Constantin Abate

Online-Durchsuchung, Quellen-Telekommunikationsüberwachung und die Tücke im Detail

Einfluss rechtlicher und technischer Entwicklungen auf verdeckte Online-Ermittlungen zur Gewährleistung der Inneren Sicherheit

Nach einer langen öffentlichen Debatte um die Rechtmäßigkeit von Online-Durchsuchungen stellte sich in der jüngsten Vergangenheit heraus, dass nach Aussage des Bundeskriminalamtes (BKA) bislang keine Online-Durchsuchung erfolgt ist (vgl. http://www.tagesschau.de/inland/onlinedurchsuchung112.html). In diesem Artikel wird der Frage nachgegangen, was die rechtlichen und technischen Gründe dafür sein können, dass das BKA die Möglichkeit zur Durchführung einer Online-Durchsuchung trotz entsprechender Ermächtigungsgrundlage noch nicht in Anspruch genommen hat.

1 Die Online-Durchsuchung – Voraussetzungen, Zugriffsmöglichkeiten, Ergebnisse

Die Online-Durchsuchung setzt zunächst voraus, dass der Zielrechner infiltriert und mit einer Spionagesoftware, dem sogenannten „Bundes-Trojaner", versehen wird. Das kann online mittels unterschiedlicher Möglichkeiten erfolgen:

Die gängigste und effizienteste Methode zur Infiltration eines Computers ist die Ausnutzung von Sicherheitslücken, die in der installierten Software existieren und bislang unentdeckt geblieben sind (Zero-Day-Exploits[1]). Eine andere Angriffsart, die auf den gleicher Vorgehensweise beruht, ist die Nutzung so genannter „Backdoors". Dabei handelt es sich um Sicherheitslücken, die wissentlich und willentlich vom Hersteller in sein Produkt eingebaut werden, um einen späteren Zugriff zu ermöglichen.[2]

Eine weitere Möglichkeit besteht darin, Downloads zu infizieren, indem sich eines Internetknotens bemächtigt wird, z.B. über die Einflussnahme auf einen großen Internet Provider. Dabei wird die Tatsache ausgenutzt, dass jeder Computernutzer von Zeit zu Zeit Downloads durchführt, um beispielsweise sein Betriebssystem auf den neuesten Stand zu bringen. Solchen Updates kann die Spionagesoftware angehängt werden, so dass diese sich von dem Computernutzer unbemerkt auf den Computer installiert.[3]

Problematisch ist dabei, dass die Infizierung von Downloads ausgehend von einem Netzknoten zwangsläufig alle anderen Computer betrifft, die mit diesem Knoten verbunden sind. Eine zielgerichtete Infiltration ist somit nicht möglich.[4]

Beliebte Infiltrationsmethoden, weil unaufwendig, nutzen Mitwirkungshandlungen des Nutzers aus. Diese können darin bestehen, dass der Nutzer viel versprechende E-Mail-Anhänge öffnet, was die Installation der Schadsoftware auslöst. Ein anderes Mittel ist das Herumliegenlassen von infizierten Datenträgern, wie CD-ROMs und USB-Sticks, die beim Einlegen in das Laufwerk bzw. dem Einstecken in den USB-Port ebenfalls die Installation der Schadsoftware bewirken.[5]

Auch hier kann die Infiltrationsmaßnahme jeden treffen, der sich des infizierten Datenträgers bemächtigt. Ein zielge-

Constantin Abate

Rechtsanwalt, Konzerndatenschutzbeauftragter bei der InterComponentWare AG.

E-Mail: ra@constantinabate.de

1 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (136).

2 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (136).

3 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (145).

4 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (145).

5 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (136).

richteter Einsatz der Spionagesoftware ist hierüber nicht möglich.

Die erfolgreiche Infiltration des Zielcomputers durch die behördliche Stelle belegt allerdings, dass auch jeder Dritte diesen Zielcomputer erfolgreich infiltrieren kann. Das wiederum zieht nach sich, dass nie mit Sicherheit gesagt werde kann, wer die Informationen, die auf dem Zielcomputer gefunden wird, dort gespeichert hat. Die Authentizität der Daten ist demnach in keiner Weise gewährleistet.[6] Damit kann die Online-Durchsuchung immer nur eine Verdachtserhärtungsmaßnahme darstellen.[7]

Somit ist festzuhalten, dass die Online-Durchsuchung unzuverlässige Ergebnisse liefert, da sie nicht zielgerichtet eingesetzt werden kann und die derart erhobenen Daten keinen Beweischarakter haben.

