Max-Planck-Institut
für ausländisches und
internationales Strafrecht

Pressemitteilung

Stellungnahme zur „Online-Durchsuchung"

- Max-Planck-Direktor als Gutachter vor dem Bundesverfassungsgericht
- Online-Durchsuchungen können in Einzelfällen wichtige Beiträge für laufende Ermittlungen leisten
- Umfassende Sicherungen für den Einsatz notwendig

Sperrfrist: 10.10.2007 13:00

In der Verhandlung des Bundesverfassungsgerichts am Mittwoch, den 10.10.2007 zur umstrittenen Online-Durchsuchung (Az. 1 BvR 370/07) wird Prof. Dr. Dr. h.c. *Ulrich Sieber*, Direktor am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg i. Br., als Gutachter aussagen. In seinem schriftlichen Gutachten für das Gericht erläutert Sieber, dass das Internet nicht nur zur Begehung von computerspezifischen Delikten (z.B. Hacking), sondern auch zur Kommunikation zwischen Straftätern bei sonstigen Kriminalitätsformen genutzt werde. Die Bandbreite der Täter reiche „vom Eierdieb bis zum Terroristen", so Sieber.

In seiner Stellungnahme plädiert Sieber für eine stärkere Differenzierung zwischen der einmaligen *Online-Durchsuchung* und einer fortdauernden *Online-Überwachung*. Die – meist einmalig durchgeführte – Online-*Durchsuchung* ermittle die auf einem System gespeicherten Daten und entspreche daher insoweit einer klassischen Durchsuchung, wobei aber heimlich gearbeitet werde. Mit Hilfe der – sehr viel eingriffsintensiveren – Online-*Überwachung* sei es darüber hinausgehend auch möglich, die laufenden Aktivitäten eines Nutzers zu registrieren und zu protokollieren, zum Beispiel Tastatureingaben, Zugriffe auf Webseiten sowie Telefongespräche, die über das Internet geführt würden.

Beide Maßnahmen – besonders aber die Online-*Überwachung* – greifen nach Siebers Auffassung sehr weitgehend in die Privatsphäre der Betroffenen ein: Auf Computersystemen seien heute ein Vielzahl von persönlichen Daten gespeichert, auch aus dem Kernbereich der privaten Lebensführung. Bei einer fehlenden rechtlichen Begrenzung könnten auch angeschlossene Mikrofone und Web-Kameras heimlich eingeschaltet und zur Raumüberwachung genutzt werden. Weiterhin sei zu beachten, dass Online-Zugriffe nicht nur bei stationären Rechnern oder Notebooks eingesetzt werden könnten, sondern z.B. auch bei Organizern, Mobiltelefonen und Smartphones. Diese wären millionenfach verbreitet und spielten eine immer wichtigere Rolle im Alltagsleben vieler Nutzer.

Für die Ermittlungsbehörden seien Online-Zugriffe wegen technischer Schwierigkeiten und des zum Teil erheblichen Aufwandes „sicher kein Königsweg". So könnten sich Betroffene grundsätzlich gegen beinahe jede denkbare Angriffsart technisch schützen. Dennoch könne man Online-Zugriffe nicht generell als wenig aussichtsreich bezeichnen: „Auch das Hinterlassen von Fingerabdrücken kann man vermeiden, indem man bei der Tatbegehung Handschuhe trägt. Dennoch werden jedes Jahr viele Täter anhand ihrer Abdrücke identifiziert." Sowohl die kriminalistische Erfah-

Referat Presse & Öffentlichkeitsarbeit

Phillip W. Brunst

Tel. +49 (761) 7081-256
Fax +49 (761) 7081-294
p.brunst@mpicc.de

Sekretariat Prof. Sieber

Martina Hog

Tel. +49 (761) 7081-203
Fax +49 (761) 7081-309
m.hog@mpicc.de

rung als auch Erkenntnisse aus dem Umgang mit Sicherheitsmaßnahmen in der Industrie zeigten, dass technische Sicherungen häufig nicht konsequent durchgehalten werden. „In Einzelfällen kann der Online-Zugriff daher sicherlich wichtige Bausteine für die Ermittlungsarbeit liefern“, so Sieber. Dies sei insbesondere dann der Fall, wenn Informationen erlangt werden müssten, ohne dass der Betroffene dabei gewarnt werde oder er die Gelegenheit zur Vernichtung von Beweisen erhalte. Auch könnten Ermittler in den Besitz von Kryptoschlüsseln und Passwörtern gelangen, mit denen Straftäter ihre Kommunikationsinhalte oder sonstige Daten sichern oder Erkenntnisse über Online-Verstecke für weitere Daten gewinnen. Derartige Kenntnisse könnten zum Beispiel für die Verhinderung und Verfolgung von terroristischen Straftaten erhebliche Bedeutung haben.

