gemeinsame Übungen vorgenommen werden und Möglichkeiten zur Überprüfung der Leistungen besteht. Insbesondere bei Übergangssituationen, z.B. beim Wechsel des Dienstleisters, ist es wichtig, zu regeln, ab wann der Dienstleister für Notfallplanung verantwortlich wird. Der hierdurch gesteigerten Verletzlichkeit des Unternehmens ist zumindest in der Anfangsphase durch besondere Aufmerksamkeit der Geschäftsleitung Rechnung zu tragen.

Eine sich verbreitende Form der IT-Notfallplanung mit Hilfe von Dritten ist, trotz aller bislang noch bestehenden Unsicherheiten,[49] die Hinterlegung von Quellcode bei einem sog. Escrow- Anbieter, mit der Absicht, den Zugriff auf den Quellcode einer für das Unternehmen kritischen Applikation auch im Falle der Insolvenz des Softwarelieferanten sicherzustellen.

49 Hierzu BGH v. 17.11.2005 – IX ZR 162/04, CR 2006, 151 mit Anm. *Plath/Scherenberg* sowie *Berger*, CR 2006, 505.

IV. Fazit und Ausblick

Die rechtlichen Anforderungen an eine IT-Notfallplanung können alle Unternehmen betreffen. Als Teil des betrieblichen Risikomanagements ist sie ständige Pflichtaufgabe der Unternehmensleitung. Im Bereich der Banken- und Finanzdienstleister ist aktuell eine weitere Zunahme der Regelungen für die IT-Notfallplanung zu beobachten. Zunehmende Bedeutung wird auch die IT-Sicherheit bekommen, denn die Sicherheit eines IT-Systems ist von dessen Verfügbarkeit nicht zu trennen. Die im Zuge von Outsourcing- und Business Process Outsourcing Projekten wachsende Abhängigkeit der Unternehmen von fremden IT-Systemen wird die Durchsetzung und Verbreitung von Standards für die IT-Notfallplanung fördern, denn der Kostendruck auf Seiten der Dienstleister erfordert die kostengünstige Realisierung solcher IT-Notfallplanungen in „genormter" Qualität. Allerdings kann die Einhaltung solcher Standards stets nur Indiz für pflichtgemäßes Verhalten sein, die Verantwortlichkeit der Unternehmensleitungen wird bleiben.

Rechtsprechung zum Computerrecht

BGH: Keine Rechtsgrundlage für heimliche Ausforschung von Computern

StPO §§ 100a, 102, 105, 106, 152, 163

Leitsatz der Redaktion

Die heimliche Ausforschung von auf dem Computer eines Beschuldigten gespeicherte Daten ist mangels Ermächtigungsgrundlage strafprozessual unzulässig.

BGH, Beschl. v. 25.11.2006 – 1 BGs 184/2006

Aus der Begründung:

1. Die beantragte Ausforschung des Computers ist strafprozessual gesetzlich nicht zulässig (§ 163 Abs. 3 StPO). Bei dem heimlichen Zugriff auf die auf dem Computer des Beschuldigten gespeicherten Daten handelt es sich um einen schwerwiegenden Eingriff in das den persönlichen Freiheitsrechten zuzuordnende Recht auf informationelle Selbstbestimmung. An der hierfür notwendigen gesetzlichen Gestattung fehlt es. Die im Beschluss des BGH v. 21.2.2006 – 3 BGs 31/06 vertretene Auffassung wird hier nicht geteilt.

a) Der allgemeine Ermittlungsauftrag an die Staatsanwaltschaft und die Polizei (§§ 152 Abs. 2, 163 Abs. 1 StPO) bietet keine Grundlage für Eingriffe in grundrechtlich geschützte Freiheitsrechte.