2 Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

Die Online-Durchsuchung nach § 5 VSG NRW a.F. (alte Fassung) war Gegenstand des Online-Urteils des Bundesverfassungsgerichts.[8] Mit § 5 VSG NRW a.F. wurde zum ersten Mal der Versuch unternommen, die Online-Durchsuchung gesetzlich zu normieren. Das Bundesverfassungsgericht nahm die Verfassungsbeschwerde gegen § 5 VSG NRW a.F. zum Anlass, die materielle Rechtmäßigkeit der Online-Durchsuchung intensiv zu betrachten. Dies führte u.a. dazu, dass eine neue Ausprägung des allgemeinen Persönlichkeitsrechts in Verbindung mit der Menschwürde (Art. 2 I i.V.m. Art. 1 I GG) in Form des Rechts auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme normiert wurde.

Auslöser für diese Rechtsprechung war die Ansicht, dass die Online-Durchsuchung eine Maßnahme sei, die eine völlig neue Eingriffsqualität aufweise. Diese neue Eingriffsqualität ergibt sich aus der Vielzahl der Informationen, die über einen Betroffenen durch den Zugriff auf das von ihm genutzte informationstechnische System gesammelt werden können.[9] Beispielsweise wird der Personal Computer heute in vielfacher Weise genutzt und bietet ein Spiegelbild der persönlichen Interessen und Neigungen.[10] Daraus ergibt sich, dass die ermittelnde Behörde mit einer einzigen Infiltrationsmaßnahme Zugriff auf eine Vielzahl von Informationen über einen Betroffenen erhält.[11] Das Bundesverfassungsgericht beschloss daher, das allgemeine Persönlichkeitsrecht fortzubilden und diese Lücke zu schließen, um den neuartigen Gefährdungen zu begegnen, die durch wissenschaftlich-technischen Fortschritt und gewandelte Lebensverhältnisse entstanden waren.[12]

Wegen der vermuteten Schutzlücke des Rechts auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht das Recht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme entwickelt, das unter der Bezeichnung „IT-Grundrecht" große Beachtung gefunden hat. Vertraulichkeit bedeutet dabei, dass eine Information nur den zur Kenntnisnahme berechtigten Personen zugänglich gemacht werden darf.

Unter Integrität ist hier zu verstehen, dass eine Information unverfälscht sein muss. Das heißt, dass keine unerwünschten Veränderungen an der Information durchgeführt werden dürfen.[13] Überträgt man diese Anforderung auf informationstechnische Systeme, so konstituiert der Integritätsschutz einen Schutz vor Veränderungen an diesem System.

Legt man diese Definition zu Grunde, erklärt sich daraus unmittelbar die Eingriffsqualität der Infiltration des Zielcomputers durch eine Spionagesoftware, denn bereits durch das Aufspielen der Spionagesoftware ändert sich der Zustand des Zielcomputers.

Das Bundesverfassungsgericht hat also den Grundrechtsschutz zeitlich vorverlagert, da die Infiltration eines informationstechnischen Systems stets zur Folge hat, dass das System kompromittiert ist, auch wenn noch keine Daten das System verlassen haben.[14] Der Grundrechtsschutz ist somit auf eine technische Vorstufe erweitert, die bisher noch keinen Eingriff in höchstpersönliche Rechte darstellte. Daher wurde auch prompt Kritik laut, die ein angeblich entpersonalisiertes Technik-Grundrecht anprangerte.[15]

Dem hält das Bundesverfassungsgericht entgegen, dass die Infiltration des Systems die wichtigste und einzige Hürde für einen vollständigen Zugriff auf personenbezogene Daten des Betroffenen darstelle und somit unter den Schutz der Verfassung zu stellen sei.[16] Außerdem sei zu bedenken, dass das Recht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme als Ausprägung des Schutzes der Persönlichkeit entwickelt wurde. Dementsprechend sei der Schutzbereich dieses Grundrechts immer vor dem Hintergrund der Gefährdungen der Persönlichkeit des Einzelnen zu begreifen. Zwar sei der Schutzgegenstand des IT-Grundrechts ein technisches System, dieser Umstand entpersonalisiere das IT-Grundrecht jedoch genauso wenig, wie es den speziellen Gewährleistungen in Art. 13 und Art. 10 GG deshalb an einem Persönlichkeitsbezug fehle, weil sie einen Raum und ein Kommunikationsmittel schützen.[17] In all diesen Fällen könne nicht von einer Entpersonalisierung des Grundrechtsschutzes ausgegangen werden.

