dsb
datenschutzbeauftragter
kanton zürich

Universität
Zürich

Datenbekanntgabe an Strafverfolgungsbehörde – Bericht der Kontrolle

Inhaltsverzeichnis

Zusammenfassung

Die Universität Zürich erstattete im September 2012 Strafanzeige wegen Verdachts der Amtsgeheimnisverletzung, nachdem in den Medien Berichte betreffend das Medizinhistorische Institut und Museum der Universität veröffentlicht worden waren. Im Herbst 2013 wurde bekannt, dass die Universität der Staatsanwaltschaft verschiedene Daten von Angehörigen der Universität sowie von Dritten herausgegeben hatte und dazu eine unbekannte Menge an Telefon- und E-Mail-Daten auf bestimmte Kontakte hin überprüft worden waren.

Der Datenschutzbeauftragte leitete darauf bei der Universität eine Kontrolle ein, um die Rechtmässigkeit dieser Datenbearbeitungen zu prüfen.

Die Kontrolle ergab, dass die Universität unrechtmässig Telefon- und E-Mail-Verkehrsdaten ihrer Mitarbeitenden und Studierenden sowie von Mitarbeitenden externer Stellen und assoziierter Institute ausgewertet hatte. Aufgrund der Ergebnisse wurden Daten von Personen, die Verbindungen mit bestimmten Telefonnummern hatten oder E-Mails an bestimmte E-Mail-Adressen oder E-Mail-Domains sandten, an die Staatsanwaltschaft herausgegeben. Für die Auswertungen, die dem Vorgehen einer Rasterfahndung entsprachen, verfügt die Universität über keine Rechtsgrundlagen, und die Auswertungen waren auch nicht verhältnismässig. Die Weitergaben der Daten an die Staatsanwaltschaft erfolgten zwar gestützt auf Bestimmungen über die strafprozessuale Rechtshilfe, verletzten jedoch – da die Daten unrechtmässig beschafft worden waren – überwiegende private Interessen der betroffenen Personen und waren deshalb ebenfalls unrechtmässig. Die Universität gab ausserdem einzelne E-Mail-Inhalte, ganze E-Mailboxen, eine Datenbank sowie einzelne Wohnadressen weiter. Die Weitergaben der E-Mail-Inhalte sowie der Datenbank erwiesen sich ebenfalls als unrechtmässig.

Die Ergebnisse der Kontrolle wurden der Universität mitgeteilt. Die Universität wird aufgefordert, Massnahmen zu treffen, dass sich solche Ereignisse nicht wiederholen, sowie die Betroffenen über die vorgenommenen Auswertungen und Datenweitergaben an die Staatsanwaltschaft zu informieren. Über die Umsetzung der Massnahmen ist dem Datenschutzbeauftragten Bericht zu erstatten.

1 Ausgangslage

Der Datenschutzbeauftragte erfuhr aus verschiedenen Medienberichten vom 1. und 2. November 2013 sowie der Medienmitteilung der Universität Zürich vom 1. November 2013, dass die Universität der Staatsanwaltschaft des Kantons Zürich im Rahmen von Ermittlungen wegen Verletzung des Amtsgeheimnisses verschiedene Daten von Angehörigen der Universität sowie von Dritten herausgegeben hat. Die Ermittlungen standen im Zusammenhang mit den Ereignissen am Medizinhistorischen Institut und Museum der Universität.

Gemäss den Medienberichten wurden verschiedene Personen, welche nicht am Medizinhistorischen Institut und Museum bzw. an der Universität angestellt sind, von den Strafverfolgungsbehörden als Auskunftspersonen einvernommen, weil sie im tatrelevanten Zeitraum Kontakt mit Journalisten gehabt hatten.[1] Dies deutete darauf hin, dass eine unbekannte Menge an Telefon- und E-Mail-Daten auf bestimmte Kontakte hin überprüft worden war. Von einem solchen Vorgehen sind eine Vielzahl von Personen in ihrem Grundrecht auf Schutz der Privatsphäre und informationelle Selbstbestimmung (Art. 10 und 13 Bundesverfassung, BV, SR 101) betroffen. Es stellt sich die Frage der Rechtmässigkeit des Vorgehens.

Dies veranlasste den Datenschutzbeauftragen, bei der Universität eine Kontrolle einzuleiten und den Sachverhalt und die Rechtslage abzuklären.

