Obergericht des Kantons Zürich

III. Strafkammer

Geschäfts-Nr.: UH130228-O/U/KIE

Mitwirkend: der Oberrichter lic. iur. Th. Meyer, Präsident, der Ersatzoberrichter lic. iur A. Schärer und die Ersatzoberrichterin lic. iur. J. Haus Stebler sowie der Gerichtsschreiber Dr. iur. J. Hürlimann

Beschluss vom 12. Dezember 2013

in Sachen

A._____,
Beschwerdeführer

verteidigt durch Rechtsanwalt MLaw X._____

gegen

Staatsanwaltschaft III des Kantons Zürich,
Beschwerdegegnerin

betreffend **Überwachungsmassnahmen und Zufallsfunde**

Beschwerde gegen die Überwachungsmassnahmen und die Verwertung von Zufallsfunden gemäss Mitteilungen der Staatsanwaltschaft III des Kantons Zürich vom 28. Juni 2013, A-1/2012/582

Erwägungen:

1. a) Mit E-Mail vom 29. November 2012 bot "B._____" verschiedenen Banken eine Datei mit 76'000 Datensätzen von deutschsprachigen Kunden der C._____ Management CH zum Preis von EUR 150'000.-- an (UH130229 Urk. 7/011006; in dieser Strafsache sind zwei Beschwerdeverfahren bei der III. Strafkammer hängig, die Untersuchungsakten finden sich im Dossier UH130229). Die Bank D._____ orientierte gleichentags die C._____, welche sich an die Staatsanwaltschaft III des Kantons Zürich und die Kantonspolizei Zürich wandte. Die Staatsanwaltschaft III des Kantons Zürich eröffnete am 3. Dezember 2013 eine Strafuntersuchung betreffend unbefugte Datenbeschaffung etc. (Urk. 7/011001).

Unter anderem erfolgten im vorliegenden Strafverfahren folgende Anordnungen der Staatsanwaltschaft:

- 4. Dezember 2012: Überwachung des noch unbekannten Nutzers der E-Mail-Adresse "…" im Sinne einer Standortidentifikation (Art. 280 lit. c StPO); dies soll dadurch erfolgen, dass in E-Mails eingebettete externe Elemente (Zählpixel oder ähnliches) an die überwachte Adresse sowie an allfällige weitere von der unbekannten Täterschaft verwendete E-Mail-Adressen gesandt werden (UH130229 Urk. 7/021001); vom Zwangsmassnahmengericht am Obergericht bewilligt mit Verfügung vom 5. Dezember 2012 (UH130229 Urk. 7/0210019).

- 31. Dezember 2012: Überwachung des Mobiltelefonanschlusses von A._____ (Beschwerdeführer), der inzwischen verdächtigt wurde, "B._____" zu sein, im Sinne einer Echtzeitüberwachung (Art. 269 StPO) und einer rückwirkenden Überwachung (Art. 273 StPO) (UH130229 Urk. 7/024011, 024013, 024014); vom Zwangsmassnahmengericht am Obergericht des Kantons Zürich bewilligt mit Verfügung vom 3. Januar 2013 UH130229 Urk. 7/024023).

- 10. Januar 2013: Überwachung des elektronischen Postdienstes und Internetzugangs und -verkehrs des Beschwerdeführers im Sinne einer Echt-

zeitüberwachung und einer rückwirkenden Überwachung (UH130229 Urk. 7/025005, 025008, 025009, 025010, 025011, 025012); vom Zwangsmassnahmengericht am Obergericht bewilligt mit Verfügung vom 11. Januar 2013 (UH130229 Urk. 7/025020).

- 21. Februar 2013: Auswertung einer Überwachung bzw. der Accounts des Beschwerdeführers auf verschiedenen Websites mit pornografischem Inhalt (UH130229 Urk. 7/026013) durch Verwendung der Login-Daten; vom Zwangsmassnahmengericht am Obergericht zuvor, mit Verfügung vom 20. Februar 2013, bewilligt (UH130229 Urk. 7/026008).

- Verwertung eines Zufallfunds (Pornografie) aufgrund der mit Verfügung vom 15. Februar 2013 erteilten Bewilligung des Zwangsmassnahmengerichts am Obergericht (UH130229 Urk. 7/027007).

Mit vier Schreiben je vom 28. Juni 2013 teilte die Staatsanwaltschaft dem Beschwerdeführer die Überwachungsanordnungen vom 31. Dezember 2012 und 10. Januar 2013, die Auswertungsanordnung vom 21. Februar 2013 und die Verwertung des Zufallfundes, je einschliesslich der betreffenden Bewilligungen des Zwangsmassnahmengerichts, mit (Urk. 3/1-4).

b) Der Beschwerdeführer beantragt mit vorliegender Beschwerde, es sei die Unzulässigkeit der genannten Überwachungs-, Nutzungs- und Verwertungsanordnungen bzw. die Unverwertbarkeit der aus diesen Anordnungen bzw. Genehmigungen gewonnen Erkenntnisse festzustellen. Weiter sei dem Beschwerdeführer eine Genugtuung von Fr. 1'000.-- zuzusprechen (Urk. 2 S. 2 Anträge 1 - 3).