b) Telekommunikationsvorgänge mögen bei der Computerausforschung unter Umständen durch Zufall tangiert sein. Die Maßnahme zielt jedoch auf umfassende Erhebung aller gespeicherten Informationen ab, unabhängig davon, ob sie aus Kommunikationsvorgängen stammen oder nicht. Im Übrigen ist auch nach der neuen (Senats-)Rechtsprechung des BVerfG mit der Abspeicherung der Kommunikationsvorgang abgeschlossen. § 100a StPO kommt somit als Eingriffsgrundlage ebenfalls nicht in Betracht.

c) § 102 StPO bietet auch keine Rechtsgrundlage zur heimlichen Ausforschung eines Computers. Die Durchsuchung gem. § 102 StPO – ein körperlicher, nicht ein elektronischer Vorgang – ist eine im Grundsatz auf Offenheit angelegte Maßnahme. So darf der „Inhaber" des Gegenstands der Durchsuchung beiwohnen – also auch in Kenntnis des Umstands, dass eine Ermittlungsmaßnahme gegen ihn vollzogen wird (§ 106 Abs. 1 Satz 1 StPO). Ist er abwesend, so sind Zeugen hinzuzuziehen (§ 106 Abs. 1 Satz 2). Dabei kann sich die Einschränkung, „wenn möglich" nicht auf ermittlungstaktischen Erwägungen beziehen, sondern hat tatsächliche Schwierigkeiten im Auge, so etwa bei der überraschend notwendig gewordenen Durchsuchung einer einsamen Hütte im Wald.

Dabei kommt es nicht darauf an, ob es sich bei den Bestimmungen über die Hinzuziehung von Zeugen (vgl. auch § 105 Abs. 2 StPO) und die Pflicht zur unmittelbaren Information des Durchsuchungsbetroffenen um Ordnungsvorschriften handelt oder nicht. Dies ist nur erheblich im Hinblick auf die Rechtsfolgen bei einem Verstoß – Verwertbarkeit der Ergebnisse oder nicht. Auch bei Ordnungsvorschriften steht deren Einhaltung nicht zur beliebigen Disposition der Normadressaten. Eine Maßnahme darf nicht von vornherein darauf abzielen, bei ihrer Umsetzung Ordnungsvorschriften, die Schutzrechte des Betroffenen beinhalten, auf jeden Fall unberücksichtigt zu lassen.

d) Eine entsprechende Anwendung der Vorschriften über die Durchsuchung (§ 102 StPO) kommt nicht in Betracht. Es ist zwar zutreffend, dass technischen Neuerungen durch entsprechende Anpassung der Auslegung auch von strafprozessualen Eingriffsnormen Rechnung zu tragen ist. § 102 bietet jedoch auch bei weitester Auslegung keine Rechtsgrundlage mehr zur heimlichen Computerausforschung. Es bliebe nur eine Analogie. Das Analogieverbot des Art. 103 Abs. 2 GG bzw. des § 1 StGB erfasst im Grundsatz zwar nicht das Strafprozessrecht. Eine Rechtsgrundlage für so schwerwiegende Eingriffe wie die heimliche Ausforschung eines Computers kann gleichwohl nicht im Wege der entsprechenden Anwendung einer anderen Eingriffsnorm gerechtfertigt werden. Dies käme einer Umgehung des Gesetzesvorbe-

halts für Eingriffe in grundrechtlich geschützte Freiheitsrechte gleich. Die notwendige ausdrückliche gesetzliche Ermächtigung hätte dann auch die Höhe der Eingriffsschranken zu bestimmen.

Im Grunde liegt der Zweck der beantragten Maßnahme neben der Verfolgung einer bereits begangenen – und noch andauernden – Straftat (§ ... StGB) im Grunde vorrangig bei der Gefahrenabwehr (Schutz vor ...). Darüber, ob die beantragte Maßnahme aus polizeirechtlicher Sicht gestattet werden kann, hat der Ermittlungsrichter (§ 162 StPO) hier nicht zu befinden.

