Pressemitteilungen

Bundesverfassungsgericht - Pressestelle -

Pressemitteilung Nr. 79/2009 vom 15. Juli 2009

Beschluss vom 16. Juni 2009 - 2 BvR 902/06 -

Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers nicht verfassungswidrig

---

Der Zweite Senat des Bundesverfassungsgerichts hat eine Verfassungsbeschwerde zurückgewiesen, die sich gegen die Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers wendete. Zwar greifen diese Maßnahmen in das verfassungsrechtlich gewährleistete Fernmeldegeheimnis aus Art. 10 Abs. 1 GG ein. Die allgemeinen strafprozessualen Vorschriften der §§ 94 ff. StPO rechtfertigen jedoch diesen Eingriff in das Fernmeldegeheimnis, wenn dem Grundsatz der Verhältnismäßigkeit und den sachlichen Erfordernissen einer entsprechenden Ausgestaltung des strafprozessualen Verfahrens Rechnung getragen wird.

Der Verfassungsbeschwerde lag folgender Sachverhalt zugrunde:

Das Amtsgericht ordnete in einem Ermittlungsverfahren gegen Dritte wegen Betrugs und Untreue die Durchsuchung der Wohnung des Beschwerdeführers an, um dort Unterlagen und Datenträger, insbesondere Textdateien und E-Mails aufzufinden, die als Beweismittel in Betracht kamen. Der Beschwerdeführer hatte sein E-Mail-Programm so eingestellt, dass seine E-Mails nicht standardmäßig auf seinen lokalen Rechner übertragen wurden, sondern auch nach dem Abruf in einem zugangsgesicherten Bereich auf dem Mailserver seines Providers gespeichert blieben. Die E-Mails konnten von dem PC des Beschwerdeführers nur abgerufen werden, indem eine Internetverbindung hergestellt wurde. Bei der Durchsuchung seiner Wohnung wies der Beschwerdeführer die Ermittlungspersonen auf diese Sachlage hin. Er verwahrte sich aber gegen einen Zugriff auf die E-Mails, weil der Durchsuchungsbeschluss dies nicht zulasse.

Das Amtsgericht ordnete daraufhin die Beschlagnahme der Daten auf dem E-Mail-Account des Beschwerdeführers bei seinem Provider an. Der Beschwerdeführer wusste von diesem Beschluss, der fernmündlich von der Staatsanwaltschaft aus seinen Räumen beantragt und vom Amtsgericht dorthin übermittelt worden war. Am selben Tag wurden beim Provider die gesamten etwa 2.500 E-Mails des Beschwerdeführers, die seit Januar 2004 bis März 2006 auf dem Mailserver gespeichert worden waren, auf einen Datenträger kopiert und den Ermittlungsbehörden übergeben. Die Beschwerde dagegen blieb ohne Erfolg. Auf einen Eilantrag des Beschwerdeführers wies die 3. Kammer des Zweiten Senats des Bundesverfassungsgerichts im Wege einer einstweiligen Anordnung das Amtsgericht an, im Einzelnen bezeichnete Datenträger, Ausdrucke und Schriftstücke zu versiegeln und in Verwahrung zu nehmen.

Der Zweite Senat des Bundesverfassungsgerichts wies die Verfassungsbeschwerde nunmehr zurück und entschied, dass die

angegriffenen Entscheidungen den verfassungsrechtlichen Vorgaben für den damit verbundenen Eingriff in Art. 10 Abs. 1 GG genügen, so dass der Beschwerdeführer durch die Sicherstellung der E-Mails auf dem Server des Providers nicht in seinen Grundrechten verletzt ist.

Der Entscheidung liegen im Wesentlichen folgende Erwägungen zu Grunde:

Der zugangsgesicherte Kommunikationsinhalt in einem E Mail-Postfach, auf das der Nutzer nur über eine Internetverbindung zugreifen kann, ist durch das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) geschützt. Der Kommunikationsteilnehmer hat keine technische Möglichkeit, die Weitergabe der E-Mails durch den Provider an Dritte zu verhindern. Dieser technisch bedingte Mangel an Beherrschbarkeit begründet die besondere Schutzbedürftigkeit durch das Fernmeldegeheimnis, welches jenen Gefahren für die Vertraulichkeit begegnen will, die sich aus der Verwendung eines Kommunikationsmediums ergeben, das einem staatlichem Zugriff leichter ausgesetzt ist als die direkte Kommunikation unter Anwesenden. Dies gilt unabhängig davon, ob eine E-Mail auf dem Mailserver des Providers zwischen- oder endgespeichert ist. Dem Schutz durch Art. 10 Abs. 1 GG steht nicht entgegen, dass während der Zeitspanne, während deren die E-Mails auf dem Mailserver des Providers „ruhen", ein Telekommunikationsvorgang in einem dynamischen Sinne nicht stattfindet. Art. 10 Abs. 1 GG folgt nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes, sondern knüpft an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an. Die spezifische Gefährdungslage und der Zweck der Freiheitsverbürgung von Art. 10 Abs. 1 GG bestehen auch dann weiter, wenn die E-Mails nach Kenntnisnahme beim Provider gespeichert bleiben. Die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails greifen in den Schutzbereich des Fernmeldegeheimnisses ein. Die Auslagerung der E-Mails auf den nicht im Herrschaftsbereich des Nutzers liegenden Mailserver des Providers bedeutet nicht, dass der Nutzer mit dem Zugriff auf diese Daten durch Dritte einverstanden ist.

Die strafprozessualen Regelungen der §§ 94 ff. StPO ermöglichen grundsätzlich die Sicherstellung und Beschlagnahme von E-Mails, die auf dem Mailserver des Providers gespeichert sind. Sie genügen insoweit den verfassungsrechtlichen Anforderungen, die an eine gesetzliche Ermächtigung für Eingriffe in das Fernmeldegeheimnis zu stellen sind. Insbesondere entsprechen sie insoweit dem Gebot der Normenbestimmtheit und Normenklarheit.