Die Staatsanwaltschaft beantragt in ihrer Vernehmlassung die Abweisung der Beschwerde (Urk. 9). Der Beschwerdeführer und die Staatsanwaltschaft halten in ihren weiteren Rechtsschriften an ihren Standpunkten fest (Urk. 13 und17).

2. a) Die Echtzeitüberwachung des Telefons, des elektronischen Postdienstes und des Internetzugangs des Beschwerdeführers gemäss Anordnungen vom 31. Dezember 2012 und vom 10. Januar 2013 erfolgte gestützt auf Art. 269 Abs. 1 und 2 StPO in Verbindung mit Art. 143 Abs. 1 StGB (UH130229 Urk. 7/024011

und 025005). Die Überwachung des Post- und Fernmeldeverkehrs kann unter anderem zur Verfolgung einer unbefugten Datenbeschaffung im Sinne von Art. 143 StGB angeordnet werden (Art. 269 Abs. 2 lit. a StPO).

Gemäss Art. 143 Abs. 1 StGB begeht derjenige eine unbefugte Datenbeschaffung, der in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbare Weise gespeicherte oder übermittelte Daten beschafft, *die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind*.

Der Beschwerdeführer, welcher bestreitet, "B._____" zu sein, macht geltend, er sei zum Zugang zu den Daten berechtigt gewesen, weshalb Art. 143 StGB nicht zur Anwendung kommen könne. Daran vermöge nichts zu ändern, dass er allenfalls zivilrechtlich nicht berechtigt gewesen sei, die Daten zu kopieren. Datenveruntreuung werde von Art. 143 StGB nicht erfasst. Zudem seien die Daten nicht gegen die unrechtmässige Verwendung gesichert gewesen. Eine andere Katalogtat (im Sinne von Art. 269 Abs. 2 StPO) sei von der Staatsanwaltschaft nicht geltend gemacht worden. Der Beschwerdeführer weist darauf hin, dass allfällige Geheimnisverletzungen keine Katalogtaten darstellten. Mangels Katalogtat erweise sich die Überwachung als unzulässig. Die gestützt auf die unzulässigen Überwachungen gewonnenen Erkenntnisse dürften nicht verwendet werden. Ohne die Erkenntnisse aus den Überwachungsmassnahmen gemäss Anordnungen vom 31. Dezember 2012 und vom 10. Januar 2013 wäre es der Staatsanwaltschaft nicht möglich gewesen, die Nutzung von Login-Daten gemäss Anordnung vom 21. Februar 2013 (UH130229 Urk. 7/026013) und die Zufallsfunde (Bewilligung des Zwangsmassnahmengericht vom 15. Februar 2013; UH130229 Urk. 7/027007) zu tätigen. Die Ergebnisse aus den unzulässigen Überwachungen seien entsprechend Art. 277 StPO und Art. 278 Abs. 4 StPO zu vernichten (Urk. 2 S. 7 f Rz. 13 - 21).

b) Unbestritten ist, dass der Beschwerdeführer aufgrund seines Aufgabenbereichs in der C._____ Zugang zu den fraglichen Daten hatte. Darf jemand Daten benützen, so sind sie auch dann "für ihn bestimmt" im Sinne von Art. 143 Abs. 1 StGB, wenn er sich nicht an vertraglich, urheberrechtlich oder anderweitig begründete

Nutzungsbeschränkungen hält. Die "Datenveruntreuung" fällt nicht unter Art. 143 StGB. In Betracht kommen dann eine Veruntreuung (Art. 138 StGB), eine ungetreue Geschäftsbesorgung (Art. 158 StGB) und Geheimnisdelikte nach Art. 161 f. StGB, Art. 47 BankG usw. (Philippe Weissenberger, Basler Kommentar, Strafrecht II, 3. Aufl., Basel 2013, N 16 zu Art. 143 StGB; Stefan Trechsel / Dean Crameri, in Trechsel/Pieth [Hsg], Schweizerisches Strafgesetzbuch, Praxiskommentar, Zürich/St. Gallen 2013, N 5 zu Art. 143 StGB).