2 Kontrolle

Der Datenschutzbeauftragte berät die öffentlichen Organe und privaten Personen in Fragen des Datenschutzes, vermittelt bei Streitigkeiten und beaufsichtigt die Datenbearbeitungen der öffentlichen Organe (§ 34 Gesetz über die Information und den Datenschutz, IDG, LS 170.4). Im Rahmen seiner Kontrollbefugnisse kann er bei öffentlichen Organen ungeachtet einer allfälligen Geheimhaltungspflicht Auskunft über das Bearbeiten von Personendaten einholen, Einsicht in die Daten nehmen und sich Bearbeitungen vorführen lassen (§ 35 IDG). Stellt er eine Verletzung von Bestimmungen über den Datenschutz fest, gibt er eine Empfehlung ab, welche Massnahmen zu ergreifen sind (§ 36 IDG). Er und seine Mitarbeitenden sind in Bezug auf Informationen, die sie bei ihrer Tätigkeit zur Kenntnis nehmen, zur gleichen Verschwiegenheit verpflichtet wie das öffentliche Organ (§ 38 IDG).

Mit Schreiben vom 6. November 2013 gelangte der Datenschutzbeauftragte zwecks Abklärung des Sachverhalts an die Universität. Es wurden diverse Fragen gestellt sowie Unterlagen verlangt. Die Universität nahm mit Schreiben vom 20. November

[1] NZZ vom 1. November 2013, S. 15; Tages-Anzeiger vom 1. November 2013, S. 15; Limmattaler Zeitung online vom 2. November 2013; Tages-Anzeiger online vom 4. November 2013.

2013 zu den Fragen Stellung. Da der Sachverhalt noch nicht geklärt war, stellte der Datenschutzbeauftragte mit Schreiben vom 12. Dezember 2013 weitere Fragen und forderte die Universität nochmals auf, die Antworten mit den entsprechenden Unterlagen zu dokumentieren. Mit Schreiben vom 30. Januar 2014 kam die Universität der Aufforderung nach.

3 Sachverhalt

Aus den von der Universität erteilten Auskünften und eingereichten Unterlagen geht hervor, dass die Universität im Rahmen von Strafuntersuchungen betreffend Amtsgeheimnisverletzung verschiedene Datenbearbeitungen vorgenommen und der Staatsanwaltschaft verschiedene Kategorien von Personendaten herausgegeben hat. Der Datenschutzbeauftragte geht von folgendem – in datenschutzrechtlicher Hinsicht relevanten – Sachverhalt aus.

3.1 Chronologisch

- Die Universität erstattete am 19. September 2012 Strafanzeige gegen Unbekannt wegen Verdachts der Amtsgeheimnisverletzung, nachdem am 11. September 2012 im Tages-Anzeiger ein Artikel über die Tätigkeit von Prof. Christoph Mörgeli am Medizinhistorischen Museum der Universität erschienen war. Anschliessend folgten weitere Berichte in der Presse und im Fernsehen. Diese enthielten Informationen aus zwei das Medizinhistorische Institut und Museum betreffenden Berichten (Akademischer Bericht 2011 und Bericht der Expertenkommission unter der Leitung von Prof. Robert Jütte). Am 15. bzw. 16. September 2012 erschienen Artikel in der Presse, unter anderem in „Der Sonntag“, in welchen berichtet wurde, dass die Universität Prof. Christoph Mörgeli entlassen wolle.
- Die Staatsanwaltschaft gelangte mit Schreiben vom 4. Oktober 2012 an die Universität mit der Bitte, die Randdaten bzw. Verkehrsdaten[2] sämtlicher Telefonanschlüsse des Medizinhistorischen Instituts für den Zeitraum 8.-16. September 2012 von ihrer Fernmeldedienstanbieterin edieren und der Staatsanwaltschaft zukommen zu lassen.
- Die Universität teilte der Staatsanwaltschaft am 8. Oktober 2012 per E-Mail mit, dass sie betreffend das Editionsbegehren vom 4. Oktober 2012 zur Verfügung stehe.

[2] Informatik- und Telekommunikationssysteme brauchen für die Abwicklung technischer Prozesse eigenständig Daten. Allgemein werden diese Daten als Randdaten bezeichnet. Im Bereich der Telekommunikation spricht man auch von Verkehrsdaten. Telefon-Verkehrsdaten enthalten Angaben, von welchem Telefonanschluss mit welchen anderen Telefonanschlüssen zu welchem Zeitpunkt wie lange kommuniziert wurde. E-Mail-Verkehrsdaten sagen aus, von welcher E-Mail-Adresse mit welchen Empfängeradressen zu welchem Zeitpunkt kommuniziert wurde.

