BGer 1B 19/2014 vom 28. Mai 2014

Bundesgericht, 2014-05-28, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bger_1B_19_2014

FR: TF 1B 19/2014 du 28 mai 2014

IT: TF 1B 19/2014 del 28 maggio 2014

Regeste

E-Mail-Verkehr; Überwachung; Beschlagnahme | Strafprozess

Erwägungen

E. 1.1

Gegen den angefochtenen Entscheid ist gemäss Art. 78 Abs. 1 BGG die Beschwerde in Strafsachen gegeben.

E. 1.2

Die Beschwerde nach Art. 393 ff. StPO steht nicht zur Verfügung. Die Beschwerde in Strafsachen ist daher gemäss Art. 80 BGG zulässig (BGE 137 IV 340 E. 2.2 S. 343; Urteil 1B_211/2012 vom 2. Mai 2012 E. 1.2, publ. in: SJ 2012 I S. 466).

E. 1.3

Die Beschwerdeführerin ist gemäss Art. 81 Abs. 1 lit. a und b Ziff. 3 BGG zur Beschwerde befugt (BGE 137 IV 340 E. 2.3 S. 344 ff.).

E. 1.4

Der angefochtene Entscheid stellt einen Zwischenentscheid gemäss Art. 93 BGG dar. Gemäss Absatz 1 lit. a dieser Bestimmung ist dagegen die Beschwerde zulässig, wenn er einen nicht wieder gutzumachenden Nachteil bewirken kann. Nach der Rechtsprechung muss es sich im Bereich der Beschwerde in Strafsachen um einen Nachteil rechtlicher Natur handeln. Ein solcher liegt vor, wenn er auch durch einen für den Betroffenen günstigen Endentscheid nicht mehr gänzlich behoben werden könnte. Ein bloss tatsächlicher Nachteil wie die Verlängerung oder Verteuerung des Verfahrens genügt nicht (BGE 137 III 324 E. 1.1 S. 328; 136 IV 92 E. 4 S. 95; je mit Hinweisen). Für die Beschwerdeführerin ist die Verwendung der E-Mails im Interesse der Erforschung der Wahrheit von wesentlicher Bedeutung. Sie hofft, damit Aufschluss über ein Tatmotiv gewinnen zu können. Bliebe es beim angefochtenen Entscheid und käme das Sachgericht zum Schluss, eine richterliche Genehmigung sei erforderlich, könnte es die Verwertbarkeit der E-Mails verneinen (Art. 277 StPO). Das gälte ebenso für allfällige Folgebeweise. Die Erforschung der Wahrheit würde dadurch erheblich gefährdet. Der Beschwerdeführerin droht insoweit ein nicht wieder gutzumachender Nachteil im Sinne von Art. 93 Abs. 1 lit. a BGG . Die Beschwerde ist auch insoweit zulässig.

E. 1.5

Da es um eine Zwangsmassnahme geht, ist Art. 98 BGG , der eine Beschränkung der Beschwerdegründe vorsieht, nicht anwendbar (zur amtlichen Publikation bestimmtes Urteil 1B_326/2013 vom 6. März 2014 E. 2.2; BGE 137 IV 340 E. 2.4 S. 346 mit Hinweisen).