Die Staatsanwaltschaft anerkennt, dass derjenige nicht unter Art. 143 StGB fällt, welcher ihm anvertraute Daten missbräuchlich verwendet. Sie hält dafür, ob Daten anvertraut seien, sei mit Blick auf die Lehre und Rechtsprechung zur Veruntreuung im Sinne von Art. 138 StGB zu beurteilen. Demnach sei zu verlangen, dass der Datenberechtigte die Daten aus der Hand gebe und dem "Datentreuhänder" ausschliesslich zu einem klar definierten Zweck überlasse. Wenn der Datenberechtigte selber weiterhin über die Daten verfüge, schliesse dies ein Treuhandverhältnis, das die Anwendbarkeit von Art. 143 StGB verhindere, nicht aus, denn Daten seien frei reproduzierbar. Entscheidend sei, ob der Datenberechtigte die faktische Kontrolle über genau die Datenkopien aufgebe, mit denen der Datenempfänger einen bestimmten Zweck verfolgen soll. Dies sei sicher dann der Fall, wenn der Datenberechtigte dem Datenempfänger die Kopien dafür herausgebe, dass dieser sie für einen bestimmten Zweck auf seinem eigenen, vom Datenberechtigten unabhängigen Computer abspeichere. Sei der Datenempfänger auch sonst organisatorisch nicht oder nur lose in den Betrieb des Datengebers eingebunden, so seien die Voraussetzungen für einen "Datendiebstahl" zweifellos zu verneinen. Anders verhalte es sich im umgekehrten Fall, in welchem die Daten dem Empfänger nicht herausgegeben würden, sondern dieser lediglich die Möglichkeit erhalte, über die Computersysteme des Datengebers im Rahmen des Pflichtenheftes als dessen Mitarbeiter auf die Daten zuzugreifen. Wer in diesem Sinne in die Hausgewalt des potentiellen Treugebers eingebunden sei, könne nicht Treuhänder sein. Gehe es um bewegliche Sachen des Arbeitgebers, auf die der Arbeitnehmer im Rahmen des Arbeitsverhältnisses Zugriff habe, gingen Lehre und Rechtsprechung vom Mitgewahrsam des Arbeitsgebers und des Arbeitnehmers aus. Der Bruch von Mitgewahrsam entspreche einem Wegnehmen im Sinne

von Art. 139 Ziff. 1 StGB. Es sei naheliegend, diese Praxis auch auf den "Datendiebstahl" anzuwenden. Allerdings gehe das Bundesgericht im Gegensatz zur herrschenden Lehre bei "Mitgewahrsam" an Forderungen, d.h. bei konkurrierenden Bankvollmachten, ebenfalls von einem Treuhandverhältnis aus. Dies sei historisch bedingt und habe ursprünglich die Schliessung einer störenden Strafbarkeitslücke, die aufgetreten sei, da es keinen "Forderungsdiebstahl" gebe, bezweckt. Diese Lücke sei längst durch den Tatbestand des "Ermächtigungsmissbrauchs" im Sinne von Art. 158 Ziff. 2 StGB behoben. Dass die von der Lehre kritisierte Rechtsprechung fortbestehe, sei auf das Bedürfnis zurückzuführen, auf berufsmässige Vermögensverwalter, die sich durch Ermächtigungsmissbrauch unrechtmässig bereicherten, den verschärften Strafrahmen von Art. 138 Ziff. 2 StGB anzuwenden. Es wäre paradox, dieser Rechtsprechung eine Reflexwirkung auf Art. 143 StGB angedeihen zu lassen und dadurch die Strafbarkeit des "Datendiebstahls" unsachgemäss einzuschränken (Urk. 9 S. 11 f. Ziff. 24 - 26).

Der von der Staatsanwaltschaft vorgetragene Vergleich des Mitgewahrsams von Arbeitgeber und Arbeitnehmer bezüglich beweglicher Sachen und bezüglich Daten vermag nicht zu überzeugen. Die Weitergabe einer beweglichen Sache durch den Arbeitnehmer an einen Dritten führt dazu, dass diese aus dem Einflussbereich des Arbeitsgebers entfernt wird, womit der Mitgewahrsam des Arbeitgebers gebrochen wird. Daten lassen sich jedoch kopieren. Die blosse Weitergabe von Daten durch den Arbeitnehmer bedeutet also nicht, dass der Arbeitgeber auf diese keinen Zugriff mehr hat. Damit wird der Mitgewahrsam des Arbeitsgebers nicht gebrochen. Daran ändert nichts, dass die fraglichen Daten möglicherweise als Folge der Weitergabe an einen unbefugten Dritten nicht mehr dem ursprünglichen Zweck entsprechend verwendet werden können oder massiv an Wert verlieren. Es liegt nach wie vor der nicht von Art. 143 StGB umfasste Tatbestand der "Datenveruntreuung" vor. Unter welchen Straftatbestand dieser zu subsumieren, ist im vorliegenden Beschwerdeverfahren nicht zu prüfen.

c) Voraussetzung der unbefugten Datenbeschaffung im Sinne von Art. 143 Abs. 1 StGB ist, dass die Daten gegen den unbefugten Zugriff des konkreten Täters besonders gesichert sind, wobei diese Sicherung physisch (z.B. Verschliessen des

Computerraums) oder elektronisch (z.B. Verwenden von Passwörtern) erfolgen kann. Es muss für den potentiellen Täter klar ersichtlich sein, dass gerade sein Zugang zu den Daten unerwünscht sei (Weissenberger, Basler Kommentar, a.a.O., N 18 zu Art. 143 StGB; Trachsel/Crameri, Praxiskommentar, a.a.O., N 6 zu Art. 143 StGB).