Anmerkung der Redaktion: Ergänzend führt der Ermittlungsrichter am BGH im Beschl. v. 28.11.2006 – 1 BGs 186/2006 aus, dass der heimliche Zugriff auf Beweismittel mit technischen (elektronischen) Mitteln seine abschließende Grundlage in §§ 100a–100i StPO findet und die beantragte Maßnahme am ehesten dem „großen Lauschangriff" des § 100c StPO entspricht, jedoch eine analoge Anwendung der Norm bei einem grundrechtsrelevanten Eingriff von solch hohem Gewicht nicht in Betracht kommt.

Anmerkung

Der (noch nicht rechtskräftige) Beschluss des Ermittlungsrichters betrifft eine technische Ermittlungs- und Gefahrenabwehrmaßnahme, deren künftige Bedeutung immens sein wird. Angesichts der Flüchtigkeit der Kommunikation über das Internet und der Verfügbarkeit sicherer Verschlüsselungsverfahren für die Übertragungswege ist es vom Standpunkt der Sicherheitsbehörden aus konsequent, unter Zuhilfenahme von Trojanern oder vergleichbarer Software den Inhalt von Computern auszuforschen, die – zumindest zeitweilig – mit dem Internet verbunden sind.

Der BGH hatte sich mit einem Antrag der Generalbundesanwältin auseinanderzusetzen, die – gestützt auf §§ 102, 105 Abs. 1, 94, 98, 169 Abs. 1 Satz 2 StPO – die „Durchsuchung des von dem Beschuldigten ... benutzen Personalcomputers/Laptops" beantragt hatte. Ein anderer Ermittlungsrichter des *BGH* hatte mit Beschluss vom 21.2.2006 – 3 BGs 31/06, n.v.) hierin eine hinreichende Ermächtigungsgrundlage gesehen (ebenso v.a. *Graf*, DRiZ 1999, 281 [285]; *Hofmann*, NStZ 2005, 121 [123 ff.] m.w.N.). Dem tritt der entscheidende Richter des vorliegenden Verfahrens ebenso entgegen wie dem Versuch, die Maßnahme auf andere Normen der Strafprozessordnung zu stützen. Beides ist sowohl inhaltlich wie im Ergebnis überzeugend.

1. Keine Ermächtigungsgrundlage in der StPO

Im Wesentlichen unstreitig dürften die Ausführungen des *Gerichts* zu §§ 152 Abs. 2, 161 Abs. 1 (im Beschluss wohl fälschlich § 163 Abs. 1) StPO und § 100a StPO sein. Eingriffsintensive Ermittlungsmaßnahmen können nicht auf § 161 Abs. 1 StPO gestützt werden (*Meyer-Goßner*, StPO, 49. Aufl. 2006, § 161 Rz. 1). Die Ausforschung kommunizierter Daten auf dem Computer des Empfängers nach Abschluss des Übermittlungsvorgangs ließe sich unter Heranziehung der Mailbox-Entscheidungen des *BGH* (BGH v. 31.7.1995 – 1 BGs 625/95 (2 BJs 94/94-6), CR 1996, 488 = NJW 1997, 1934; v. 14.3.2003 – 2 StR 341/02, CR 2003, 572 = NJW 2003, 2034; zust. *Vassilaki*, JR 2000, 446; abl. *Palm/Roy*, NJW 1996, 1791) ggf. noch unter § 100a StPO fassen, auch wenn hiergegen die neuere Rechtsprechung des BVerfG spricht, wonach in diesem Fall keine Kommunikation mehr vorliegt (BVerfG v. 2.3.2006 – 2 BvR 2099/04, CR 2006, 383 m. Anm. *Störing* = NJW 2006, 976). In jedem Fall kann nicht allein aus der Tatsache, dass ein Computer auch zur Telekommunikation verwendet wird, gefolgert werden, die Ausforschung seines gesamten (Festplatten-)Inhalts sei „Überwachung und Aufzeichnung der Telekommunikation" i.S.v. § 100a StPO (ebenso *Bär*, MMR 1998, 463 [467]; ähnlich *Hofmann*, NStZ 2005, 121 [122 f.]).