- Mit E-Mail vom 9. Oktober 2012 dehnte die Staatsanwaltschaft die Anfrage auf die Erhebung der Verkehrsdaten sämtlicher Mobil- und Festnetzanschlüsse der Universität für den Zeitraum 1. Januar 2012 - 30. September 2012 aus und verlangte Auskunft über alle Verbindungen mit bestimmten, von ihr vorgegebenen Telefonnummern – dies nachdem gleichentags ein telefonischer Kontakt zwischen der Universität und der Staatsanwaltschaft stattgefunden und die Universität der Staatsanwaltschaft eine E-Mail geschickt hatte. Die Universität hatte der Staatsanwaltschaft mitgeteilt, dass sie die Daten sämtlicher universitätsinterner Anschlüsse selber erheben könne.
- Die Universität nahm eine Auswertung sämtlicher in das Telefon-Netzwerk der Universität integrierten Festnetzanschlüsse sowie der von der Universität abonnierten Mobilanschlüsse hinsichtlich Verbindungen mit bestimmten Telefonnummern vor und lieferte der Staatsanwaltschaft die Resultate in zwei Tranchen. Am 12. Oktober 2012 gab die Universität das Resultat der Auswertung der Telefon-Verkehrsdaten der Festnetzanschlüsse, welche für den Zeitraum 1. Januar 2012 - 10. Oktober 2012 überprüft worden waren, sowie der Mobilanschlüsse, welche für den Zeitraum 1. Januar 2012 - 31. August 2012 überprüft worden waren, heraus. Am 20. November 2012 folgte die Herausgabe des Resultats der Überprüfung der Mobilanschlüsse für den Zeitraum 1. September 2012 - 31. Oktober 2012. Von den beiden Datenherausgaben betroffen waren 66 Festnetz- und Mobilanschlüsse, die persönlich genannten Mitarbeitenden der Universität zugeordnet werden konnten, zehn Sammelanschlüsse der Universität, welche verschiedenen Personen zugänglich waren, vier Anschlüsse des Staatsarchivs, ein Anschluss des Kinderspitals, ein Anschluss des Europa Instituts Zürich, zwei Anschlüsse des Tox-Zentrums sowie ein Anschluss der Unitectra. Die Übermittlung der Telefon-Verkehrsdaten an die Staatsanwaltschaft erfolgte beide Male unverschlüsselt per E-Mail.
- Am 10. Oktober 2012 ersuchte die Staatsanwaltschaft die Universität per E-Mail um den Abgleich des E-Mail-Verkehrs sämtlicher universitärer E-Mail-Adressen auf Verbindungen mit genau bezeichneten E-Mail-Adressen bzw. E-Mail-Domains.
- Am 15. Oktober 2012 teilte die Universität der Staatsanwaltschaft per E-Mail (verschlüsselt) mit, dass sie betreffend die Anfrage vom 10. Oktober 2012 zur Verfügung stehe.
- Die Universität wertete den E-Mail-Verkehr sämtlicher über das Netzwerk der Universität verkehrenden E-Mails für den Zeitraum 5. August 2012 - 15. Oktober 2012 aus und überbrachte das Resultat der Staatsanwaltschaft am 22. Oktober 2012 auf einem Datenträger. Dessen Datenmenge betrug fünf Megabyte; die Zahl der von der Herausgabe Betroffenen ist nicht näher bestimmt. Von der Herausgabe betroffen waren Angehörige der Universität (Mitarbeitende und Studierende) sowie Dritte, deren E-Mail-Verkehr über das Netzwerk der Universität läuft (z.B. Zentralbibliothek).