Die Staatsanwaltschaft bringt vor, sie habe im Januar und Februar 2013, als sie die angefochtenen Anordnungen getroffen habe, über die Informationen verfügt, der Beschwerdeführer sei ein ehemaliger Mitarbeiter der C._____ und habe aufgrund seiner Stellung vermutlich Zugriff auf die inkriminierte Datei gehabt. Ferner habe die Staatsanwaltschaft ganz zu Beginn der Untersuchung die Information erhalten, gegen unbefugte Entwendungen von Daten durch Mitarbeitende gebe es bei der C._____ klare rechtliche und auch gewisse technische Sicherheiten. Die technischen Sicherheiten hätten sich im Lauf der Jahre verbessert. Die zu Beginn von der C._____ vorgelegten Unterlagen (UH130229 Urk. 7/011013 f., 011015ff.) bezögen sich zwar nicht ausdrücklich auf das Problem, dass ein Mitarbeiter Daten in sein eigenes Computersystem übertrage, zeigten aber, dass die C._____ komplexe organisatorische Vorkehren treffe, um eine rigide Kontrolle über den Umgang ihrer Mitarbeitenden mit ihren Daten auszuüben. Es sei zudem notorisch, dass die Datensicherheit bei den Schweizer Banken einen äusserst hohen Stellenwert einnehme, besonders wenn es um Kundendaten gehe. Ferner sei es dem fallführenden Staatsanwalt auch deshalb als glaubhaft erschienen, dass bei der C._____ technische und rechtliche Sicherheiten gegen Datenentwendungen durch Mitarbeitende bestünden, weil dies dem gegenwärtigen Standard für grössere Betriebe mit sensiblen Daten entspreche und beispielsweise auch im Bereich Strafverfolgung Erwachsene des Kantons Zürich so sei. Insbesondere bei der Übertragung von Daten auf USB-Memory-Sticks oder CD/DVD-Roms gäbe es verschiedene technische Hürden zu überwinden. Aufgrund all dieser Umstände habe kein Anlass bestanden, zu Beginn der Untersuchung ernsthaft zu bezweifeln, dass die Massnahmen der C._____ gegen Datenentwendungen dem Massstab von Art. 143 StGB genügten. Vielmehr habe dies unter dem Gesichtspunkt des Tatverdachts bejaht werden dürfen.

Die Staatsanwaltschaft verweist auf ihre weiteren im August 2013 - und damit nach Anordnung der fraglichen Überwachungsmassnahmen - angestellten Abklärungen zur Datensicherung bei der C._____. Gemäss Bericht der C._____ zum Informationsschutz (UH130229 Urk. 7/070220 ff.) sei die Verwendung der USB-Ports und der CD/DVD-Laufwerke seit April 2009 technischen Restriktionen unterworfen gewesen (070229). Mitte 2011 sei zudem ein Meldesystem bei "Data Leckage" implementiert gewesen (070223). Aus dem Bericht gehe hervor, dass die Mitarbeiter auch ausserhalb der C._____ AG die Geschäftsdaten über deren gesicherte Computersysteme hätten nutzen können (070228), so dass es kaum je einen Grund dafür geben könne, einem Mitarbeiter den Datenexport auf ein privates System zu erlauben. Der Datenexport via Internet sei seit Herbst 2008 durch verschärfte Kriterien zur Filterung von Internet-Adressen minimiert (070228). Daten könnten bei der C._____ nur hausintern ausgedruckt werden, wobei alle Druckaufträge aufgezeichnet würden und auswertbar seien (070229). Technische Schutzrichtlinien bestünden auch für C._____-E-Mails (070205). Jeder Datenexport werde durch Art. 14 Abs. 3 des Mitarbeiterreglements (UH130229 Urk. 7/070119) und den gleichlautenden Art. 14 Abs. 3 des Arbeitsvertragsreglements Direktion (UH130229 Urk. 7/070148) untersagt:

"Es ist dem Arbeitnehmer untersagt, dem Geschäfts- und/oder dem Bankkundengeheimnis unterstehende Daten aller Art und unabhängig von der Form ohne betriebliche Notwendigkeit zu verwenden, insbesondere auch, diese auf externe Speichermedien oder externe Datenverarbeitungssystem zu übertragen."

Es sei schon bei der Anordnung der Überwachungsmassnahmen kein Grund ersichtlich gewesen, weshalb die C._____ dem Beschwerdeführer je im Sinne einer Ausnahme erlaubt haben sollte, 76'000 detaillierte Kundenstämme auf seine privaten Computer zu übertragen. Sollte der Beschwerdeführer mit "B._____" identisch sein, so müsse er die Daten irgendwann unbefugt auf private Datenträger übertragen haben, denn auf eine interne Quelle habe er am 29. November 2012 (Datum des E-Mails von "B._____" an verschiedene Banken mit dem fraglichen Angebot) keinen Zugriff mehr gehabt. Selbst wenn er intern über eine Zugriffsberechtigung betreffend die inkriminierte Datei verfügt haben sollte, müsste er irgendwann die Daten ohne Berechtigung und unter Überwindung von technischen Schranken in ein privates System exportiert haben. Damit seien die Vorausset-

zungen für eine unbefugte Datenbeschaffung erfüllt (Urk. 9 S. 12 - 14 Ziff. 27 - 30).