§§ 94 ff. StPO sind hinsichtlich der Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails auch verhältnismäßig. Die wirksame Strafverfolgung, die Verbrechensbekämpfung und das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren sind legitime Zwecke, die eine Einschränkung des Fernmeldegeheimnisses rechtfertigen können. Zur Wahrung der Verhältnismäßigkeit ist es nicht geboten, den Zugriff auf beim Provider gespeicherte E-Mails auf Ermittlungen zu begrenzen, die zumindest Straftaten von erheblicher Bedeutung betreffen, und Anforderungen an den Tatverdacht zu stellen, die über den Anfangsverdacht einer Straftat hinausgehen.

Auch der konkrete Eingriff aufgrund von §§ 94 ff. StPO war verhältnismäßig. Dem Schutz des Fernmeldegeheimnisses muss bereits in der Durchsuchungsanordnung, soweit die konkreten Umstände dies ohne Gefährdung des Untersuchungszwecks erlauben, durch Vorgaben zur Beschränkung des Beweismaterials auf den erforderlichen Umfang Rechnung getragen werden. Beim Zugriff auf umfangreiche elektronisch gespeicherte E-Mail-Bestände sind die ver-fassungsrechtlichen Grundsätze zu gewährleisten, die der Senat in seinem Beschluss zur Durchsuchung und Beschlagnahme eines umfangreichen elektronischen Datenbestands (vgl.

BVerfGE 113, 29 <52 ff.>) entwickelt hat. Die Gewinnung überschießender, für das Verfahren bedeutungsloser Daten ist nach Möglichkeit zu vermeiden.

Eine sorgfältige Sichtung und Trennung der E-Mails nach ihrer Verfahrensrelevanz wird am Zugriffsort nicht immer möglich sein. Sofern die Umstände des jeweiligen strafrechtlichen Vorwurfs und die auch technische Erfassbarkeit des Datenbestands eine unverzügliche Zuordnung nicht erlauben, muss die vorläufige Sicherstellung größerer Teile oder gar des gesamten E-Mail-Bestands erwogen werden, an die sich eine Durchsicht gemäß § 110 StPO zur Feststellung der potenziellen Beweiserheblichkeit und -verwertbarkeit der E-Mails anschließt. Ist den Strafverfolgungsbehörden im Verfahren der Durchsicht unter zumutbaren Bedingungen eine materielle Zuordnung der verfahrenserheblichen E-Mails einerseits oder eine Löschung oder Rückgabe der verfahrensunerheblichen E Mails an den Nutzer andererseits nicht möglich, steht der Grundsatz der Verhältnismäßigkeit einer Beschlagnahme des gesamten Datenbestands nicht entgegen. Es muss dann aber im Einzelfall geprüft werden, ob der umfassende Datenzugriff dem Übermaßverbot Rechnung trägt.

Bestehen tatsächliche Anhaltspunkte dafür, dass ein Zugriff auf gespeicherte Telekommunikation Inhalte erfasst, die zum Kernbereich privater Lebensgestaltung zählen, hat er insoweit zu unterbleiben. Es muss sichergestellt werden, dass Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist.

Der effektive Schutz materieller Grundrechte bedarf auch einer entsprechenden Ausgestaltung des Verfahrens. Werden in einem Postfach auf dem Mailserver des Providers eingegangene E-Mails sichergestellt, ist der Postfachinhaber im Regelfall zuvor von den Strafverfolgungsbehörden zu unterrichten, damit er jedenfalls bei der Sichtung seines E-Mail-Bestands seine Rechte wahrnehmen kann. Werden auf dem Mailserver des Providers gespeicherte E-Mails ausnahmsweise ohne Wissen des Postfachinhabers sichergestellt, so ist dieser so früh, wie es die wirksame Verfolgung des Ermittlungszwecks erlaubt, zu unterrichten. Diesen Anforderungen wird durch § 35 StPO und § 98 Abs. 2 Satz 6 StPO Rechnung getragen.

Die Durchsicht gemäß § 110 StPO bezweckt die Vermeidung einer übermäßigen und auf Dauer angelegten Datenerhebung. Zur Wahrung der Verhältnismäßigkeit kann es im Einzelfall geboten sein, den Inhaber der sichergestellten E-Mails in die Prüfung der Verfahrenserheblichkeit einzubeziehen. Ob eine Teilnahme an der Sichtung sichergestellter E-Mails geboten ist, ist im jeweiligen Einzelfall unter Berücksichtigung einer wirksamen Strafverfolgung einerseits und der Intensität des Datenzugriffs andererseits zu entscheiden.

Soweit E-Mails von den Ermittlungsbehörden gespeichert und ausgewertet werden, kann es erforderlich sein, den Betroffenen Auskunft über die Datenerhebung zu erteilen, um sie in den Stand zu versetzen, etwaige Grundrechtsbeeinträchtigungen abzuwehren. Dem wird durch die besonderen strafprozessualen Auskunftsregelungen gemäß § 147, § 385 Abs. 3, § 397 Abs. 1 Satz 2 in Verbindung mit § 385 Abs. 3, § 406e und § 475 StPO sowie bei Nichtverfahrensbeteiligten durch § 491 StPO Rechnung getragen. Der begrenzte Zweck der Datenerhebung gebietet grundsätzlich die Rückgabe oder Löschung aller nicht zur Zweckerreichung benötigten kopierten E-Mails. § 489 Abs. 2 StPO enthält entsprechende Schutzvorkehrungen.

Zum ANFANG des Dokuments