Der Schutzbereich des „IT-Grundrechts" umfasst das eigengenutzte informationstechnische System des Grundrechtsträgers. Der Begriff des informationstechnischen Systems ist bewusst offen formuliert und umfasst jedes elektronische System, mit dem Informationen verarbeitet werden.[18] Gerade für den Schutz der Internetkommunikation ist es darüber hinaus wesentlich, dass der Begriff des informationstechnischen Systems keinen räumlichen Zusammenhang voraussetzt. Vielmehr können auch Netze, die aus mehreren räumlich getrennten Komponenten bestehen, als ein System angesehen werden, wenn die verbundenen Geräte funktional eine Einheit bilden.[19]

Weiterhin stellt das Bundesverfassungsgericht im „Online-Urteil" fest, dass ein

6 Hansen / Pfitzmann, DRiZ 2007, S. 227; Roggan, NJW 2009, S. 261.

7 Roggan, in: Roggan (Hrsg.), Online Durchsuchungen, S. 102.

8 BVerfG NJW 2008, 822.

9 BVerfG NJW 2008, 822 (825).

10 Hoffmann-Riem, JZ 2008, S. 1012.

11 Eifert, NVwZ 2008, S. 521.

12 BVerfG NJW 2007, 2465.

13 https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/g/g05/g05085.html

14 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (133).

15 Eifert, NVwZ 2008, S. 521 (522).

16 BVerfG NJW 2008, 822 (825).

17 Bäcker, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgericht: Erörtert von den wissenschaftlichen Mitarbeitern, S. 99 (126).

18 Bäcker, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgericht: Erörtert von den wissenschaftlichen Mitarbeitern, S. 99 (126).

19 BVerfG NJW 2008, 822.

Eingriff in informationstechnische Systeme erst vorgenommen werden darf, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Als hinreichend wichtiges Rechtsgut für die Rechtfertigung einer Online-Durchsuchung gelten ausschließlich Leib, Leben und Freiheit von Personen oder solche Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlage für die Existenz von Menschen berühren.[20] Weitere Voraussetzung für den Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist eine im Einzelfall drohende Gefahr, d.h. ein konkretisiertes und zeitlich absehbares Geschehen sowie die Beteiligung bestimmter Personen.[21]

Damit stellt das Bundesverfassungsgericht hohe Anforderungen an einen rechtmäßigen Eingriff in das Recht auf Vertraulichkeit und Integrität von eigengenutzten informationstechnischen Systemen.

3 Technische Entwicklungen

Neben der höchstrichterlichen Rechtsprechung haben auch technische Entwicklungen einen Einfluss auf die Tätigkeit der Polizeibehörden und Geheimdienste im Umfeld informationstechnischer Systeme, daher werden diese im Folgenden näher beleuchtet.

Bei der Betrachtung der Entwicklung der Datenverarbeitung sind zwei sich deutlich abzeichnende Mega-Trends zu verzeichnen: Die Allgegenwärtigkeit der Datenverarbeitung, die unter dem Schlagwort des „ubiquitous computing“[22] Bekanntheit erlangt hat und die ständig steigende Verfügbarkeit der elektronisch gestützten Datenverarbeitung für jedermann.[23]

Die derzeit letzte Stufe dieser Entwicklung ist das Cloud Computing. Hierunter ist die Zurverfügungstellung verschiedenster Services von Speicherplatz über Rechenleistung bis zur Software mittels einer Vielzahl von Servern, die über das Internet miteinander verbunden sind, zu verstehen.[24] Ein Cloud Provider macht diese Services für einen Kunden nutzbar. Der Cloud Provider nimmt die Daten des Kunden entgegen und weist diese, durch die Nutzung entsprechender Algorithmen, verteilten Servern flexibel zu.[25] Dem Kunden entzieht sich dabei die Kenntnis darüber wo genau seine Daten verarbeitet werden.

Aufgrund der Attraktivität dieser Services ist zu erwarten, dass in Zukunft vermehrt derart über das Internet bereit gestellte Anwendungen mit der auf privaten Rechner installierter Software zusammenwachsen werden.[26] Dieser Prozess geht einher mit der steigenden Akzeptanz des Cloud Computing. Daraus resultiert, dass zukünftig eine Online-Durchsuchung der Datenspeicher, die von einer Person genutzt werden, entweder unmöglich oder nur stark verzögert möglich sein wird, da diese zunächst ausfindig gemacht werden müssen.