Mit ihren Vorbringen zeigt die Staatsanwaltschaft allenfalls auf, dass die Person, welche am 29. November 2012 unter dem Namen "B._____" verschiedenen Banken 76'000 Kundenstämme der C._____ zum Kauf angeboten hatte, sollte es sich um einen Mitarbeiter der C._____ gehandelt haben, in durch das Mitarbeiterreglement verbotener Weise eine Kopie der betreffenden Datei erstellt hat und dass die technischen Schutzmassnahmen die Kopierung der Datei nicht verhindert und nicht in später nachvollziehbarer bzw. dem Täter zuordnungsbarer Weise registriert haben. Sie zeigt aber nicht auf, dass der Beschwerdeführer, sollte er "B._____" sein, tatsächlich eine technische Schranke hätte überwinden müssen, um die besagte Datei auf einen externen Datenträger übertragen zu können.

Es bleibt deshalb dabei, dass der Beschwerdeführer aufgrund seiner Stellung Zugang zu den fraglichen Daten hatte, diese also "für ihn bestimmt" waren, weshalb keine unbefugte Datenbeschaffung im Sinne von Art. 143 StGB vorliegt. Eine andere "Katalogtat" im Sinne von Art. 269 Abs. 2 StPO wird von der Staatsanwaltschaft nicht zur Begründung der Echtzeitüberwachung angeführt und ist auch nicht ersichtlich.

3. Liegt keine "Katalogtat" bzw. kein Verdacht, dass eine solche begangen wurde, vor, so fehlt es an einer Voraussetzung zur Anordnung einer Echtzeitüberwachung, weshalb die auf einer solchen beruhenden Aufzeichnungen nicht ausgewertet und die daraus sich ergebenden Erkenntnisse nicht verwertet werden dürfen. Dies mag unbefriedigend sein, ist aber Folge der gesetzlichen Regelung von Art. 269 StPO, in welchem die Zulässigkeit nicht bloss von allgemeinen Voraussetzungen (dringender Verdacht, Schwere der Straftat, Erfolglosigkeit der bisherigen Untersuchungshandlungen oder Aussichtslosigkeit bzw. unverhältnismässige Erschwerung der Ermittlungen ohne eine solche Überwachung; Art. 269 Abs. 1 StPO) abhängig gemacht wird. Vielmehr hat der Gesetzgeber eine abschliessende Aufzählung von Straftaten ("Katalogtaten"), deren Verfolgung die Echtzeitüberwachung erlaubt, ins Gesetz aufgenommen. Diese Einschränkung ist von den rechtsanwendenden Behörden zu respektieren.

Somit ist die Echtzeitüberwachung des Mobiltelefonanschlusses sowie des elektronischen Postdienstes und Internetzugangs und -verkehrs des Beschwerdeführers zu Unrecht angeordnet worden. Dasselbe gilt für die Auswertung der darauf beruhenden Aufzeichnungen.

Nicht zu überzeugen vermag das Argument der Staatsanwaltschaft, selbst wenn die Beschwerdeinstanz zur Auffassung gelangen sollte, die angeordneten Überwachungsmassnahmen seien zu Unrecht genehmigt worden, hätte dies nicht die Unverwertbarkeit des Zufallsfunds zur Folge, denn dieser sei im Rahmen einer ordnungsgemäss und in guten Treuen angeordneten und genehmigten Überwachungsmassnahme entdeckt worden (Urk. 9 S. 14 Ziff. 32). Im Gegensatz zur vorliegend nicht angefochtenen ursprünglichen Überwachung des noch unbekannten Nutzers der E-Mail-Adresse "…" (Verfügung der Staatsanwaltschaft vom 4. Dezember 2012) richtete sich die Überwachung gemäss Verfügungen vom 31. Dezember 2012 und 10. Januar 2013 ausdrücklich gegen den Beschwerdeführer. Sein Zugang zu den fraglichen Daten aufgrund seiner Stellung bei der C._____ war der Staatsanwaltschaft bekannt oder hätte sie bei der C._____, was die Einzelheiten angeht, grundsätzlich abklären können. Lässt die Staatsanwaltschaft eine Überwachung aufgrund besonderer Dringlichkeit oder wegen fehlerhafter rechtlicher Würdigung ohne vorherige diesbezügliche Abklärung durchführen, trägt sie das Risiko, dass die gewonnenen Erkenntnisse allenfalls nicht verwendet werden können und kann dieses nicht unter dem Titel der ordnungsgemäss und in guten Treuen angeordneten und genehmigten Überwachungsmassnahme auf den Beschwerdeführer abwälzen.

4. a) Die Staatsanwaltschaft ordnete die Überwachung des Mobiltelefonanschlusses und des elektronischen Postdienstes und Internetzugangs und -verkehrs des Beschwerdeführers nicht nur im Sinne einer Echtzeitüberwachung (Art. 269 StPO), sondern auch im Sinne einer rückwirkenden Überwachung (Verkehrsdaten, Art. 273 StPO) an. Voraussetzung einer solchen Überwachung ist neben dem dringenden Tatverdacht, dass die Schwere der Straftat die Überwachung rechtfertigt und dass die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig er-

schwert würden (Art. 273 Abs. 1 StPO in Verbindung mit Art. 269 Abs. 1 lit. b und c StPO). Nicht vorausgesetzt ist, dass eine "Katalogtat" im Sinne von Art. 269 Abs. 2 StPO verfolgt wird. Es genügt, dass der dringende Tatverdacht ein Verbrechen oder Vergehen (oder eine hier nicht zur Diskussion stehende Übertretung von Art. 179^{septies} StGB, Missbrauch einer Fernmeldeanlage) betrifft. In der Folge ist zu prüfen, ob die angeordnete rückwirkende Überwachung zulässig war.