E. 1.6
Die weiteren Sachurteilsvoraussetzungen geben zu keinen Bemerkungen Anlass.

E. 2.1
Art. 23 ff. der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF; SR 780.11) regeln die Überwachung des Internets. Art. 24a VÜPF sieht die Echtzeit-Überwachung vor, Art. 24b die rückwirkende Überwachung. Gemäss Art. 2 VÜPF sind die in dieser Verordnung verwendeten Begriffe im Anhang definiert. Danach ist unter Echtzeit-Überwachung zu verstehen das Abfangen in Echtzeit und die simultane, leicht verzögerte oder periodische Übertragung der Post- oder Fernmeldeverkehrsdaten, inklusive Nutzinformationen, durch die Anbieterinnen von Post- oder Fernmeldediensten gemäss den Angaben der Überwachungsanordnung (Ziff. 3); unter rückwirkender Überwachung die Herausgabe der Verkehrs- und Rechnungsdaten (d.h. der Randdaten) der zurückliegenden sechs Monate durch die Anbieterinnen von Post- oder Fernmeldediensten (Ziff. 4). Die Vorinstanz erwägt, es gehe hier weder um eine Echtzeit-Überwachung nach Art. 24a VÜPF noch eine rückwirkende Überwachung nach Art. 24b VÜPF , weshalb auf das Genehmigungsgesuch nicht einzutreten sei. Die Y._____ AG habe die Daten des E-Mail-Verkehrs gestützt auf die Editionsverfügung der Beschwerdeführerin herauszugeben. Die Beschwerdeführerin bringt vor, sie sei inzwischen der Auffassung, es gehe um eine Überwachungsmassnahme, weshalb die Vorinstanz auf ihr Gesuch hätte eintreten müssen.

E. 2.2
Der 5. Titel der Strafprozessordnung (Art. 196 ff.) regelt die Zwangsmassnahmen. Das 4. Kapitel dieses Titels (Art. 241 ff.) hat die Durchsuchungen und Untersuchungen zum Gegenstand. Gemäss Art. 241 StPO werden Durchsuchungen und Untersuchungen in einem schriftlichen Befehl angeordnet (Abs. 1 Satz 1). Der Befehl bezeichnet namentlich die zu durchsuchenden Aufzeichnungen (Abs. 2 lit. a). Nach Art. 246 StPO dürfen insbesondere Schriftstücke, Datenträger sowie Anlagen zur Verarbeitung und Speicherung von Informationen durchsucht werden, wenn zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen. Gemäss Art. 248 StPO sind Aufzeichnungen und Gegenstände, die nach Angaben der Inhaberin oder des Inhabers wegen eines Aussage- oder Zeugnisverweigerungsrechts oder aus anderen Gründen nicht durchsucht oder beschlagnahmt werden dürfen, zu versiegeln und dürfen von den Strafbehörden weder eingesehen noch verwendet werden (Abs. 1). Stellt die Strafbehörde nicht innert 20 Tagen ein Entsiegelungsgesuch, so werden die versiegelten Aufzeichnungen und Gegenstände der berechtigten Person zurückgegeben (Abs. 2). Stellt sie ein Entsiegelungsgesuch, so entscheidet darüber innerhalb eines Monats endgültig: a. im Vorverfahren das Zwangsmassnahmengericht; b. in den anderen Fällen das Gericht, bei dem der Fall hängig ist (Abs. 3). Das 7. Kapitel (Art. 263 ff.) regelt die Beschlagnahme. Gemäss Art. 263 Abs. 1 lit. a StPO können Gegenstände einer beschuldigten Person oder einer Drittperson beschlagnahmt werden, wenn die Gegenstände voraussichtlich als Beweismittel gebraucht werden. Nach Art. 265 Abs. 1 StPO ist die Inhaberin oder der Inhaber verpflichtet, Gegenstände, die beschlagnahmt werden sollen, herauszugeben. Das 8. Kapitel betrifft die geheimen Überwachungsmassnahmen, sein 1. Abschnitt (Art. 269 ff.) die Überwachung des Post- und Fernmeldeverkehrs. Gemäss Art. 269 Abs. 1 StPO kann die Staatsanwaltschaft den Post- und Fernmeldeverkehr überwachen lassen, wenn: a. der dringende Verdacht besteht, eine in Absatz 2 genannte Straftat (namentlich eine vorsätzliche Tötung nach Art.

