Online-Durchsuchung – (grund-)rechtliche Überlegungen

Christian Bergauer

Karl-Franzens-Universität Graz
Institut für Rechtsphilosophie, Rechtssoziologie und Rechtsinformatik
Universitätsstraße 15, 8010 Graz
christian.bergauer@uni-graz.at

Schlagworte: Ermittlungsmaßnahmen, StPO, Bundestrojaner, Art. 8 EMRK, Art. 10a StGG, § 1 DSG

Abstract: Voraussichtlich wird die „Online-Durchsuchung" als neue Ermittlungsmaßnahme in die österreichische Strafprozessordnung Einzug halten. Dabei sollen Computersysteme verdeckt durchsucht, aber auch Kommunikationsvorgänge innerhalb von Computersystemen besser überwacht werden können. Aktuell wird heftig über die Durchführung von Online-Durchsuchungen durch die Verwendung von sog. „Polizei- bzw. Bundestrojanern" diskutiert. Doch welche (grund-)rechtlichen Schranken müssen bei derartigen Maßnahmen beachtet werden?

1. Gesetzgeberisches Vorhaben

Der Ministerrat hat sich im Oktober letzten Jahres darauf geeinigt, dass in Zukunft eine Online-Durchsuchung von Computersystemen als Ermittlungsmaßnahme in die Strafprozessordnung Eingang finden soll. Dabei sollen Strafverfolgungsbehörden unbemerkt IT-Systeme von Verdächtigen durchsuchen dürfen. Zudem soll die gesamte Kommunikation, sämtliche Benutzereingaben und der gesamte Datenbestand der IT-Systeme verdächtiger Personen besser überwacht bzw. durchsucht werden. Aller Voraussicht nach soll die Einführung dieser neuen Ermittlungsmaßnahme bis Herbst 2008 erfolgen.

2 Staatliche Eingriffe in Grundrechte

Die Durchführung einer derartigen Ermittlungsmaßnahme greift in mehrere Grundrechte von verschiedenen Betroffenen ein. Dabei handelt es sich jedenfalls um das Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK), das Fernmeldegeheimnis (Art. 10a StGG) und das Grundrecht auf Datenschutz (§ 1 DSG).

2.1 Recht auf Achtung des Privat- und Familienlebens

Staatliche Eingriffe in die Schutzbereiche des Art. 8 EMRK wie z. B. die Achtung des Privatlebens und der Korrespondenz sind nur dann gerechtfertigt, wenn die Maßnahme gesetzlich vorgesehen, klar und präzise formuliert ist, einem legitimen Ziel wie etwa dem Schutz der nationalen und öffentlichen Sicherheit, der Verhütung von Straftaten usw. dient und die Erreichung des Ziels notwendig und verhältnismäßig ist. Art. 8 EMRK enthält aber keinen ausdrücklichen Richtervorbehalt.[1]

2.2 Fernmeldegeheimnis

Staatliche Eingriffe in Art. 10a StGG sind nur auf Grund eines richterlichen Befehls nach Maßgabe von gesetzlichen Ermächtigungen zulässig. Der Schutzbereich des Art. 10a StGG umfasst jedenfalls „Inhaltsdaten", also gedankliche Mitteilungen. Auch gehen die strafrechtliche Literatur und Judikatur davon aus, dass ebenso „Verkehrsdaten", also „äußere Mitteilungsdaten" (wie Informationen über die Teilnehmerkennung, Übertragungsprotokolle usw.), von Art. 10a StGG erfasst werden.[2]

2.3 Grundrecht auf Datenschutz

Staatliche Eingriffe in das Grundrecht auf Datenschutz (§ 1 DSG 2000) müssen sich an den Schranken des Art. 8 EMRK orientieren. Der Gesetzgeber ist auch hier an den materiellen Gesetzesvorbehalt des Art. 8 Abs. 2 EMRK

1 *Grabenwarter*, Europäische Menschenrechtskonvention (2003) 201 ff.; siehe auch *Reindl*, WK-StPO Vor. §§ 149a – c Rz. 4 ff.

2 *Reindl*, WK-StPO Vor §§ 149a – c Rz. 9 m. w. N.

gebunden.[3] Das Grundrecht auf Datenschutz garantiert einen Anspruch auf Geheimhaltung von personenbezogenen Daten, sofern ein schutzwürdiges Geheimhaltungsinteresse daran besteht. Unter personenbezogenen Daten werden gem. § 4 Z 1 DSG alle Daten über Betroffene verstanden, deren Identität zumindest indirekt bestimmt bzw. bestimmbar ist. „Indirekt personenbezogene Daten" sind Daten, die vom konkreten Verwender nur mit rechtlich unzulässigen Mitteln auf eine Person zurückgeführt werden können, z. B. wenn Daten einer Person nicht unter ihrem Namen, sondern unter einer Nummer gespeichert werden, die nur derjenige auf den Namen rückführen kann, der rechtmäßig im Besitz des Namens und der dazugehörenden Nummer ist (z. B. KFZ-Kennzeichen). Anonymisierte Daten, die keiner Person zuordenbar sind, fallen nicht in den Schutzbereich des Datenschutzgesetzes.[4]