Die angebotene Weitergabe von Kundendaten durch den Beschwerdeführer, sollte er "B._____" sein, dürfte zumindest eine Verletzung des Bankkundengeheimnisses im Sinne von Art. 47 Abs. 1 lit. a BankenG darstellen. Eine solche Tat wird mit Gefängnis bis zu drei Jahren oder mit Geldstrafe bestraft, ist also ein Vergehen (Art. 10 Abs. 3 StGB). Angesichts des Umfangs der Tatbegehung und dem gezielten Vorgehen (76'000 Datensätze, Angebot an mehrere Banken) liegt entgegen der Ansicht des Beschwerdeführers (Urk. 2 S. 11 Ziff. 29) eine Schwere der Straftat vor, welche im Sinne von Art. 273 Abs. 1 StPO in Verbindung mit Art. 269 Abs. 1 lit. b StPO die Überwachung rechtfertigt.

b/aa) E._____, Executive Director Group Security Service der C._____ (vgl. Visitenkarte, UH130229 Urk. 7/011005) bezeichnete in einem E-Mail vom 28. Dezember 2012, welches in Kopie an den fallverantwortlichen Staatsanwalt ging, den Beschwerdeführer als "potentiellen Täter". Er hielt fest, dieser sei per 1. April 1990 in die Dienste der damaligen C1._____ eingetreten und sukzessive befördert worden, zuletzt per 1. März 2007 zum stellvertretenden Direktor. Er habe zahlreiche Funktionen bekleidet, so unter anderem die Leitung des Teams Daten & Analyse per 1. Februar 2008, die Leitung des Ressorts Management Office des … Management Schweiz per 1. September 2009 (mit den Einheiten … Segment Management, … Sales Management, … Fachführung sowie … Management Office) und die Leitung des Ressorts Business Management per 1. Januar 2011. In den beiden letztgenannten Funktionen sei er direkt dem Segmentsleiter … Management Schweiz unterstellt und an zentraler und leitender Stelle für dasjenige Kundensegment zuständig gewesen, aus welchem die Kundendaten angeboten würden. Der Zugang zu den entsprechenden Daten erscheine naheliegend bzw. möglich.

Zum möglichen Motiv hielt E._____ fest, aufgrund von "organisatorischen Anpassungen" (Anführungs- und Schlusszeichen durch E._____ gesetzt) sei der Beschwerdeführer schliesslich nicht mehr weiter beschäftigt worden. Sein letzter Arbeitstag sei der 22. November 2011 gewesen. Der formelle Austritt sei per 31. Oktober 2012 erfolgt. Auf das Datum des Austritts hin habe der Beschwerdeführer eine Abgangsentschädigung im Betrag von Fr. 213'400.-- erhalten. Die vom Arbeitgeber initiierte Trennung nach über 20 Jahren intensiver und loyaler Tätigkeit könnte Grundlage für ein entsprechendes Motiv sein. Die Adressierung an Segments-Chefs von Konkurrenzbanken (z.B. F._____ Private Banking) liessen sich mit seiner businessnahen Position vereinbaren. Ziel könne neben Geld auch ein Nadelstich gegen seinen ehemaligen Vorgesetzten, den Segmentshead, sein. Der Täter wolle das Management treffen, aber nicht die Bank als Ganzes schädigen. Durch die scheinbar weitgestreute Auswahl von Banken habe er einen Massenversand vorgetäuscht. Der Umstand, dass der Täter Kunden mit dem Namen "Meier" gewählt habe, deute auf Schonung hin. Es scheine ihm ein Anliegen zu sein, nicht die Kunden zu schädigen, sondern seinem ehemaligen Arbeitgeber / Vorgesetzten eins auszuwischen. Durch die Auswahl der "Meier" exponiere er auch keine Prominenten.

Der Beschwerdeführer, so E._____ weiter, verfüge über einen militärischen und nachrichtendienstlichen Hintergrund. Er habe während seiner Anstellung regelmässig unbezahlten Urlaub bezogen, um Militärdienst im … Bundesheer / Nachrichtendienst zu leisten. E._____ nahm weiter eine Sprachanalyse des fraglichen Anbietermails vor: Diese lasse den Beschwerdeführer als möglichen Autor erscheinen. So deute dieses auf eine Person hin, welche sowohl einen Bezug zur Schweiz habe ("Natel, "Büro"-Nummer). Der Gebrauch des Doppel"ss", "sz" deute auf eine nicht schweizerische, möglicherweise … sprachliche Orientierung hin, so auch Formulierungen wie "hiermit möchte ich … anbieten", "möge mir der Unterhändler … seine Kontaktdaten mitteilen". Ein höfliches, gepflegtes muttersprachliches Deutsch, "Austausch Ware gegen Geld", deute auf einen akademischen, ökonomischen Background. Präzise Anweisungen könnten auf einen militärischen Hintergrund hinweisen. Die Wahl des Pseudonyms B._____ liesse sich mit ihm eigenen Esprit / Witz vereinbaren (UH130229 Urk. 7/050087 f.)