111 StGB oder ein Mord nach Art. 112 StGB) sei begangen worden; b. die Schwere der Straftat die Überwachung rechtfertigt; und c. die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Nach Art. 270 lit. a StPO dürfen Postadresse und Fernmeldeanschluss der beschuldigten Person überwacht werden. Gemäss Art. 272 Abs. 1 StPO bedarf die Überwachung des Post- und des Fernmeldeverkehrs der Genehmigung durch das Zwangsmassnahmengericht. Besteht der dringende Verdacht, ein Verbrechen oder Vergehen oder eine Übertretung nach Artikel 179septies StGB sei begangen worden, und sind die Voraussetzungen nach Art. 269 Abs. 1 lit. b und c StPO erfüllt, so kann die Staatsanwaltschaft gemäss Art. 273 StPO Auskunft verlangen: a. darüber, wann und mit welchen Personen oder Anschlüssen die überwachte Person über den Post- oder Fernmeldeverkehr Verbindung hat oder gehabt hat; b. über Verkehrs und Rechnungsdaten (Abs. 1). Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht (Abs. 2). Auskünfte nach Absatz 1 können unabhängig von der Dauer der Überwachung und bis 6 Monate rückwirkend verlangt werden (Abs. 3). Die Bestimmungen der Strafprozessordnung zur Überwachung des Post- und Fernmeldeverkehrs (Art. 269-279) entsprechen weitgehend den früheren strafprozessualen Normen des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1), die mit dem Inkrafttreten der Strafprozessordnung aufgehoben worden sind. Im Übrigen steht das BÜPF weiterhin in Kraft und regelt namentlich die Aufgaben des Dienstes sowie die Pflichten der Anbieterinnen von Post- und Fernmeldediensten. Das BÜPF gilt gemäss dessen Art. 1 Abs. 2 insbesondere für Internet-Anbieterinnen. In Kraft steht sodann nach wie vor die VÜPF. Mit Botschaft vom 27. Februar 2013 schlägt der Bundesrat eine Totalrevision des BÜPF vor (BBl 2013 2638 ff.). Die Vorlage befindet sich in der parlamentarischen Beratung.

E. 2.3

Gemäss Art. 13 Abs. 1 BV hat jede Person Anspruch auf Achtung ihres Brief-, Post- und Fernmeldeverkehrs. Gleichartige Garantien enthalten Art. 8 Ziff. 1 EMRK und Art. 17 UNO-Pakt II (BGE 126 I 50 E. 5a S. 61 mit Hinweis). Das verfassungsrechtliche Fernmeldegeheimnis schützt die Privatsphäre. Die Kommunikation mit fremden Mitteln wie Post und Telefon soll gegenüber Drittpersonen geheim erfolgen können. Immer wenn die Kommunikation durch einen Anbieter von Fernmeldediensten erfolgt, soll sie unter Achtung der Geheimsphäre vertraulich geführt werden können, ohne dass das Gemeinwesen Einblick erhält und daraus gewonnene Erkenntnisse gegen den Betroffenen verwendet. Dies gilt auch für den E-Mail-Verkehr über das Internet. Die Geheimsphäre der E-Mail-Benützer ist durch das Fernmeldegeheimnis verfassungsrechtlich geschützt (BGE 126 Ia 50 E. 6a S. 65 f. mit Hinweisen).

E. 2.4

Das Fernmeldegeheimnis schützt den Kommunikationsvorgang. Vor dessen Beginn und nach dessen Abschluss greift es nicht (ANDREAS DONATSCH/ALBERT SCHMID, Der Zugriff auf E-Mails im Strafverfahren - Überwachung [BÜPF] oder Beschlagnahme?, in: Schwarzenegger und andere [Hrsg.], Internet-Recht und Strafrecht, 2005, S. 157; MICHAEL AEPLI, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, 2004, S. 18; MARC JEAN-RICHARD-DIT-BRESSEL, Die Mailbox, Ziel oder Weg?, ZStrR 125/2007, S. 170/171; STEFAN HEIMGARTNER, Strafprozessuale Beschlagnahme, 2011, S. 38/39 und 175). Bei der Überwachung wird auf Daten heimlich