Die eigentliche Frage ist folglich die direkte oder analoge (das Analogieverbot gilt im Strafprozessrecht nach h.M. nicht) Anwendung von § 102 StPO. Entscheidendes Argument des *Gerichts* hiergegen ist die aus §§ 105 Abs. 2, 106 f. StPO ableitbare Offenheit der gesetzlich normierten Durchsuchung, die hier nicht möglich ist. Diese Auslegung des Durchsuchungsbegriffs ist nicht etwa „dogmatisch bereits im Ansatz nicht haltbar" (so aber *Hofmann*, NStZ 2005, 121 [124]), sondern im Rahmen der systematischen Auslegung überzeugend: Unabhängig vom Charakter der Normen als Ordnungsvorschriften (BGH, NStZ 1983, 375) und der Möglichkeit einer heimlichen Durchsuchung im Einzelfall zeigt sich an ihrem Wortlaut deutlich, dass der Gesetzgeber vom hergebrachten Bild einer Durchsuchung durch örtlich anwesende Beamte ausging. Zwar ist anerkannt, dass die Auslegung strafprozessualer Normen sich mit dem Wandel der Technik ändern kann. Dies kann aber nicht soweit gehen, dass Maßnahmen eingesetzt werden, für die normierte Schutzvorschriften per se nicht anwendbar sind.

Hierfür – und gegen die analoge Anwendung der Normen – spricht noch ein Weiteres. Die heimliche Ausforschung des gesamten Inhalts eines Computers weist eine außerordentliche Eingriffstiefe auf. Es ist weder zutreffend, dass diese Maßnahme gegenüber der klassischen Durchsuchung milder sei, noch, dass durch sie nicht in die räumlich abgeschottete Privatsphäre der Betroffenen eingegriffen werde (so *Graf*, DRiZ 1999, 281 [285]; *Hofmann*, NStZ 2005, 121 [124]). Heutzutage werden auf privaten und betrieblichen Rechnern elektronische Steuerdaten (für das ELSTER-Verfahren), Kontoführungsinformationen, elektronische Rechnungen, Betriebs- und Geschäftsgeheimnisse, Gesundheitsinformationen (Korrespondenz, Befunde, künftig auch Daten der elektronischen Gesundheitskarte), Einzelverbindungsnachweise über Telekommunikationsvorgänge, E-Mails, wissenschaftliche Texte, private Fotos, Videos, intime Briefe und Tagebücher gespeichert – die Liste ließe sich fortsetzen –, und Mikrofone und Webcams an sie angeschlossen. Der geheime Zugriff auf diese Daten ist so wesentlich, dass eine ausdrückliche gesetzliche Ermächtigungsgrundlage erforderlich ist und der für die Betroffenen unmerkliche Zugriff nicht auf eine Ermächtigungsgrundlage gestützt werden kann, die hierfür erkennbar nicht geschaffen wurde (ebenso *Bär*, MMR 1998, 463 [466 ff.]).

2. Gesetzgeberische Aktivitäten

Als erstes Bundesland hat Nordrhein-Westfalen seinem Landesverfassungsschutz mit Gesetz vom 20.12.2006 (GV. NRW, 620; s.a. die Begründung, LT-Drucks. 14/2211) den „heimlichen Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel" (§ 5 Abs. 2 Nr. 6b VSG NRW) gestattet. Anders als bei anderen heimlichen Maßnahmen ist eine Genehmigung durch die G10-Kommission des Landes nicht erforderlich. Niedersachsen will dem nordrhein-westfälischen Beispiel noch 2007 folgen, während die Bundesregie-

rung angekündigt hat, im Falle einer bestätigenden Entscheidung des 3. Strafsenats des *BGH* (dieser hatte angekündigt, im Januar 2007 über die Beschwerde gegen die vorliegende Entscheidung zu verhandeln) den gesetzgeberischen Handlungsbedarf für eine spezialgesetzliche Regelung in der StPO zu prüfen. Gleichzeitig erprobt das *Bundeskriminalamt*, gestützt auf § 2 Abs. 6 Nr. 3 BKAG, hierzu die technischen Möglichkeiten (s. Antworten der Bundesregierung auf die Kleinen Anfrage der FDP, BT-Drucks. 16/3972, und der Fraktion DIE LINKE, BT-Drucks. 16/3787).

