BGer 1B_235/2015 vom 11. Dezember 2015

Bundesgericht, 2015-12-11, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bger_1B_235_2015

FR: TF 1B_235/2015 du 11 décembre 2015

IT: TF 1B_235/2015 del 11 dicembre 2015

Erwägungen

E. 1

Das Bundesgericht prüft die Sachurteilsvoraussetzungen einer ihm unterbreiteten Beschwerde von Amtes wegen und mit freier Kognition (Art. 29 Abs. 1 BGG ; vgl. BGE 140 IV 57 E. 2 S. 59).

E. 1.1

Die verfahrensleitende Staatsanwaltschaft, welche am vorinstanzlichen Verfahren teilgenommen hat, ist zur Beschwerde in Strafsachen gegen Entscheide über streitige Untersuchungsmassnahmen, insbesondere Zwangsmassnahmen, berechtigt (Art. 81 lit. a und lit. b Ziff. 3 BGG; Art. 16 i.V.m. Art. 308 Abs. 1 und Art. 311 Abs. 1 StPO). Dies gilt nach der Praxis des Bundesgerichtes insbesondere für Entsiegelungen (Urteile 1B_65/2014 vom 22. August 2014 E. 1; 1B_517/2012 vom 27. Februar 2013 E. 4). Zur Wahrnehmung ihrer Leitungs- und Koordinationsfunktionen ist in Fällen wie dem vorliegenden grundsätzlich auch die kantonale Oberstaatsanwaltschaft beschwerdebefugt (vgl. BGE 139 IV 25 E. 1 S. 27; nicht amtlich publ. E. 1 von BGE 141 IV 108).

E. 1.2

Zu prüfen bleibt, ob die Sachurteilsvoraussetzung des nicht wieder gutzumachenden Rechtsnachteils (Art. 93 Abs. 1 lit. a BGG) erfüllt ist (vgl. BGE 135 I 261 E. 1.2 S. 263 mit Hinweisen).

Die Oberstaatsanwaltschaft legt dar, dass im Falle der Abweisung des Entsiegelungsgesuches ein empfindlicher und irreversibler Beweisverlust bei der Aufklärung schwer wiegender Delikte drohe. Untersucht werde ein schwerer Fall internationaler (Cyber-) Wirtschaftskriminalität. Die Täterschaft habe mehrfach versucht, diverse Datenverarbeitungsanlagen betrügerisch zu missbrauchen, unrechtmässige Überweisungen aus fremden Bankkonten zu veranlassen und sich oder Dritte mit mehr als Fr. 1,267 Mio. zu bereichern. Bei internationaler Cyberkriminalität sei das Risiko der Täterschaft, ermittelt und überführt zu werden, besonders gering. Es bestehe die Gefahr, dass die Täter gefahrlos die nötige Anzahl weiterer Versuche unternehmen könnten, von denen erfahrungsgemäss nur ein kleiner Prozentsatz die Maschen aller Sicherheitssysteme der Banken passiere. Dieses Täterkalkül sei durchaus erfolgreich und führe weltweit zu Schäden in Milliardenhöhe bei verschwindend geringen Aufklärungsraten. Solchen Zusammenhängen sei auch bei der Prüfung des hinreichenden Tatverdachtes bei konkreten strafprozessualen Ermittlungsansätzen ausreichend Rechnung zu tragen.

E. 1.3

Auch die übrigen Sachurteilsvoraussetzungen von Art. 78 ff. BGG sind erfüllt und geben zu keinen Vorbemerkungen Anlass.

E. 2

Das Entsiegelungsgericht hat im Vorverfahren darüber zu entscheiden, ob die Geheimnisschutzinteressen, welche von der Inhaberin oder dem Inhaber der versiegelten Aufzeichnungen und Gegenstände angerufen werden, einer Durchsuchung und weiteren strafprozessualen Verwendung durch die Staatsanwaltschaft entgegen stehen (Art. 248 Abs. 1 StPO ; BGE 141 IV 77 E. 4.1 S. 81; 137 IV 189 E. 4 S. 194 f.; 132 IV 63 E. 4.1-4.6 S. 65 ff.). Strafprozessuale Zwangsmassnahmen setzen auch voraus, dass ein hinreichender Tatverdacht vorliegt (Art. 197 Abs. 1 lit. b StPO ; BGE 141 IV 87 E. 1.3.1 S. 90) und der damit verbundene Eingriff verhältnismässig erscheint (Art. 197 Abs. 1 lit. c-d und Abs. 2 StPO). Insbesondere müssen die zu durchsuchenden Unterlagen untersuchungsrelevant sein (BGE 141 IV 77 E. 4.3 S. 81; 138 IV 225 E. 7.1 S. 229; je mit Hinweisen).