3. Möglicher Gesetzesentwurf

Die sinngemäße Anwendung der derzeit möglichen in der StPO[5] normierten und in Rechte von Personen eingreifenden Ermittlungsmaßnahmen kommt für eine Online-Durchsuchung nicht infrage, da jedenfalls eine explizite gesetzliche Ermächtigung bestehen muss.[6]

Hinsichtlich der Eingriffszulässigkeitsvoraussetzungen wird sich der Gesetzgeber an der rechtlichen Ausgestaltung des großen Lauschangriffs und des großen automationsunterstützten Datenabgleichs (Rasterfahndung) orientieren können. Danach darf eine Online-Durchsuchung lediglich zur Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder eines Verbrechens nach § 278a oder § 278b StGB[7] (kriminelle Organisation bzw. terroristische Vereinigung) genehmigt werden, sofern das zu durchsuchende IT-System einer „dringend" tatverdächtigen Person zuordenbar ist. Zu diesen materiellen Voraussetzungen müsste, um dem Fernmeldegeheimnisschutz Rechnung zu tragen, die Maßnahme unter Richtervorbehalt stehen, d. h. die Ermittlungsmaßnahme selbst kann von

3 *Jahnel*, Datenschutzrecht, in *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] (2003) 241 ff.

4 *Jahnel*, a. a. O.

5 Strafprozessordnung 1975, BGBl 1975/631 (WV) i.d.F. BGBl I 2007/109.

6 *Babek*, Ermittlungsmaßnahmen – Aufgaben und Befugnisse von Kriminalpolizei und Staatsanwaltschaft StPO-neu Teil IV, ÖJZ 2008/17.

7 Strafgesetzbuch 1975, BGBl 1974/60 i.d.F. BGBl I 2007/112.

der Staatsanwaltschaft angeordnet werden, bedarf aber einer gerichtlichen Genehmigung[8] (i. S. d. § 137 Abs. 1 StPO). Im Wege einer Online-Durchsuchung werden in erster Linie Daten heimlich durchsucht, die auf dem Computersystem gespeichert sind. Dies unterscheidet sich grundsätzlich von einer Online-Überwachung, bei der die bestehende gesetzliche Eingriffsermächtigung bezüglich eines „Lauschangriffs" i. d. R. ausreichend wäre. Deshalb sollte als erhöhter Schutz vor Fehlentscheidungen die Genehmigungsbefugnis einer Online-Durchsuchung jedenfalls einem „Drei-Richter-Senat" obliegen.

Zur umfassenden Kontrolle einer Online-Durchsuchung müsste – wie auch schon jetzt bei den Ermittlungsmaßnahmen nach § 147 Abs. 1 Z. 1 bis 5 StPO – der Rechtsschutzbeauftragte ermächtigt werden. Und hinsichtlich der Verwendung (Verarbeitung und Übermittlung) einer relativ hohen Anzahl von personenbezogenen Daten unterschiedlichster Betroffener wäre auch eine Beschwerdelegitimation der Datenschutzkommission – wie etwa bei der Rasterfahndung – sinnvoll (i. S. d. § 142 Abs. 4 StPO). Denn nur hinreichende gesetzliche Determinierung und effektive öffentliche Kontrollmechanismen bilden angemessene und wirkungsvolle Garantien gegen Missbräuche der staatlichen Datenermittlungsbefugnisse.

4. Zusammenfassung

Die gesetzliche Ausgestaltung der neuen Ermittlungsmaßnahme „Online-Durchsuchung" wird sich aus (grund-)rechtlicher Sicht durchaus realisieren lassen. Wichtig dabei ist die Beachtung der Rechtfertigungsvoraussetzungen für Eingriffe in das Grundrecht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK), in das Fernmeldegeheimnis (Art. 10a StGG) und in das Grundrecht auf Datenschutz (§ 1 DSG 2000).

Viel problematischer wird sich vermutlich die technische Durchführbarkeit der neuen Ermittlungsmaßnahme in der Praxis darstellen.

8 Zum Problem „richterliche Bewilligung" statt „richterlichem Befehl" in Anbetracht des Fernmeldegeheimnisses (Art. 10a StGG) siehe *Reindl*, Die neue Stellung des Gerichts im Ermittlungsverfahren, JAP 2005/2006/1.

5. Literatur

Babek: Ermittlungsmaßnahmen – Aufgaben und Befugnisse von Kriminalpolizei und Staatsanwaltschaft StPO-neu Teil IV, ÖJZ 2008/17.

Fuchs/Ratz (Hrsg.): Wiener Kommentar zur Strafprozessordnung (2003).

Grabenwarter: Europäische Menschenrechtskonvention (2003).

Jahnel/Schramm/Staudegger (Hrsg.): Informatikrecht[2] (2003).

Reindl: Die neue Stellung des Gerichts im Ermittlungsverfahren, JAP 2005/2006/1.