



POSTANSCHRIFT Bundesministerium der Justiz, 11015 Berlin

An die
Landesjustizverwaltungen

nachrichtlich:

a) An das
Bundesministerium des Innern
- Arbeitsgruppe ÖS I 3 -
[REDACTED]

b) An den
Generalbundesanwalt

c) An den
Bundesbeauftragten
für den Datenschutz und die
Informationsfreiheit

HAUSANSCHRIFT Mohrenstraße 37, 10117 Berlin
POSTANSCHRIFT 11015 Berlin

BEARBEITET VON [REDACTED]
REFERAT R B 3
TEL (030) 18 580 - 96 [REDACTED]
FAX (030) 18 580 - 9525
E-MAIL poststelle@bmj.bund.de
AKTENZEICHEN R B 3 - zu 4104/8 - 1 - R5 39/2008
DATUM Berlin, 2. Februar 2009

BETREFF: Homepageüberwachung

HIER: Maßnahmen des Bundeskriminalamtes im Rahmen von strafrechtlichen Ermittlungsverfahren der Länder

Das Bundeskriminalamt (BKA) betreibt eine Internetseite (www.bka.de), auf der u. a. Fahndungsausschreibungen eingestellt werden. Hierbei wird das BKA nicht nur in eigener Sache, sondern auch für Ermittlungsbehörden der Länder tätig. Gegenwärtig ist dies – soweit zugleich eine Homepageüberwachung erfolgt – in 16 Verfahren der Fall (vgl. beigefügte tabellarische Aufstellung). Bei der Homepageüberwachung werden mit technischen Maßnahmen (u. a. sogenannten Cookies¹ und Web Bugs²) bei ausgewählten Fahndungsseiten die

¹ Ein **Cookie** ist ein kleines Programm, das bei dem Besuch einer Webseite von dieser auf dem Rechner des Besuchers gespeichert wird und bei erneuten Besuchen derselben Webseite "Meldung macht", dass es sich um denselben Computer handelt.

² **Web Bugs** sind winzige GIFs (**Graphics Interchange Format** = Grafikaustausch-Format, ein Grafikformat mit Komprimierung für Bilder) mit einer Größe von normalerweise 1x1 Pixel, die auch in anderen Grafiken versteckt werden können und von dem Besucher der Internetseite nur bei Einsatz entsprechender Zusatzprogramme wahrgenommen werden können. Ein solcher Web Bug sendet in der Regel die IP-Adresse des Nutzers, die URL (**Uniform Resource Locator**) der besuchten Webseite (z. B. www.bka.de), die URL des Web Bug GIFs, den Zeitpunkt, an dem der Web Bug „angeschaut“ wurde, den vom Nutzer eingesetzten Browsertyp (z. B. Internet Explorer) sowie die Informationen eines zuvor gesetzten Cookies an einen Server des Webseitenbetreibers.

Zugriffe von Internetnutzern in einer Weise registriert, die Schlüsse darauf zulässt, ob von einem bestimmten Computer oder Anschluss aus auffällig oft eine bestimmte Fahndungsmeldung abgerufen wurde (= sog. Homepageüberwachung). Durch die dabei erfolgende Registrierung der zugreifenden IP-Adresse und die sich anschließende Bestandsdatenauskunft nach den §§ 161, 163 StPO i. V. m. § 113 TKG können Name und Anschrift des jeweiligen Anschlussinhaber ermittelt werden. Dahinter steht die Annahme, dass insbesondere die gesuchte Person an Informationen über die Fahndung nach ihr interessiert ist und deshalb die sie betreffende Fahndungsseite wiederholt aufrufen wird, so dass die Registrierung dieser Vorgänge zum Auffinden der Person beitragen kann.

Das Bundesministerium des Innern und das Bundesministerium der Justiz haben Fragen der Zulässigkeit der Homepageüberwachung geprüft und sind hierbei zu dem Ergebnis gelangt, dass die Homepageüberwachung durchgreifenden Bedenken begegnet. Die wesentlichen Gesichtspunkte hierbei sind:

- Die Homepageüberwachung führt zu einer Speicherung und Verwendung personenbezogener und damit personenbezogener Daten im Sinne des § 3 Abs. 1 BDSG, mithin zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der dem Gesetzesvorbehalt unterliegt. Darüber hinaus erscheint auch das durch Art. 5 Abs. 2 Satz 1 GG geschützte Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten, beeinträchtigt.
- Der Umstand, dass bei der Homepageüberwachung eine große Anzahl von Daten - sämtliche Internetzugriffe auf eine bestimmte Seiten der Homepage - erhoben, gespeichert und ausgewertet werden, lässt eine spezielle Befugnisnorm für dieses Vorgehen erforderlich erscheinen. Eine solche ist indessen nicht ersichtlich. Allenfalls könnte eine Anwendbarkeit der §§ 100a, 100b und 100g StPO in Erwägung gezogen werden. In den bislang bekannt gewordenen Fällen mangelte es aber schon an einer entsprechenden gerichtlichen Anordnung (§ 100b Abs. 1 StPO). Ohne etwaigen gerichtlichen Entscheidungen zu dieser Frage vorgreifen zu wollen, erscheint es auch zweifelhaft, ob diese Regelungen eine - gegenüber einer gewöhnliche Telekommunikationsüberwachung anders geartete - Homepageüberwachung rechtfertigen können (BKA als Nachrichtenmittler im Sinne von § 100a Abs. 3 StPO? Einsatz technischer Mittel, wie Cookies und Web Bugs, von TKÜ-Befugnis umfasst? Verhältnismäßigkeit?).
- Die allgemeinen Befugnisse nach den §§ 161, 163 StPO bieten lediglich für solche Ermittlungshandlungen, die weniger intensiv in Grundrechte eingreifen, eine geeignete Rechtsgrundlage. Aus grundrechtlicher Sicht können diese Ermittlungsgeneralklauseln nicht die Speicherung einer großen Anzahl von - auch durch Artikel 5 Abs. 1 Satz 1

GG geschützten - Daten erlauben, die bei den Zugriffen auf eine Homepage an den Homepagebetreiber übermittelt werden, um diese Daten als Ermittlungsansatz verwenden zu können. Es bedürfte, wie bereits ausgeführt, einer spezialgesetzlichen Norm, die – im Hinblick auf das Grundrecht, sich aus allgemein zugänglichen Quellen ungehindert unterrichten zu dürfen - zudem den Voraussetzungen des Artikels 5 Abs. 2 GG genügen müsste.

Selbst wenn man aber die §§ 161, 163 StPO hinsichtlich der Homepageüberwachung als in Betracht kommende Befugnisnormen ansehen wollte, könnten diese die Homepageüberwachung im Ergebnis nicht rechtfertigen. Denn § 160 Abs. 4 StPO bestimmt, dass eine (strafprozessuale) Maßnahme unzulässig ist, soweit besondere gesetzliche Verwendungsregelungen, entgegenstehen. Solche entgegenstehenden Verwendungsregelungen finden sich im Telemediengesetz (TMG):

Das Betreiben der (Fahndungs)Webseite ist ein Telemediendienst im Sinne des § 1 Abs. 1 TMG. Nach § 15 Abs. 1 Satz 1 TMG dürfen personenbezogene Daten eines Nutzers (Nutzungsdaten) nur erhoben und gespeichert werden, soweit dies erforderlich ist, um die Inanspruchnahme des Telemediendienstes zu ermöglichen und abzurechnen. Nutzungsdaten sind nach § 15 Abs. 1 Satz 2 TMG insbesondere Merkmale zur Identifikation des Nutzers, wie z. B. die IP-Adresse, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung (Zeitpunkte des Besuchs der Fahndungswebseite) und Angaben über die vom Nutzer in Anspruch genommenen Telemedien (Fahndungsseite).

Zur Inanspruchnahme des Dienstes müssen diese Daten vorliegend nicht über den Zeitraum der Inanspruchnahme (Besuch der Webseite) hinaus gespeichert oder verwendet werden. Auch eine Abrechnung im Sinne des § 15 Abs. 1 Satz 1 TMG kommt bei unentgeltlich betriebenen Fahndungswebseiten nicht in Betracht. Da auch eine nach § 12 TMG grundsätzlich mögliche, nach § 13 TMG indessen an mehrere Voraussetzungen geknüpfte Einwilligung der Nutzer in die Erhebung und Verwendung der Daten regelmäßig nicht vorliegen wird, ist die Verwendung der vorgenannten Daten gemäß § 15 Abs. 4 TMG über das Ende des Nutzungsvorgangs hinaus nicht zulässig.

Aufgrund dieser rechtlichen Überlegungen veranlasst der Generalbundesanwalt keine Maßnahmen zur Homepageüberwachung.

Das Bundesministerium des Innern hat parallel zu diesem Schreiben das Bundeskriminalamt über die vorstehenden rechtlichen Gesichtspunkte informiert und das Unterlassen von Maßnahmen zur Homepageüberwachung veranlasst.

Ich rege an, dass Sie die Strafverfolgungsbehörden in Ihrem Zuständigkeitsbereich entsprechend unterrichten.

Im Auftrag



Beglaubigt



Tarifbeschäftigte