In erster Linie aufgrund dieser Ausführungen von E._____ ordnete die Staatsanwaltschaft am 31. Dezember 2012 die Überwachung des Mobiltelefons des Beschwerdeführers und hernach die weiteren Überwachungen und Auswertungen an.

bb) Der Beschwerdeführer hält dafür, die von der C._____ angeführten Gründe vermöchten keinen dringenden Tatverdacht zu begründen. Die C._____ selber schreibe von einer blossen Hypothese. Auch die Staatsanwaltschaft vermöge lediglich vorzutragen, dass die von der C._____ vorgebrachten Verdachtsgründe "für sich genommen einem dringenden Tatverdacht zumindest nahe" seien. Sie stelle deshalb auf verschiedene Äusserungen von "B._____" gegenüber dem verdeckten Ermittler ab, welche auf den Beschwerdeführer deuten würden und womit der Tatverdacht sich zur Dringlichkeit steigern würde. In diesem Zusammenhang bringe die Staatsanwaltschaft vor, dass "B._____" die Daten nicht Enkelkind-Betrügern, sondern nur einer Institution anbieten wolle, welche die Daten "einen sinnvollen und ethisch verantwortbaren Verwendung zuführen" werde. Dies sei vereinbart mit der Geschichte des Beschwerdeführers, der zwar die C._____ ärgern möchte, aber eine gewisse Treue und Verantwortung gegenüber den Kunden bewahrt habe. Weiter werde vorgetragen, dass "B._____" von verschiedenen Sicherheitsfirmen und nachrichtendienstlichen Personen spreche, was auf den Beschwerdeführer hinweise, der im Nachrichtendienst … tätig sei (siehe Gesuch der Staatsanwaltschaft an das Zwangsmassnahmengericht am Obergericht vom 31. Dezember 2013, UH130229 Urk. 7/024016 ff.).

Die von der C._____ vorgebrachten Punkte, so der Beschwerdeführer weiter, vermöchten allenfalls einen Hinweis auf eine mögliche Täterschaft liefern, nicht aber einen dringenden Tatverdacht zu begründen. Dies erkenne nicht bloss die C._____, sondern auch die Staatsanwaltschaft. Auch die Argumente der Staatsanwaltschaft, welche diese glaube, aus der Korrespondenz zwischen "B._____" und dem verdeckten Ermittler ziehen zu können, hielten einer Hinterfragung nicht stand. Das vermeintliche "Verantwortungsbewusstsein" "B._____s" sei wohl kaum einzigartig und dürfte auf zahlreiche aktuelle und ehemalige Mitarbeiter sowie allenfalls auch auf Externe zutreffen und damit kaum geeignet sein, einen konkre-

ten Tatverdacht zu erhärten. Das Gleiche gelte für den Verweis auf den nachrichtendienstlichen Hintergrund des Beschwerdeführers. Sein nachrichtendienstlicher Beitrag bestehe im Verfassen wirtschaftlicher Länder- und Regionenberichte sowie in der Beurteilung deren potenzieller sicherheitspolitischer Implikationen zuhanden … Behörden.

Mangels dringenden Tatverdachts, so der Beschwerdeführer weiter, erwiesen sich die Überwachungsmassnahmen als unzulässig. Infolgedessen seien auch die darauf basierende Nutzung von Login-Daten und die Verwertung von Zufallsfunden unzulässig und daraus folgende Erkenntnisse unverwertbar (Urk. 2 S. 9 f. Ziff. 25 - 27).

cc) Die Anordnung von Überwachungsmassnahmen erfordert zwar einen dringenden Tatverdacht, nicht aber bereits eine nahezu die Gewissheit der Täterschaft herbeiführende Beweislage. Weiter spielt eine Rolle, dass blosse Randerhebungen bedeutend weniger in die Rechte des Betroffenen eingreifen als die Erhebung der Kommunikationsinhalte, weshalb für eine Überwachung nach Art. 273 StPO weniger hohe Anforderungen zu stellen sind als für eine Überwachung nach Art. 269 StPO (Thomas Hansjakob, in Donatsch/Hansjakob/Lieber, Kommentar zur schweizerischen Strafprozessordnung, Zürich 2010, N 9 zu Art. 273 StPO; Marc Jean-Richard-dit-Bressel, in Niggli/Heer/Wiprächtiger, Schweizerische Strafprozessordnung, Basler Kommentar, a.a.O., N 4 zu Art. 273 StPO)