E. 3

Dem Entsiegelungsgesuch der Staatsanwaltschaft liegt ein sog. Cyberangriff (Hacking) zugrunde, mit welchem eine unbekannte Täterschaft am 23. und 25. April 2013 mithilfe eines "Trojaners" bei einem Schweizer Finanzinstitut insgesamt neun Zahlungsaufträge im Gesamtbetrag von ca. Fr. 1,267 Mio. auszulösen versuchte. Die drei grössten Zahlungen hätten an zwei Unternehmen geleistet werden sollen, von denen das eine in Spanien (Teneriffa) und das andere in Sarnen domiziliert ist. Der private Beschwerdegegner hatte (unbestritten) mit beiden Firmen bzw. den daran berechtigten Privatpersonen geschäftliche bzw. private Kontakte: Während es sich bei der in Teneriffa ansässigen Unternehmung um die Gesellschaft eines russischen Partners handelt, pflegt er seit Jahren eine freundschaftliche Beziehung zum Eigentümer der Schweizer Gesellschaft.

Die Staatsanwaltschaft erachtet es als sehr unwahrscheinlich, dass der Beschwerdegegner aus blossem Zufall zwei der durch die versuchten illegalen Zahlungen am meisten Begünstigten kenne. Vielmehr bestehe der Verdacht, dass er als Bindeglied zwischen den Hackern und den Zahlungsempfängern gedient habe. Ausserdem mache ihn verdächtig, dass er über mehrere gefälschte Ausweise und ein (in einer Krawatte verstecktes) illegales Aufnahmegerät verfüge. Der Beschwerdegegner bestreitet einen Zusammenhang zwischen den beiden oben erwähnten Bekanntschaften und dem Cyberangriff. Die Vorinstanz ist ebenfalls der Auffassung, die Kontakte mit den Berechtigten an den genannten Unternehmen, zu deren Gunsten die illegalen Zahlungen hätten ausgeführt werden sollen, begründeten noch keinen Anfangsverdacht.

E. 4.1

Gemäss Art. 197 Abs. 1 StPO können strafprozessuale Zwangsmassnahmen (Art. 196-298 StPO) nur ergriffen werden, wenn sie gesetzlich vorgesehen sind, ein hinreichender Tatverdacht vorliegt, die damit angestrebten Ziele nicht durch mildere Massnahmen erreicht werden können und die Bedeutung der Straftat die Zwangsmassnahme rechtfertigt. Hinweise auf eine strafbare Handlung müssen nach der Praxis des Bundesgerichtes erheblich und konkreter Natur sein, um einen hinreichenden Tatverdacht (Art. 197 Abs. 1 lit. b StPO) begründen zu können (BGE 141 IV 87 E. 1.3.1 S. 90; 137 IV 122 E. 3.2 S. 126; je mit Hinweisen).

E. 4.2

Bei der Prüfung des hinreichenden Tatverdachtes ist im vorliegenden Fall den Besonderheiten der untersuchten internationalen Cyber-Wirtschaftskriminalität Rechnung zu tragen. Gemäss den bisherigen Untersuchungsergebnissen bestanden im Tatzeitraum

zunächst enge wirtschaftliche und persönliche Beziehungen zwischen dem Beschuldigten und dem wirtschaftlich Berechtigten und einzigen Verwaltungsrat der von den Hackerangriffen mit ca. Fr. 1,18 Mio. hauptbegünstigten (Schweizer) Gesellschaft. Der Beschuldigte hat den wirtschaftlich Berechtigten (nach dessen Aussagen) sodann mehrfach angefragt, ob grössere Zahlungen über das Konto seiner Gesellschaft geleitet werden könnten. Der Beschuldigte habe dabei jeweils "Zeitdruck gemacht". Nach Aussagen des wirtschaftlich Berechtigten seien diese Anfragen zwischen Ende 2011 und Mai 2013 erfolgt. Diese Zusammenhänge wurden schon im Entsiegelungsgesuch dargelegt. Die Erwägungen der Vorinstanz, es könne "im Knüpfen von Freundschaften kein Anzeichen für ein strafbares Verhalten" gesehen werden und die in Aussicht gestellten Zahlungen wären angeblich "von russischen Immobilienkunden respektive deren Firmen" gekommen, greifen zu kurz. Auffällig erscheint hier auch, dass der wirtschaftlich Berechtigte der (im April 2013) hauptbegünstigten Gesellschaft nach eigenen Aussagen die Zugangsdaten für das Online-Banking der Gesellschaft (Login-Daten und Token) im Sommer 2013 an Drittpersonen ("Kunden") weitergab.