- Am 14. November 2012 gewährte die Universität einem von der Staatsanwaltschaft beigezogenen Sachverständigen vor Ort Einblick in drei E-Mail-Boxen. Betroffen waren drei Mitarbeitende des Medizinhistorischen Instituts.
- Am 2. Dezember 2012 lieferte die Universität dem betreffenden Sachverständigen auf mündliche Anweisung des am 14. November 2012 ebenfalls anwesenden Staatsanwalts eine Kopie von zwei der drei E-Mail-Boxen (Momentaufnahme per 14. November 2012). Die Übermittlung erfolgte auf einem Datenträger per Post.
- Am 21. November 2012 übergab die Universität dem von der Staatsanwaltschaft beigezogenen Sachverständigen eine Kopie der Datenbank Akademische Berichte inklusive Zugriffslogs. Die Daten wurden auf einem Memory-Stick persönlich übergeben.
- Am 30. November 2012 ersuchte die Staatsanwaltschaft die Universität per E-Mail um einen erneuten Abgleich sämtlicher Festnetz- und Mobilanschlüsse auf allfällige Kontakte mit einer weiteren Telefonnummer.
- Am 3. Dezember 2012 übermittelte die Universität das Resultat, welches einen Anschluss eines Mitarbeitenden betraf, per E-Mail (unverschlüsselt) an die Staatsanwaltschaft. Die Überprüfung umfasste den Zeitraum 1. Mai 2012 - 3. Dezember 2012 (Festnetzanschlüsse) sowie 1. Mai 2012 - 31. Oktober 2012 (Mobilanschlüsse).
- Am 3. April 2013 gelangte die Staatsanwaltschaft an die Universität, nachdem am 27. März 2013 in der Sendung «Rundschau» auf SRF 1 aus einem Gutachten über eine Dissertation zitiert worden war, welches unter anderem von Prof. Christoph Mörgeli unterzeichnet war. Gemäss Schreiben der Staatsanwaltschaft machte Prof. Christoph Mörgeli im Nachgang zur Sendung gegenüber den Medien geltend, dass solche Gutachten nur universitätsintern verfügbar seien, weshalb das in der Sendung verwendete Gutachten unter Verletzung des Amtsgeheimnisses an das Schweizer Fernsehen gelangt sein müsse. Die Staatsanwaltschaft bat die Universität, sämtliche universitären E-Mail-Adressen bzw. Telefonanschlüsse auf Verbindungen mit einer bestimmten E-Mail-Domain bzw. mit bestimmten Telefonnummern für den Zeitraum 1. September 2012 - 27. März 2013 zu überprüfen und die Resultate der Staatsanwaltschaft zu übermitteln.
- Die Universität nahm wiederum eine Auswertung sämtlicher in das Telefon-Netzwerk integrierten Festnetzanschlüsse, der von der Universität abonnierten Mobilanschlüsse sowie der über das Netzwerk der Universität verkehrenden E-Mails vor und übergab der Staatsanwaltschaft das Resultat am 25. April 2013 auf einem Datenträger. Von der Herausgabe der Telefon-Verkehrsdaten betroffen waren 26 Festnetzanschlüsse, die persönlich genannten Mitarbeitenden zugeordnet werden konnten, zwei Sammelanschlüsse der Universität, welche verschiedenen Personen zugänglich waren, sowie zwei Anschlüsse des Staatsarchivs. Ob auch Telefon-Verkehrsdaten von Mobilanschlüssen herausgegeben wurden, ist unklar. Von der Herausgabe der E-Mail-Verkehrsdaten betroffen waren Angehörige der Universität (Mitarbeitende und Studierende) sowie Dritte, deren E-Mail-Verkehr über das Netzwerk der Universität läuft (z.B. Zentralbiblio-

thek). Deren Zahl ist nicht näher bestimmt; die Datenmenge betrug fünfzehn Megabyte.

- Mit Schreiben vom 30. Mai 2013 ersuchte die Staatsanwaltschaft die Universität um die Herausgabe der Inhalte von zwölf E-Mails.
- Am 10. Juni 2013 übermittelte die Universität der Staatsanwaltschaft sechs E-Mail-Inhalte auf einer CD-ROM per Post. Betroffen waren vier Mitarbeitende der Universität sowie drei weitere Personen, welche in einer der herausgegebenen E-Mails als Absender bzw. Empfänger aufgeführt waren.
- Mit Schreiben vom 24. Juli 2013 ersuchte die Staatsanwaltschaft die Universität um die Herausgabe von 43 E-Mail-Inhalten, unter anderem auch von Mitarbeitenden der Zentralbibliothek. Die Universität teilte der Staatsanwaltschaft gleichentags mit, dass die Zentralbibliothek über eine eigene Rechtspersönlichkeit verfüge, weshalb die entsprechenden E-Mail-Inhalte bei dieser erhältlich zu machen seien.
- Am 7. August 2013 lieferte die Universität der Staatsanwaltschaft fünfzehn E-Mail-Inhalte, welche sieben Mitarbeitende betrafen. Diese wurden auf einem Datenträger verschlüsselt per Post übermittelt.
- Mit Verfügung vom 4. September 2013 beauftragte die Staatsanwaltschaft die Kantonspolizei Zürich mit der Einvernahme genau bezeichneter Personen als Auskunftspersonen. Die Universität erhielt eine Ausfertigung der Verfügung.
- Am 25. September 2013 gab die Universität der Kantonspolizei die Wohnadressen von drei Mitarbeitenden sowie einer Person, welche am Europa Institut Zürich angestellt ist, bekannt.