zugegriffen in einem Zeitpunkt, da der Absender die Datenherrschaft aufgegeben und sie der Empfänger noch nicht erlangt hat (vgl. Jean-Richard-dit-Bressel, a.a.O., S. 171 f.). Dies stellt einen schweren Eingriff in die Privatsphäre dar. Da die Betroffenen davon nichts wissen, können sie sich dagegen rechtlich nicht unmittelbar wehren. Aus diesen Gründen stellt das Gesetz bei einer Überwachung erhöhte Anforderungen, und verlangt es eine richterliche Genehmigung. Bei einem Brief liegt danach eine Überwachung vor, wenn ihn der Absender abgeschickt hat und die Behörden, bevor er beim Empfänger angekommen ist, darauf zugreifen. Der Brief wird so abgefangen. Ist der Brief beim Empfänger angekommen und befindet er sich damit in dessen Herrschaftsbereich, ist der Übertragungsvorgang abgeschlossen. Ein Abfangen ist nicht mehr möglich. Der Brief kann - wie jeder andere Gegenstand im Besitz des Empfängers - beschlagnahmt werden. Dasselbe gilt, wenn der Empfänger den Brief einem Dritten zur Aufbewahrung übergibt (Thomas Hansjakob, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2006 [im Folgenden: Kommentar BÜPF], Vorbemerkungen zum BÜPF N. 17; Jean-Richard-dit-Bressel, a.a.O., S. 159; Donatsch/Schmid, a.a.O.; Aepli, a.a.O.; Heimgartner, a.a.O., S. 177).

E. 2.5
Es stellt sich die Frage, wann ein Brief als beim Empfänger angekommen gelten kann.

E. 2.5.1
Dies trifft sicher dann zu, wenn der Postbote den Brief dem Empfänger persönlich übergibt, was insbesondere bei eingeschriebenen Sendungen der Fall ist.

E. 2.5.2
Angekommen ist der Brief ebenso, wenn ihn der Postbote in den Briefkasten des Empfängers wirft. Zwar hat der Empfänger davon in der Regel keine unmittelbare Kenntnis. Der Brief befindet sich jedoch in seinem alleinigen Herrschaftsbereich. Was damit geschieht, bestimmt einzig der Empfänger. Der Übertragungsvorgang ist deshalb abgeschlossen (Jean-Richard-dit-Bressel, a.a.O., S. 172; Aepli, a.a.O., S. 18 Fn. 87).

E. 2.5.3
Legt die Post den Brief in das Postfach des Empfängers, befindet er sich ebenfalls in dessen Herrschaftsbereich. Der Empfänger kann auf das Postfach wie auf den Briefkasten jederzeit zugreifen und den Brief entnehmen. Im Unterschied zum Briefkasten hat die Post ihre Herrschaft jedoch noch nicht aufgegeben. Sie kann auf das Postfach weiterhin jederzeit zugreifen. Es besteht somit eine geteilte Datenherrschaft (
JEAN-RICHARD-DIT-BRESSEL, a.a.O., S. 172). Die Post kann den in das Postfach gelegten Brief daraus wieder entnehmen und den Behörden von seinem Inhalt Kenntnis geben. Tut sie das, wird der Brief weiterhin abgefangen. Es kann insoweit keinen Unterschied machen, ob die Post den Behörden den Inhalt des Briefes zugänglich macht, kurz bevor sie diesen in das Postfach legt, oder ob sie das tut, nachdem sie den Brief in das Postfach gelegt und daraus sogleich wieder entnommen hat. Da die Post nach wie vor Herrschaftsmacht hat, muss der Empfänger - der das Postfach nicht ständig kontrollieren kann - weiterhin darauf vertrauen können, dass sie ihre Stellung nicht missbraucht und die Vertraulichkeit der Daten wahrt. Der Empfänger verdient deshalb nach wie vor den Schutz des Fernmeldegeheimnisses (ebenso HEIMGARTNER, a.a.O., S. 180). Der Abschluss des Kommunikationsvorgangs ist daher auf jenen Zeitpunkt festzulegen, in dem der Empfänger die alleinige Datenherrschaft erlangt. Das ist dann der Fall, wenn er das Postfach öffnet. Ab