Es trifft wohl zu, dass die einzelnen von E._____ (C._____) und von der Staatsanwaltschaft genannten Verdachtsmomente auf zahlreiche Personen insbesondere im Umfeld der C._____ zutreffen: sprachliche Gepflogenheiten, welche auf intensive Verbindungen zur Schweiz ("Natel" für Mobiltelefon), jedoch auch zum weiteren deutschsprachigen Raum (Verwendung des Doppel-S; "ß" im schriftlichen Verkehr) hinweisen, Verlust des Arbeitsplatzes bei der C._____, berufsbedingter Zugang zu Daten der C._____, präzise und ökonomisch geprägte Ausdrucksweise, usw.). Jedes einzelne Element vermag für sich allein noch keinen dringenden Tatverdacht begründen. Bemerkenswert ist jedoch die Kombination dieser Elemente, welche nicht häufig auftritt. Wird noch berücksichtigt, dass der Beschwerdeführer in eben jenem Bereich der C._____ eine leitende Stellung inne

hatte, aus welchem die von "B._____" angebotenen Kundendaten stammen, so drängt sich der Verdacht - der eben nicht einer Gewissheit gleichzusetzen ist - auf, dass der Beschwerdeführer "B._____" sei oder diesem zumindest nahe stehe.

Somit waren die Voraussetzungen zur Anordnung einer rückwirkenden Überwachung des Mobiltelefonanschlusses und des elektronischen Postdienstes und Internetzugangs und -verkehrs des Beschwerdeführers im Sinne von Art. 273 StPO erfüllt, weshalb diesbezüglich die Beschwerde abzuweisen ist.

Es wird Sache der Staatsanwaltschaft und allenfalls des erkennenden Gerichts sein, zu prüfen, wie weit die Auswertung der Überwachung und die Zufallsfunde verwertbare Früchte der zulässigen rückwirkenden Überwachung oder unverwertbare Früchte der unzulässigen Echtzeitüberwachung sind.

5. Die Regelung der Kosten- und Entschädigungsfolgen hat im Endentscheid zu erfolgen (Art. 421 Abs. 1 StPO). Ebenfalls wird im Endentscheid darüber zu befinden sein, ob dem Beschwerdeführer für die teilweise unzulässige Überwachung eine Genugtuung zuzusprechen sei (vgl. Antrag 3 der Beschwerde).

Die Gerichtsgebühr für das Beschwerdeverfahren ist zuhanden der das Strafverfahren abschliessenden Strafbehörde in Beachtung der Bemessungskriterien von § 2 Abs. 1 lit. b-d GebV OG (Bedeutung des Falls, Zeitaufwand des Gerichts, Schwierigkeit des Falls) und gestützt auf § 17 Abs. 1 GebV OG auf Fr. 800.-- festzusetzen.

Es wird beschlossen:

1. In teilweiser Gutheissung der Beschwerde wird festgestellt, dass die Echtzeitüberwachungen des Mobiltelefonanschlusses und des elektronischen Postdienstes und Internetzugangs des Beschwerdeführers gemäss Verfügungen der Staatsanwaltschaft III des Kantons Zürich vom 31. Dezember 2012 und vom 10. Januar 2013 unzulässig waren.

   Entsprechend war die Nutzung von Login-Daten gemäss Verfügung der Staatsanwaltschaft III des Kantons Zürich vom 20. Februar 2013 und die Verwertung des sich daraus ergebenden Zufallsfunds unzulässig, soweit diese auf der Echtzeitüberwachung gemäss Art. 269 StPO beruhen.

2. Betreffend die mit den gleichen Verfügungen der Staatsanwaltschaft III des Kantons Zürich angeordneten rückwirkenden Überwachungen gemäss Art. 273 StPO und einer allfälligen Nutzung und Verwertung der sich daraus ergebenden Erkenntnisse wird die Beschwerde abgewiesen.

3. Die Gerichtsgebühr wird auf Fr. 800.-- festgesetzt.

4. Die Regelung der Kosten- und Entschädigungsfolgen erfolgt im Endentscheid.

5. Schriftliche Mitteilung an:

   - Rechtsanwalt MLaw X._____, zweifach, für sich und zuhanden des Beschwerdeführers, per Gerichtsurkunde
   - die Staatsanwaltschaft III des Kantons Zürich, ad A-1/2012/582, gegen Empfangsbestätigung

   und nach Ablauf der Rechtsmittelfrist bzw. nach Erledigung allfälliger Rechtsmittel:

   - an die zentrale Inkassostelle der Gerichte (elektronisch)

6. Rechtsmittel:
   Gegen diesen Entscheid kann unter den einschränkenden Voraussetzungen von Art. 93 des Bundesgerichtsgesetzes **Beschwerde in Strafsachen** erhoben werden.

Die Beschwerde ist innert **30 Tagen**, vom Empfang an gerechnet, bei der Ersten öffentlich-rechtlichen Abteilung des Bundesgerichtes (1000 Lausanne 14) in der in Art. 42 des Bundesgerichtsgesetzes vorgeschriebenen Weise schriftlich einzureichen.
Die Beschwerdelegitimation und die weiteren Beschwerdevoraussetzungen richten sich nach den massgeblichen Bestimmungen des Bundesgerichtsgesetzes.

Zürich, 12. Dezember 2013

Obergericht des Kantons Zürich
III. Strafkammer

Präsident:	Gerichtsschreiber:
lic. iur. Th. Meyer	Dr. iur. J. Hürlimann