3.2 Thematisch

- Auswertung von Telefon-Verkehrsdaten: Die Universität nahm mehrmals eine Auswertung sämtlicher in das Telefon-Netzwerk der Universität integrierten Festnetzanschlüsse sowie der von der Universität abonnierten Mobilanschlüsse hinsichtlich Verbindungen mit bestimmten Telefonnummern vor.
- Auswertung von E-Mail-Verkehrsdaten: Die Universität wertete mehrmals den E-Mail-Verkehr sämtlicher über das Netzwerk der Universität verkehrenden E-Mails im Hinblick auf E-Mail-Verkehr mit bestimmten E-Mail-Adressen bzw. mit einer bestimmten Domain aus.
- Weitergabe von Telefon- und E-Mail-Verkehrsdaten: Die Universität gab die Ergebnisse der Auswertungen von Telefon- und E-Mail-Verkehrsdaten an die Staatsanwaltschaft weiter.
- Herausgabe von E-Mail-Inhalten: Die Universität gab Inhalte verschiedener E-Mails von Mitarbeitenden der Universität an die Staatsanwaltschaft heraus.
- Einsicht in bzw. Herausgabe von E-Mail-Boxen: Die Universität gewährte einem von der Staatsanwaltschaft beigezogenen Sachverständigen vor Ort Einblick in drei E-Mail-Boxen und lieferte der Staatsanwaltschaft eine Kopie von zwei der drei E-Mail-Boxen.

- Herausgabe einer Datenbank: Die Universität übergab dem von der Staatsanwaltschaft beigezogenen Sachverständigen eine Kopie der Datenbank Akademische Berichte inklusive Zugriffslogs.
- Bekanntgabe von Wohnadressen: Die Universität gab der Kantonspolizei die Wohnadressen von drei Mitarbeitenden sowie einer Person, welche am Europa Institut Zürich angestellt ist, bekannt.

4 Anwendbarkeit des IDG auf den Sachverhalt

4.1 Geltungsbereich des IDG

Das IDG regelt den Umgang der öffentlichen Organe mit Informationen (§ 1 Abs. 1 IDG). Zu den öffentlichen Organen zählen u.a. Behörden und Verwaltungen des Kantons sowie Organisationen des öffentlichen und privaten Rechts, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind (§ 3 [Abs. 1] IDG).
Die Universität ist eine öffentlich-rechtliche Anstalt des Kantons Zürich mit eigener Rechtspersönlichkeit (§ 1 Abs. 1 Universitätsgesetz, UniG, LS 415.11). Sie ist damit ein öffentliches Organ im Sinne von § 3 [Abs. 1] lit. c IDG.
Die Staatsanwaltschaft ist die Strafverfolgungsbehörde des Kantons Zürich. Sie ist Teil der Direktion der Justiz und des Innern und damit der kantonalen Verwaltung. Auch für sie gilt das IDG.

Vom Geltungsbereich des IDG ausgenommen sind u.a. Gerichte, soweit sie nicht Verwaltungsaufgaben erfüllen (§ 2 IDG). Auf die Rechtsprechungstätigkeit der Gerichte ist das IDG somit nicht anwendbar. Bis zum Zeitpunkt, in welchem ein Verfahren beim Gericht rechtshängig wird, ist das IDG hingegen anwendbar.[3]

Die Universität hat der Staatsanwaltschaft im Rahmen einer Strafuntersuchung Personendaten herausgegeben. Vorliegend erfolgten die Datenbekanntgaben auf Begehren der Staatsanwaltschaft im Rahmen der Strafuntersuchung. Bis zum Zeitpunkt der Anklageerhebung und damit der Rechtshängigkeit des Verfahrens beim Gericht[4] ist das IDG anwendbar (vgl. § 2 Abs. 1 IDG).

[3] Die Ausnahme in § 20 Abs. 3 IDG, wonach sich in nicht rechtskräftig abgeschlossenen Verwaltungs- und Verwaltungsjustizverfahren das Recht auf Zugang zu Informationen nach dem massgeblichen Verfahrensrecht richtet, bezieht sich nicht auf den Geltungsbereich des IDG an sich, sondern lediglich auf das Akteneinsichtsrecht, welches sich - entgegen dem Wortlaut – in sämtlichen hängigen Verfahren nach dem massgeblichen Verfahrensrecht und nicht nach dem IDG richtet.