Zwar böten Online-Zugriffe erhebliche Probleme und Risiken. So sei es fraglich, inwiefern die gewonnenen Informationen zum Beweis in einer gerichtlichen Hauptverhandlung geeignet oder lediglich ein Instrument zum Auffinden neuer Ermittlungsansätze seien. Weiterhin ließen sich vielfältige Umgehungsmöglichkeiten und Gefahren von Beweismittelveränderungen andenken. „Diese Missbrauchsmöglichkeiten sind qualitativ aber nichts Neues“ stellt der Max-Planck-Direktor fest. Ein Missbrauch von Beweismitteln sei theoretisch auch in anderen Bereichen möglich, z.B. durch das Hinzufügen von DNS-Spurenträgern. Auch ermöglichten einige existierende Maßnahmen bereits den Zugriff auf eine Vielzahl von intimen Daten, z.B. im Rahmen der Wohnraumüberwachung. Man müsse daher vor allem die im Straf- und Sicherheitsrecht entwickelten Sicherungsmaßnahmen aufgreifen, anwenden und weiterentwickeln. Sieber fordert daher, dass die folgenden Einschränkungen im Hinblick auf die Zulassung von Online-Zugriffen geprüft werden sollten:

- Eine **gesetzliche Unterscheidung** in der Eingriffsnorm zwischen Online-Durchsuchungen einerseits und Online-Überwachungen andererseits (sowie ggf. den – beide Kategorien betreffenden – Spezialfall der Quellen-Telekommunikationsüberwachung);
- Eine Begrenzung von Überwachungsmaßnahmen auf eine **bestimmte Dauer**;
- Eine **Begrenzung des Anwendungsbereichs** der Eingriffsnorm auf Fälle einer Gefahr besonderer Schwere oder Erheblichkeit und/oder einen bestimmten Verdachtsgrad (der z.B. durch konkrete Tatsache belegt sein müsse);
- Eine **Anordnungsbefugnis** nur durch den Richter sowie ggf. bei Eingriffen in den Wohnbereich und bei Online-Überwachung durch ein aus drei Richtern bestehendes Richterkollegium;
- Eine Möglichkeit zur richterlichen **Beschränkung auf bestimmte Datenarten** (z.B. nur Zugriffe auf E-Mail, Internet-Telefonie oder Kryptoschlüssel);
- Besondere Anforderungen an die Personen, die mit der **Durchsicht** der durch die Maßnahme erlangten Daten betraut sind;
- Eine Verpflichtung zur (nachträglichen) **Benachrichtigung des Betroffenen** und für den Fall einer Nichtbenachrichtigung aus ermittlungstaktischen Gründen die Prüfung der Maßnahme durch einen Ombudsmann (entsprechend den Vorbildern in ausländischen Rechtsordnungen);
- Eine gesetzliche Regelung von **Beweiserhebungs- und Beweisverwertungsverboten**, die sich auf die Daten von Berufsgeheimnisträgern (etwa Ärzte oder Rechtsanwälte) und auf Daten im Kernbereich von Grundrechten beziehen;
- Eine nachträgliche **Kontrolle von Maßnahmen**, zum Beispiel durch Begründungs- und Berichtspflichten der verantwortlichen Personen, Vorschriften zur Protokollierung und Dokumentation, Pflicht zur Hinzuziehung von Zeugen, Kontrollmöglichkeiten durch unabhängige Dritte (z.B. Parlamentsabgeordnete, Datenschützer oder spezielle Ombudspersonen).

Insgesamt sei festzustellen, dass die moderne Informationstechnik nicht nur neue Möglichkeiten für Kriminelle, sondern auch ein beträchtliches Überwachungspotential ermögliche, das Freiheitsrechte gefährde. Das Verfassungsrecht und die Kriminalpolitik müssten diese neuen informationstechnischen Ermittlungsmaßnahmen durch den präzisen Einsatz herkömmlicher und neuer rechtsstaatlicher Ausgleichsmechanismen auf die richtigen Verdachts- und Gefahrenkonstellationen begrenzen. Dies gelte nicht nur für Online-Zugriffe, sondern auch für andere Maßnahmen, wie z.B. die Vorratsdatenspeicherung von Telekommunikationsdaten. Die Politik sei deswegen gut beraten, wenn sie sich nicht auf die politische Kontroverse für oder gegen derartige Maßnahmen beschränke, sondern stattdessen eine sorgfältige Analyse von Nutzen, Gefahren und möglichen Ausgleichsmechanismen vornehme.

Prof. Dr. Dr. h.c. Ulrich Sieber ist Direktor am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg i. Br. Seine Interessen- und Forschungsschwerpunkte liegen auf den Gebieten des Informationsrecht und der Rechtsinformatik, der Strafrechtsvergleichung, dem Europäischen Strafrecht, dem internationalen Strafrecht, der organisierten Kriminalität, der Wirtschaftskriminalität und dem Terrorismus. Weitere Informationen über Prof. Sieber: http://www.mpicc.de/ww/de/pub/home/sieber.htm
Das **Gutachten** ist ab 13 Uhr abrufbar: http://www.mpicc.de/ww/de/ext/aktuelles/pressematerialien/pressemitteilungen.htm