bär, MMR 2008, 215, 218; krit. zum Beschluss des AG Hamburg in StraFo 2009, 512 auch Kudlich in JA 2010, 310

13 Henrichs, Kriminalistik 2008, 438; LG Hamburg, Beschluss vom 13. September 2009 – 608 Qs 17/10

14 Ermittlungsrichter des BGH NJW 1997, 2189; BGHSt 46, 266, 273 f.; Schneider, NStZ 1999, 388

15 BVerfG Rn. 188, 234 und 236

Das Gewicht des Grundrechtseingriffs ist von besonderer Schwere, wenn eine heimliche Infiltration die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten ermöglicht. ...

Schließlich ist zu berücksichtigen, dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechniken zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff unterlaufen. die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs."

Die Ermächtigungsnormen in §§ 100a, 100b StPO sind auf eine anschlussbasierte Telekommunikationsüberwachung zugeschnitten und enthalten daher gerade keine rechtlichen Vorgaben, um die Integrität eines infiltrierten Endgerätes unter Verhältnismäßigkeitsgesichtspunkten zu minimieren und Datenveränderungen oder Datenerfassungen über die bloße Überwachung hinaus auszuschließen.[16]

2. Über

Herrn Referatsleiter TE 1
Herrn AL TE
Herrn Referatsleiter TE 4

mit der Bitte um Kenntnisnahme zugeleitet.

Im Auftrag

[redacted]

16 Buermeyer/Bäcker, HRRS 2009, 433, 438