[4] Gemäss Art. 328 Strafprozessordnung (StPO, SR 312.0) wird das Verfahren mit Eingang der Anklageschrift beim Gericht rechtshängig. Mit der Rechtshängigkeit gehen die Befugnisse im Verfahren auf das Gericht über.

4.2 Personendaten

Personendaten sind Informationen, welche sich auf eine bestimmte oder bestimmbare Person beziehen (§ 3 [Abs. 3] IDG). Informationen sind alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen (§ 3 [Abs. 2] IDG). Die Person muss bestimmt oder bestimmbar sein. Eine Person ist bestimmt, wenn sich ihre Identität unmittelbar aus den Daten ergibt. Sie ist bestimmbar, wenn sich ihre Identität aus dem Kontext der Daten oder durch Kombination mit anderen Daten ergibt.

4.2.1 Telefon- und E-Mail-Verkehrsdaten

Bei der Benutzung von Telefon und E-Mail fallen aus technischen Gründen Verkehrsdaten an. Die Verkehrsdaten geben Auskunft darüber, wann von welchem Anschluss aus eine Person jemanden angerufen und wie lange das Gespräch gedauert hat bzw. wer wann wem eine E-Mail geschickt hat. Können die Telefonanschlüsse bzw. E-Mail-Accounts einer bestimmten oder bestimmbaren Person zugeordnet werden, besteht ein Personenbezug, und es handelt sich bei den Telefon- und E-Mail-Verkehrsdaten um Personendaten.[5] Es ist dabei von der Vermutung auszugehen, dass der jeweilige Inhaber der Anschlüsse einen Anruf getätigt bzw. eine E-Mail versandt bzw. erhalten hat.

Die bei der Universität vorhandenen Telefon-Verkehrsdaten enthalten die Telefonnummer des Anschlusses, von welchem aus angerufen wurde, den Namen des Instituts und der Person(en), auf welche der Anschluss gemeldet ist, die gewählte Zielnummer, das Datum und die Uhrzeit des Telefonats und den Rechnungsbetrag; teilweise ist die Gesprächsdauer enthalten. Die betroffenen Telefonanschlüsse können mehrheitlich einer Person bzw. bei Sammelanschlüssen, welche auf den Namen mehrerer Personen gemeldet sind (z.B. in einem Büro mit mehreren Arbeitsplätzen), einigen wenigen namentlich genannten Personen zugeordnet werden. Die betroffenen Personen sind daher bestimmt bzw. bestimmbar. Die Bestimmbarkeit ist nur bei Anschlüssen zu verneinen, bei welchen eine sehr grosse oder unbestimmte Anzahl von Personen Zugang hat, etwa bei öffentlichen Anschlüssen.

Die bei der Universität vorhandenen E-Mail-Verkehrsdaten enthalten die E-Mail-Adressen des Absenders und der Empfänger, einen Zeitstempel sowie weitere technische Informationen. Der Betreff der E-Mail ist nicht enthalten. Ist die Person des Absenders bzw. Empfängers aus der E-Mail-Adresse ersichtlich, was bei E-Mail-Adressen von Mitarbeitenden der Universität zutrifft (diese enthalten Vor- und Nachname des Inhabers der E-Mail-Adresse, z.B. hans.muster@beispiel.uzh.ch), besteht ein Personenbezug, und die betroffenen Personen sind bestimmt. Bei allgemeinen E-Mail-Adressen (z.B. auskunft@beispiel.uzh.ch) ist die Bestimmbarkeit in den meisten Fällen aufgrund von weiteren Faktoren gegeben. Somit handelt es

[5] Vgl. BGE 136 II 508, E. 3, betreffend Qualifikation von IP-Adressen als Personendaten.

sich beim weitaus grössten Anteil der betroffenen E-Mail-Verkehrsdaten um Personendaten.

4.2.2 E-Mail-Inhalte und E-Mail-Box-Kopie

Der Inhalt einer E-Mail enthält in der Regel eine Aussage über die Person, welche das E-Mail verfasst hat sowie gegebenenfalls auch über deren Adressat und über Dritte. Sind der Verfasser und der Adressat einer E-Mail sowie eine darin erwähnte Drittperson bestimmt oder bestimmbar, liegt ein Personenbezug vor, und es handelt sich um Personendaten.