E. 4.3

Sodann wurde im Entsiegelungsgesuch ebenfalls schon dargelegt, dass der private Beschwerdegegner nicht nur zum wirtschaftlich Berechtigten der hauptbegünstigten Schweizer Gesellschaft im Tatzeitraum eine enge Beziehung unterhielt, sondern gleichzeitig auch zum Inhaber der von den Hackerangriffen (mit Fr. 59'478.61) am zweitstärksten begünstigten spanischen Gesellschaft mit Sitz auf Teneriffa Kontakte pflegte, wo im Übrigen auch der Beschuldigte wohnt. Dieser bestreitet nicht, dass er den Inhaber der spanischen Gesellschaft als seinen "Partner aus Russland" bezeichnet hat, mit dem er gemeinsame Investitionen getätigt habe. Wie sich darüber hinaus den Einvernahmeprotokollen entnehmen lässt, welche die Staatsanwaltschaft dem Zwangsmassnahmengericht vorlegte, hat der Beschuldigte ausgesagt, er sei sich sicher, dass der Inhaber der spanischen und der wirtschaftlich Berechtige der Schweizer Gesellschaft sich nicht kannten. Auch Letzterer hat zu Protokoll gegeben, dass ihm die spanische Gesellschaft nicht bekannt sei.

E. 4.4

Aus dem Gesagten ergibt sich zulasten des Beschuldigten ein sehr auffälliges und verdächtiges Beziehungs- und Verhaltensmuster: Einerseits pflegte er im Tatzeitraum teilweise sehr enge Beziehungen zum wirtschaftlich Berechtigten bzw. zum Inhaber der beiden von den Hackerangriffen (bei Weitem) am stärksten begünstigten Gesellschaften. Anderseits gibt es nach den bisherigen Ermittlungsergebnissen keinerlei persönliche oder sachliche Verbindungen zwischen diesen beiden Gesellschaften oder ihren wirtschaftlich Berechtigten. Gemäss den Aussagen des Beschuldigten und einer der begünstigten Personen kannten sich diese untereinander nicht einmal. Dass er im Tatzeitraum aus purem Zufall ausgerechnet in Kontakt zu den beiden Hauptbegünstigten der diversen Hackerangriffe (mit begünstigten Konten in der Schweiz, in Spanien, in der Slowakei, in Tschechien und in Polen) gestanden haben soll, erscheint daher sehr unwahrscheinlich.

E. 4.5

Das Vorbringen der Oberstaatsanwaltschaft, wonach keinerlei persönlichen oder sachlichen Verbindungen zwischen den fraglichen beiden Gesellschaften oder ihren wirtschaftlich Berechtigten ersichtlich sind bzw. dass sich Letztere gar nicht kannten, stellt im Übrigen

kein unzulässiges Novum (im Sinne von Art. 99 Abs. 1 BGG) dar:

Die oben genannten wesentlichen Verdachtsgründe bildeten bereits Gegenstand des Entsiegelungsgesuches. Es wurde darin auch dargelegt, dass die eine Gesellschaft in der Schweiz und die andere in Spanien (Teneriffa) domiziliert ist, wo auch der Beschuldigte wohnt. Ebenso geht aus dem Gesuch hervor, dass weder die Gesellschaftsorgane noch die betroffenen Konten der beiden Gesellschaften Übereinstimmungen aufweisen. Die Konten befinden sich bei unterschiedlichen Banken in unterschiedlichen Ländern. Dass zwischen den Gesellschaften oder ihren (ebenfalls erwähnten) wirtschaftlich Berechtigten sonst irgendeine erkennbare personelle oder geschäftliche Verbindung bestanden hätte, wurde von der Staatsanwaltschaft im Entsiegelungsgesuch (mit Recht) nicht behauptet. Nötigenfalls hätte die Vorinstanz dies auch noch in den umfangreichen Akten, auf die sich das Entsiegelungsgesuch ausdrücklich stützt, verifizieren können. Daran ändert der Umstand nichts, dass die Oberstaatsanwaltschaft in der Beschwerdeschrift auch noch ergänzend auf die Einvernahmeprotokolle hinweist, laut denen sich die wirtschaftlich Berechtigten der beiden Gesellschaften nicht einmal kannten. Zwar fand sich dieser ausdrückliche Hinweis im Entsiegelungsgesuch noch nicht. Auch die fraglichen Protokolle hatte die Staatsanwaltschaft der Vorinstanz jedoch unbestrittenermassen vorgelegt.