diesem Zeitpunkt bestimmt einzig er, was mit dem Brief geschieht. Der Empfänger kann den Brief - ob geöffnet oder nicht - mitnehmen oder fortwerfen; er kann ihn aber auch im Postfach belassen und dort aufbewahren. Tut er Letzteres, kann der Brief im Postfach beschlagnahmt werden. Es kann insoweit keinen Unterschied machen, ob der Empfänger den Brief zu Hause, bei der Post im Postfach oder bei einem anderen Dritten aufbewahrt. Greifen die Behörden auf einen Brief zu, den der Empfänger - wo auch immer - aufbewahrt, tun sie das nach Abschluss des Kommunikationsvorgangs und nicht heimlich. Dies stellt keine Überwachungsmassnahme dar.

E. 2.6

Die Zustellung eines E-Mails ist vergleichbar mit der Zustellung eines Briefes in das Postfach (Jean-Richard-dit-Bressel, a.a.O., S. 172; Heimgartner, a.a.O., S. 180). Das E-Mail gelangt auf dem Server des Fernmeldedienstanbieters ("Provider") des Empfängers in dessen E-Mail-Konto. Dies entspricht dem Einlegen des Briefes in das Postfach. Der Empfänger erhält erst dann Kenntnis vom Eingang des E-Mails, wenn er sein Konto abruft, d.h. eine Verbindung mit dem Server des Providers herstellt und das E-Mail für ihn sichtbar macht. Dies entspricht dem Öffnen des Postfachs. Ab diesem Zeitpunkt bestimmt allein der Empfänger, was mit dem E-Mail geschieht. Er kann es sofort löschen. Er kann es auf seine lokale Datenverarbeitungsanlage herunterladen und auf dem Server des Providers entfernen. Er kann das E-Mail aber auch auf dem Server des Providers belassen, womit er darauf weiterhin von überall her Zugriff hat. Belässt der Empfänger das E-Mail auf dem Server des Providers, bewahrt er es dort auf. Damit kann es wie der im Postfach belassene Brief beschlagnahmt werden. Es besteht kein Grund, das E-Mail, das der Empfänger auf dem Server seines Providers belässt und dort aufbewahrt, besser zu schützen als jenes, das er in seiner lokalen Datenverarbeitungsanlage oder sonst wo aufbewahrt (ebenso Jean-Richard-dit-Bressel, a.a.O., S. 179). Wie bei der Zustellung eines Briefes in das Postfach kann es bei alldem keine Rolle spielen, ob der Empfänger das E-Mail geöffnet hat, also auf das als ungelesen gekennzeichnete (häufig fett hervorgehobene) E-Mail geklickt hat, um den Inhalt zu lesen. Bevor der Empfänger sein E-Mail-Konto abgerufen hat, dauert der Datenübertragungsvorgang an. Auf die bis zu jenem Zeitpunkt auf dem Server des Providers gespeicherten E-Mails kann deshalb nur durch eine Überwachungsmassnahme gegriffen werden. Dabei handelt es sich um eine Echtzeit-Überwachung, da das E-Mail auf dem Weg vom Absender zum Empfänger heimlich abgefangen wird (ebenso TPF 2008 42, S. 43 unten; Jean-Richard-dit-Bressel, a.a.O., S. 174; Hansjakob, Kommentar BÜPF, Vorbemerkungen zum BÜPF N. 20 und dortige Fn. 27). Dieses Abfangen zeichnet nach der Begriffsumschreibung von Ziffer 3 Anhang VÜPF die Echtzeit-Überwachung aus. Damit darf vom Kommunikationsinhalt Kenntnis genommen werden. Dies im Gegensatz zur rückwirkenden Überwachung, mit der lediglich Randdaten erhoben werden dürfen, welche im Wesentlichen darüber Auskunft geben, wer wann mit wem Verbindung gehabt hat.

E. 2.7

Danach ergibt sich Folgendes: Die abgerufenen E-Mails auf dem Server der Y._____ AG können - soweit sie dort noch vorhanden sind - beschlagnahmt werden. Die nicht abgerufenen E-Mails können unter den Voraussetzungen der Echtzeit-Überwachung erhoben werden (Jean-Richard-dit-Bressel, a.a.O., S. 174; Hansjakob, Kommentar BÜPF, Vorbemerkungen zum BÜPF N. 20).