An dieser Stelle kann weder erörtert werden, ob und in welcher Ausprägung die Online-Durchsuchung verfassungsrechtlich zulässig ist, noch, ob es hierfür tatsächlich ein „unabweisbares Bedürfnis" gibt (*Hofmann*, NStZ 2005, 121 [125]) bzw. es „keinen Zweifel geben [kann], dass wir diese Möglichkeit brauchen" (Bundesinnenminister *Schäuble*, *www.heise.de/newsticker/meldung/82962)*. Angesichts der Eingriffstiefe (s.o.) sind jedenfalls materielle und prozessuale Sicherungsmechanismen vorzusehen, um der Rechtsprechung des *BVerfG* zum Kernbereich des Persönlichkeitsrechts (v.a. BVerfGE 109, 279) zu genügen. Ob dies in der nordrhein-westfälischen Regelung gelungen ist, lässt sich mit guten Gründen bezweifeln.

Dr. Gerrit Hornung, LL.M., Universität Kassel.

OLG Frankfurt: Durchsetzung eines Software-Besichtigungsanspruchs im einstweiligen Rechtsschutz

BGB § 809

Leitsatz der Redaktion

Der Besichtigungsanspruch nach § 809 BGB hinsichtlich Software kann auch im Wege der einstweiligen Verfügung geltend gemacht werden. Die Sicherungsverfügung darf jedoch nur anordnen, dass der Antragsgegner die Besichtigung der Datenträger einem vom Gericht bestimmten, zur völligen Verschwiegenheit verpflichteten Sachkundigen zu ermöglichen hat. Dessen bei Gericht zu hinterlegender Bericht steht dem Antragsteller grundsätzlich erst zur Einsichtnahme frei, wenn dieser einen Hauptsachetitel über den Besichtigungsanspruch erlangt hat.

OLG Frankfurt, Beschl. v. 17.1.2006 – 11 W 21/05 (LG Frankfurt/M., Beschl. v. 1.9.2005 – 7 L 07/15)

Aus den Gründen:

Die statthafte und auch im Übrigen zulässige sofortige Beschwerde (§§ 91a Abs. 2, 567 Abs. 1 Nr. 1, 569 ZPO) hat in der Sache teilweise Erfolg. Nachdem die Parteien das Eilverfahren in der Hauptsache übereinstimmend für erledigt erklärt haben, war über die Kosten unter Berücksichtigung des bisherigen Sach- und Streitstands nach billigem Ermessen zu entscheiden (§ 91a ZPO).

1. Die Verfügungsklägerin hat einen Teil der Kosten zu tragen, weil ihr Antrag von Anfang an (teilweise) unbegründet war, soweit sie die Übergabe des Sachverständigenberichts einschließlich der von dem Sachverständigen ermittelten Dateien und/oder des Quellcodes des Programms „..." an sich verlangt hat.