E. 4.6

Schliesslich fällt auch noch ins Gewicht, dass aufgrund der bisherigen Untersuchungsergebnisse (Ausschreibung von Interpol Spanien) auch in Spanien gegen den privaten Beschwerdegegner (anscheinend wegen Internetkriminalität) ermittelt wurde, dass bei ihm (in einer Krawatte versteckt) ein illegales Aufnahmegerät sichergestellt wurde und dass er über offenbar gefälschte Personalausweise verfügt bzw. unter mehreren Alias-Identitäten auftrat. Sein Vorbringen, bei einem der Familiennamen handle es sich um seinen "ledigen Namen", überzeugt nicht. Zum einen legt er nicht dar, weshalb durch Heirat auch noch seine Staatsangehörigkeit (automatisch) gewechselt hätte. Zum anderen sind bei einer der Alias-Identitäten nicht nur der Nachname und die Staatsangehörigkeit geändert worden, sondern auch noch der Vorname. Wie es sich damit genau verhält, braucht nicht weiter vertieft zu werden. Bei den genannten Umständen handelt es sich jedenfalls um belastende Indizien, die auf eine gewisse Neigung des Beschwerdegegners zu illegalem Geschäftsgebaren schliessen lassen. Zu erwähnen ist auch, dass gefälschte Ausweise und falsche Identitäten es gerade den (mutmasslichen) Teilnehmern an grenzüberschreitender Cyberkriminalität erleichtern können, sich zu tarnen und zu organisieren. Die Ansicht der Vorinstanz, es sei insofern keinerlei Bezug zu den untersuchten Internetdelikten ersichtlich, verkennt diese Zusammenhänge.

E. 4.7

Bei gesamthafter Betrachtung dieser vorläufigen Untersuchungsergebnisse hält die Verneinung des hinreichenden Tatverdachtes einer Teilnahme des privaten Beschwerdegegners an einem Wirtschaftsdelikt (Art. 197 Abs. 1 lit. b StPO i.V.m. Art. 147, Art. 22 und Art. 24 f. StGB) vor dem Bundesrecht nicht stand.

Hinzu kommt noch Folgendes: Unbestrittenermassen besteht der konkrete (und dringende) Verdacht, dass eine noch unbekannte Täterschaft mehrfach versucht hat, mittels eines "Trojaners" und unter Missbrauch von Datenverarbeitungsanlagen hohe Überweisungen aus fremden Bankkonten zu veranlassen und die Konteninhaber finanziell zu schädigen. Eine Entsiegelung des sichergestellten Laptops des Beschwerdegegners wäre grundsätzlich

selbst dann möglich, wenn er nicht selbst beschuldigt und der Teilnahme an den untersuchten Delikten hinreichend verdächtig wäre: Beweisrelevante Aufzeichnungen könnten grundsätzlich auch bei Drittpersonen beschlagnahmt werden (Art. 263 Abs. 1 Ingress und lit. a StPO). Wie bereits dargelegt, besteht ein ausreichend konkreter Bezug zwischen der verdächtigen Geschäftstätigkeit des Beschwerdegegners und den untersuchten Delikten. Die Untersuchungsrelevanz der sichergestellten Aufzeichnungen ist daher im Prinzip zu bejahen. Auch dient die streitige Zwangsmassnahme der Aufklärung von schweren (Cyber-) Wirtschaftsdelikten, nämlich versuchten Verbrechen (Art. 147 i.V.m. Art. 22 und Art. 10 Abs. 2 StGB) mit einem Deliktsbetrag von mehr als Fr. 1,26 Mio. Auch unter diesem Gesichtspunkt erscheint der Eingriff grundsätzlich - nämlich vorbehältlich allfälliger schutzwürdiger Geheimhaltungsinteressen und etwaiger nicht untersuchungsrelevanter konkreter Dateien (aufgrund entsprechender Substanzierungen des Beschwerdegegners) - als verhältnismässig (Art. 197 Abs. 1 lit. c-d und Abs. 2 StPO; vgl. BGE 141 IV 77 E. 4.3 S. 81; 138 IV 225 E. 7.1 S. 229; je mit Hinweisen).

E. 5

Das Zwangsmassnahmengericht hat sich darauf beschränkt, den hinreichenden Tatverdacht (zu Unrecht) zu verneinen. Die übrigen Entsiegelungsvoraussetzungen (etwa das Fehlen von schutzwürdigen Geheimhaltungsinteressen oder die Untersuchungsrelevanz der konkreten elektronischen Aufzeichnungen) hat es nicht geprüft. Die Beschwerde ist daher gutzuheissen, der angefochtene Entscheid aufzuheben und die Sache (entsprechend dem Hauptantrag der Beschwerdeführerin) zur Neubeurteilung im Sinne der vorstehenden Erwägungen an die Vorinstanz zurückzuweisen.

Dem Ausgang des Verfahrens entsprechend sind die Gerichtskosten dem unterliegenden privaten Beschwerdegegner aufzuerlegen (Art. 66 Abs. 1 BGG). Eine Parteientschädigung ist nicht zuzusprechen (Art. 68 BGG).