Weiterhin hat das zur Folge, dass zukünftig die Durchsuchungen von Infrastrukturkomponenten jeglicher Art im Internet unter einem Grundrechtsvorbehalt stehen, denn die Vernetzung, Virtualisierung und Allgegenwärtigkeit informationstechnischer Systeme lässt es nicht mehr zu, Teile von ihnen vom Grundrechtsschutz auszunehmen.[27]

Ergänzend ist noch darauf hinzuweisen, dass jedem Computernutzer eine Vielzahl offen zugänglicher Verschlüsselungsprogramme zur Verfügung steht, mit denen er gespeicherte Daten effektiv vor unbefugter Einsichtnahme durch jedwede Spionagesoftware schützen kann.

4 Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)

Diese technischen Schwierigkeiten sowie die erhöhte Eingriffsschwelle für die Durchführung der Online-Durchsuchung haben dazu geführt, dass zunehmend die sogenannte Quellen-TKÜ, also die Telekommunikationsüberwachung an der Quelle, als präferierter Lösungsansatz von Ermittlungsbehörden propagiert wird.[28] Hierbei gilt, dass der Telekommunikationsbegriff auch den Datenverkehr in Computernetzen erfasst.[29]

Als Quellen-TKÜ wird ein Überwachungsvorgang bezeichnet, der Daten, die versendet werden sollen, vor der Verschlüsselung durch den Versender oder eingehende Daten nach der Entschlüsselung durch den Empfänger erfasst.[30] Zeitlich erfolgt das Abgreifen der Informationen, die über Mittel der Fernkommunikation einer anderen Partei mitgeteilt werden sollen, bevor diese tatsächlich übermittelt werden. Bei Informationen die empfangen und folglich zunächst übermittelt wurden, erfolgt der Zugriff durch die Quellen-TKÜ nach dem Abschluss der Übermittlung, wenn die Daten auf dem Zielrechner gespeichert sind.

Technisch wird das über eine Spionagesoftware bewerkstelligt, die als „Key-Logger“ charakterisiert wird. Im Gegensatz zu einem Trojaner erfasst ein Key-Logger nicht den Inhalt der Speichermedien eines Rechners. Der Key-Logger zeichnet vielmehr Tastaturanschläge und Bildschirminhalte auf, die auf dem Zielrechner gemacht bzw. angezeigt werden.[31] Es besteht somit unter technischen Gesichtspunkten fast kein Unterschied zwischen Key-Loggern und Trojanern, abgesehen von den Informationen, auf die sie abzielen (Tastatureingaben vs. Speicherinhalte). Die Form der Infiltration und die Übermittlung der erhobenen Daten, zumeist per E-Mail an eine vorher definierte und in der Spionagesoftware einprogrammierte Adresse, sind gleich.

Wird die Quellen-TKÜ mittels eines Key-Loggers realisiert, unterscheidet sie sich folglich grundlegend von der Telekommunikationsüberwachung, wie sie z.B. in § 20l BKAG geregelt ist. Diese darf sich nach § 20l Abs. 2 Ziff. 1 BKAG nur auf die Überwachung der laufenden Kommunikation erstrecken. Die Daten, die durch

20 Hoffmann-Riem, JZ 2008, S. 1012 (1020).

21 Kühne, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl., S. 85 (90).

22 Schaar, Das Ende der Privatsphäre, Der Weg in die Überwachungsgesellschaft, 2. Aufl., S. 49; Schoch, Jura 2008, S. 353.

23 Hoffmann-Riem, JZ 2008, S. 1012 (1020).

24 Schulz**, in:** Taeger/Wiebe (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, S. 403.

25 Fickert**, in:** Taeger/Wiebe (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, S. 420.

26 Hoffmann-Riem, JZ 2008, S. 1012 (1021).

27 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (146).

28 Gercke, in: Taeger/Wiebe (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, S. 500 (504).

29 Gercke, in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl.,S. 146 (152).

30 Hoffmann-Riem, JZ 2008, S. 1012 (1021).

31 Hansen/Pfitzmann, in: Roggan (Hrsg.), Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 1. Aufl, S. 131 (137).

die Quellen-TKÜ abgegriffen werden, befinden sich dahingegen statisch auf dem infiltrierten Computer. Greift eine staatliche Stelle nach dem Abschluss eines Kommunikationsvorgangs auf Kommunikationsdaten zu, die im Herrschaftsbereich des Empfängers gespeichert sind, so realisiert sich nicht ein kommunikationsspezifisches, sondern ein allgemeines informationstechnisches Risiko.[32] Nichts anderes gilt, wenn der Zugriff auf Daten erfolgt, die durch entsprechende Eingaben an der Tastatur im Entstehen begriffen sind, bevor diese Gegenstand eines Kommunikationsvorganges werden. Die Quellen-TKÜ ist somit kein Unterfall der Telekommunikationsüberwachung sondern eine Ausprägung der verdeckten Online-Ermittlung.