E. 2.8

Die Voraussetzungen für die Echtzeit-Überwachung gemäss Art. 269 Abs. 1 i.V.m. Abs. 2 lit. a StPO sind hier erfüllt. Es besteht der dringende Verdacht einer vorsätzlichen Tötung (Art. 111 StGB) bzw. eines Mords (Art. 112 StGB). Die Schwere der Straftat rechtfertigt die Überwachung. Die bisherigen Ermittlungen sind, was die Klärung eines allfälligen Tatmotivs betrifft, erfolglos geblieben. Der Beschuldigte bestreitet die Tötung nicht, gibt aber an, sich daran nicht erinnern zu können. Es bestehen Anhaltspunkte dafür, dass er in der Türkei seit Langem "nach Brauch" mit einer Landsfrau verheiratet ist, mit der er mehrere Kinder hat; ebenso dafür, dass er seine schweizerische Ehefrau beseitigte, nachdem diese sich von ihm scheiden lassen wollte, womit er insbesondere keine Aussicht auf eine erleichterte Einbürgerung mehr gehabt hätte. Die Klärung eines allfälligen Tatmotivs ist wichtig, da es bei einem Schuldspruch für die rechtliche Qualifikation der Tat bzw. die Strafzumessung von Bedeutung wäre.

E. 2.9.1

Das Bundesgericht genehmigt die Überwachung selber (Art. 107 Abs. 2 Satz 1 BGG), womit eine Rückweisung an die Vorinstanz - und damit eine Verlängerung des Verfahrens - vermieden werden kann.

E. 2.9.2

Gemäss Art. 274 Abs. 4 StPO äussert sich die Genehmigung ausdrücklich darüber, ob: a. Vorkehren zum Schutz von Berufsgeheimnissen getroffen werden müssen; b. Direktschaltungen zulässig sind. Vorkehren zum Schutz von Berufsgeheimnissen sind hier nicht erforderlich. Eine Anordnung zu Direktschaltungen erübrigt sich, da Art. 274 Abs. 4 lit. b StPO technisch überholt ist. In der Praxis sind heute alle Überwachungen Direktschaltungen (Thomas Hansjakob, in: Donatsch und andere [Hrsg.], Kommentar zur Schweizerischen Strafprozessordnung, 2010, N. 12 zu Art. 274 StPO ; Niklaus Schmid, Schweizerische Strafprozessordnung, Praxiskommentar, 2. Aufl. 2013, N. 11 zu Art. 274 StPO).

E. 2.9.3

Gemäss Art. 274 Abs. 5 StPO ist die Genehmigung zu befristen. Sie kann für höchstens 3 Monate erteilt werden, aber ein- oder mehrmals um jeweils höchstens 3 Monate verlängert werden. Da es um ein schweres Verbrechen geht, rechtfertigt es sich, die Genehmigung für die Höchstdauer von 3 Monaten zu erteilen. Diese Dauer läuft ab dem Zeitpunkt der Überwachungsanordnung (Hansjakob, Kommentar BÜPF, N. 25 zu Art. 7 BÜPF), hier also bis zum 10. März 2014. Die Beschwerdeführerin wird vom Inhalt sämtlicher nicht abgerufener E-Mails, die bis zu diesem Zeitpunkt auf dem E-Mail-Konto des Beschuldigten eingegangen sind, Kenntnis nehmen dürfen.

E. 2.10

Soweit die E-Mails der Beschlagnahme unterliegen, kann der Beschuldigte die Siegelung verlangen (zur Legitimation BGE 140 IV 28 E. 4.3.4 f.). Tut er dies, entscheidet auf entsprechendes Gesuch der Beschwerdeführerin hin das zuständige Gericht über die Zulässigkeit der Durchsuchung.

E. 3

Kosten sind keine zu erheben (Art. 66 Abs. 4 BGG).