Die Universität hat der Staatsanwaltschaft 21 E-Mail-Inhalte herausgegeben. Bei sämtlichen E-Mails sind Name und Vorname des betroffenen Mitarbeitenden sowie des Journalisten, welcher in Kontakt mit dem jeweiligen Mitarbeitenden stand, ersichtlich. In einer E-Mail sind drei weitere Personen mit Name und Vorname als Absender bzw. Empfänger ersichtlich. Sämtliche betroffenen Personen sind somit bestimmt oder bestimmbar. Die herausgegebenen E-Mail-Inhalte sind Personendaten.

Eine E-Mail-Box enthält eine Vielzahl von E-Mail-Inhalten. Die Universität hat der Staatsanwaltschaft bzw. dem von ihr beigezogenen Sachverständigen Einblick in drei E-Mail-Boxen von Mitarbeitenden der Universität gewährt und hat zwei der drei E-Mail-Boxen in Kopie herausgegeben. Die drei betroffenen Personen sind bestimmt. Die Inhalte der E-Mail-Boxen, nämlich die eingegangenen und versandten E-Mails, enthalten weitere Personendaten von Dritten.

4.2.3 Datenbank Akademische Berichte inklusive Zugriffslogs

Die Universität hat der Staatsanwaltschaft eine Kopie der Datenbank „Akademische Berichte“ inklusive Zugriffslogs herausgegeben.

Logdaten sind eine Aufzeichnung der Zugriffe auf eine Datenbank. Sie geben Auskunft darüber, welcher Nutzer wann auf welchen Inhalt der Datenbank zugegriffen hat. Der Nutzer ist über den Systemadministrator bestimmbar. Logdaten sind daher Personendaten.

Die Akademischen Berichte sind die Jahresberichte der Fakultäten, Institute, Seminare, Kliniken, assoziierten Institute sowie der Zentren der Universität. Sie dienen als Rechenschaftsbericht und geben Auskunft über die Tätigkeit der entsprechenden Organisationseinheit. Auch die Berichte selbst enthalten Personendaten, insbesondere über Universitätsangehörige, teilweise auch über Dritte. Um diese Daten geht es vorliegend jedoch nicht.

4.2.4 Wohnadressen

Die Universität hat der Staatsanwaltschaft die Wohnadressen von vier Personen herausgegeben. Diese Wohnadressen sind ebenfalls Personendaten.

4.3 Bearbeiten und Bekanntgeben

4.3.1 Bearbeiten

Öffentliche Organe dürfen Personendaten bearbeiten, soweit dies zur Erfüllung ihrer gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist (§ 8 IDG). Die Rechtmässigkeit von Datenbearbeitungen setzt somit eine genügende gesetzliche Grundlage sowie die Einhaltung des Verhältnismässigkeitsprinzips voraus. Das Bearbeiten von Personendaten hat zweckgebunden zu erfolgen, das heisst, dass ein öffentliches Organ Personendaten nur zu dem Zweck bearbeiten darf, zu dem sie erhoben worden sind. Die Bearbeitung von Personendaten zu einem anderen Zweck setzt voraus, dass eine rechtliche Bestimmung eine Weiterverwendung erlaubt oder die betroffene Person ihre Einwilligung erteilt (§ 9 Abs. 1 IDG).

Die Universität bearbeitet Personendaten über Universitätsangehörige. Angehörige der Universität sind einerseits die Mitarbeitenden, bestehend aus dem Lehrkörper, dem Mittelbau sowie dem administrativen und technischen Personal (§§ 8-10 UniG). Anderseits sind die Studierenden Angehörige der Universität (§ 13 UniG).

Die Universität darf Personendaten über Mitarbeitende bearbeiten, sofern dies für das Anstellungsverhältnis geeignet und erforderlich ist (§ 34 Abs. 1 Personalgesetz, LS 177.10, in Verbindung mit § 2 Personalverordnung der Universität Zürich, LS 415.21, und § 24 Universitätsordnung der Universität Zürich, LS 415.111). Soweit die Universitätsordnung und die Personalverordnung der Universität keine abweichenden Regelungen treffen, ist das allgemeine kantonale Personalrecht anwendbar (§ 11 UniG, § 2 Personalverordnung der Universität Zürich).

Studierende der Universität befinden sich nicht in einem (personalrechtlichen) Anstellungsverhältnis mit der Universität, sondern in einem Anstaltsnutzungsverhältnis. Sie haben sich gemäss § 13 UniG zu immatrikulieren. Personendaten von Studierenden darf die Universität bearbeiten, wenn sich dies aus der universitären Gesetzgebung ergibt, insbesondere wenn dies mit dem Studium in einem direkten Zusammenhang steht (§ 12 Verordnung über die Zulassung zum Studium an der Universität Zürich, VZS, LS 415.31).