a) Der Besichtigungsanspruch nach § 809 BGB kann auch im Wege der einstweiligen Verfügung geltend gemacht werden (Palandt/Sprau, BGB, 65. Aufl., § 809, Rz. 13 m.w.N.). Dabei ist jedoch zu berücksichtigen, dass die einstweilige Verfügung nur zur Sicherung, nicht zur Befriedigung des Hauptanspruchs führen darf. Das Gericht darf daher nicht aussprechen, dass der Antragsgegner die zu besichtigenden Datenträger dem Antragsteller persönlich zugänglich machen muss oder ein Dritter seine bei der Besichtigung gewonnenen Erkenntnisse und Feststellungen an den Antragsteller weitergeben darf. Vielmehr darf die Sicherungsverfügung nur anordnen, dass der Antragsgegner die Besichtigung der Datenträger einem vom Gericht bestimmten, zur völligen Verschwiegen verpflichteten Sachkundigen zu ermöglichen hat. Der Sachkundige hat seinen Bericht bei Gericht zu hinterlegen. Er steht dem Antragsteller grundsätzlich erst zur Einsichtnahme frei, wenn dieser einen Hauptsachetitel über den Besichtigungsanspruch aus § 809 BGB erlangt hat (Bork, NJW 1997, 1665 [1671]; wohl auch KG v. 11.8.2000 – 5 U 3069/90, NJW 2001, 233).

b) Dieser Auffassung folgt der Senat. Die Vorwegnahme der Hauptsache im Eilverfahren lässt sich nicht allein mit Praktikabilitätserwägungen rechtfertigen. Es ist auch nicht ersichtlich, warum die Offenbarung der Ergebnisse der Besichtigung (erst) nach Abschluss des Berufungsverfahrens – unter Umständen erst nach Abschluss des Hauptsacheverfahrens nach § 809 BGB – dem Sinn des § 809 BGB im Eilverfahren zuwider laufen würde. Die Durchsetzung eines Besichtigungsanspruchs im Wege der Hauptsacheklage ist der Regelfall, unter besonderen Umständen kommt die vorläufige Sicherung dieses Anspruchs im Wege der einstweiligen Verfügung in Betracht. Zur vorläufigen Sicherung des Besichtigungsanspruchs, über den endgültig erst im Hauptsacheverfahren zu entscheiden ist, wird in aller Regel aber die sachkundige Besichtigung und die Hinterlegung der sachkundigen Feststellungen bei Gericht ausreichen, um die Gefahr einer nachträglichen Veränderung auszuschließen. Dann aber entspricht es dem Zweck und vorläufigen Charakter einer einstweiligen Verfügung, (nur) diejenigen Maßnahmen anzuordnen, die eine Veränderung des bestehenden Zustands und eine dadurch bedingte Vereitelung des Rechts des Anspruchsstellers verhindern sollen (§ 935 ZPO). Auch wenn gelegentlich im Schrifttum Bedenken wegen der befürchteten Langwierigkeit des Verfahrens erhoben werden (vgl. etwa Tilmann/Schreibauer, GRUR 2002, 1015; Brandi/Dohrn, CR 1987, 835; a.A. aber die bei Bork, a.a.O., Fn. 79 angeführten Nachweise) besteht kein Anlass, bei der Durchsetzung eines Besichtigungsanspruchs im Wege der einstweiligen Verfügung andere Maßstäbe anzusetzen als bei sonstigen Eilverfahren. Dies rechtfertigt sich insb. nicht mit der Erwägung, der Besichtigungsanspruch sei bloßer Hilfsanspruch zum nachfolgenden Verletzungsprozess, weil daraus nicht die Zulässigkeit der Vorwegnahme der Erfüllung des Hilfsanspruchs im Wege der einstweiligen Verfügung folgt (so aber wohl Tilmann/Schreibauer a.a.O.).

Diese Ansicht wird auch dem Erfordernis des Art. 50 Abs. 1 des TRIPS-Abkommens gerecht, schnelle wirksame Maßnahmen zur Verhinderung von Verletzungen des Rechts am geistigen Eigentum zu schaffen. Auf die entsprechenden Ausführungen im Urteil des KG und von Bork (jeweils a.a.O.) wird verwiesen (a.A. wohl Tilmann/Schreibauer a.a.O.).

Selbst wenn die Herausgabe zu beschleunigen wäre, könnte dies allenfalls dazu führen, dass dies am Ende des