Somit kommt auch § 20l BKAG als Ermächtigungsgrundlage für diese Form der Quellen-TKÜ entgegen landläufiger Meinung[33] nicht in Betracht. Einschlägig ist vielmehr § 20k BKAG. Das ergibt sich auch daraus, dass der Key-Logger bei der Aufzeichnung nicht unterscheiden kann zwischen Daten, die zur Kommunikation bestimmt sind und Daten, die lokal gespeichert werden sollen, beispielsweise in einem Word-Dokument, und er somit ausnahmslos alle Tastaturanschläge und Bildschirminhalte aufzeichnet.

Seit der „Online-Entscheidung" und der Entwicklung des Rechts auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, besteht Klarheit darüber, dass es unerheblich ist mit welchem technischen Mittel genau personenbezogene Daten aus einem informationstechnischen System abgezogen werden. Ein Grundrechtseingriff ist bereits dann zu bejahen, wenn die technische Integrität des Systems verletzt worden ist. Das Aufbringen des zur Quellen-TKÜ notwendigen „Bundes-Key-Loggers" tut das in der gleichen Weise wie das Aufbringen eines „Bundes-Trojaners", so dass nach heutiger Rechtslage auch bei der Quellen-TKÜ von einem Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme auszugehen ist. Diese unterliegt somit der gleichen Eingriffsschwelle wie die Online-Durchsuchung. Voraussetzung für die Durchführung einer Quellen-TKÜ ist demnach auch eine Gefahr für Leib, Leben oder Freiheit von Personen oder solche Rechtsgüter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlage für die Existenz von Menschen berühren.

5 Fazit

Da sowohl die Weiterentwicklung informationstechnischer Systeme als auch die höchstrichterliche Rechtsprechung zur Online-Durchsuchung deren Einsatzmöglichkeiten erheblich eingeschränkt haben, ist zukünftig von einem erhöhten Einsatz der Quellen-TKÜ als Mittel der verdeckten Online-Ermittlung auszugehen, da diese zumindest die technischen Probleme bezüglich der verteilten Datenhaltung und des Einsatzes von Verschlüsselungstechnologien umgehen kann.

Darüber hinaus sind die Online-Durchsuchung und die Quellen-TKÜ, sofern diese mittels einer Software die funktional einem Key-Logger entspricht durchgeführt wird, sowohl technisch wie auch dogmatisch gleichwertige Maßnahmen zur verdeckten online Ermittlung.

Ein Blick in die Gesetzesbegründung für den § 20k BKAG zeigt auch, dass der Gesetzgeber mit den dort benannten technischen Mitteln sowohl den „Bundes-Trojaner", wie auch den „Bundes-Key-Logger" erfassen wollte.[34] Auch unter diesem Gesichtspunkt ist die Durchführung der Quellen-TKÜ als Telekommunikationsüberwachung auf der Grundlage von § 20l BKAG oder § 100a StPO rechtswidrig und stellt eine Umgehung angemessener Rechtfertigungserfordernissen dar. Daraus folgt, dass sowohl die Online-Durchsuchung, wie auch die Quellen-TKÜ nur von dem BKA und nur auf Grundlage des § 20k BKAG rechtmäßig durchgeführt werden können. Alle anderen Polizeibehörden sowie die Inlands-Geheimdienste müssen sich bis zur Schaffung einer entsprechenden Ermächtigungsgrundlage für den verdeckten Eingriff in informationstechnische Systeme mit der Telekommunikationsüberwachung im engeren Sinne begnügen. Strafverfolgungsorgane können darüber hinaus noch die Beschlagnahme von informationstechnischen Systemen oder deren Teile nach § 94 II StPO nutzen.

32 Hoffmann-Riem, JZ 2008, S. 1012 (1017).

33 So z.B. Roggan NJW 2009, S. 261 (262).

34 Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, Deutscher Bundestag Drucksache 16/10121, 16. Wahlperiode, 13.08.2008, S. 29.