Die Universität hat mehrmals Auswertungen des Telefon- und E-Mail-Verkehrs vorgenommen. Diese Datenbearbeitungen werden nachfolgend unter Ziffer 5 rechtlich beurteilt.

4.3.2 Bekanntgeben

Ein öffentliches Organ darf Personendaten bekannt geben, wenn eine rechtliche Bestimmung dazu ermächtigt oder die betroffene Person im Einzelfall eingewilligt hat (§§ 16 und 17 jeweils Abs. 1 IDG). Des Weiteren dürfen Personendaten im Einzelfall und auf Gesuch hin einem anderen öffentlichen Organ bekannt gegeben werden, sofern dieses die Daten zur Erfüllung seiner gesetzlichen Aufgaben benötigt und nicht auf anderem Weg, insbesondere bei der betroffenen Person, beschaffen kann (Amtshilfe, §§ 16 und 17 jeweils Abs. 2 IDG). Auch bei der Bekanntgabe sind die Grundsätze der Verhältnismässigkeit und der Zweckbindung zu beachten.

Die Universität und die Staatsanwaltschaft sind verschiedene öffentliche Organe mit unterschiedlichen gesetzlichen Aufgaben. Die Weitergabe von Personendaten durch die Universität an die Staatsanwaltschaft ist eine Datenbekanntgabe im Sinne des IDG.

Die Bekanntgabe ist zu verweigern, zu beschränken oder aufzuschieben, wenn eine rechtliche Bestimmung oder ein überwiegendes öffentliches oder privates Interesse entgegensteht (Interessenabwägung, § 23 IDG). Rechtliche Bestimmungen, welche einer Bekanntgabe von Personendaten entgegenstehen können, sind beispielsweise Vorschriften über Geheimhaltungspflichten. Dazu zählen auch spezialgesetzliche Schweigepflichten oder das Berufsgeheimnis. Mögliche öffentliche Interessen, die einer Bekanntgabe entgegenstehen können, sind in § 23 Abs. 2 IDG aufgezählt, z.B. das Interesse an einem freien Meinungsbildungsprozess. Ein privates Interesse liegt insbesondere vor, wenn durch die Bekanntgabe der Information die Privatsphäre Dritter beeinträchtigt wird (§ 23 Abs. 3 IDG).

Die Universität hat der Staatsanwaltschaft mehrmals verschiedene Kategorien von Daten bekannt gegeben. Diese Datenbekanntgaben werden nachfolgend unter Ziffer 6 rechtlich beurteilt.

5 Beurteilung der Auswertungen der Telefon- und E-Mail-Verkehrsdaten durch die Universität

5.1 Rolle der Universität in der Strafuntersuchung

Parteien in einem Strafverfahren sind die beschuldigte Person, die Privatklägerschaft sowie die Staatsanwaltschaft (Art. 104 Abs. 1 StPO). Als Privatklägerschaft gilt die geschädigte Person, die ausdrücklich erklärt, sich am Strafverfahren als Straf- oder Zivilklägerin oder -kläger zu beteiligen. Der Strafantrag ist dieser Erklärung gleichgestellt (Art. 118 StPO). Geschädigter ist, wer durch die Straftat in seinen Rechten unmittelbar verletzt worden ist. Die zur Stellung eines Strafantrags berechtigte Person gilt in jedem Fall als geschädigte Person (Art. 115 StPO).

Der Straftatbestand der Amtsgeheimnisverletzung ist ein Offizial- und kein Antragsdelikt (Art. 320 Strafgesetzbuch, StGB, SR 311.0). Eine Geschädigtenstellung der Universität aufgrund eines Rechts zur Stellung eines Strafantrags fällt somit ausser Betracht.

Verwaltungsbehörden oder öffentlich-rechtliche Anstalten und Körperschaften sind Geschädigte i.S.v. Art. 115 StPO, soweit sie durch die Straftat in ihren Rechten wie eine Privatperson verletzt worden sind (z.B. Veruntreuung öffentlicher Gelder, Sachbeschädigung an einem Verwaltungsgebäude).[6] Bei Delikten, welche primär allgemeine Interessen schützen, gelten nur diejenigen als Geschädigte, deren private Interessen unmittelbar mitbeeinträchtigt werden, weil diese Beeinträchtigung die unmittelbare Folge der tatbestandsmässigen Handlung ist.[7] Geschädigter einer Amtsgeheimnisverletzung ist demnach die Privatperson, welche durch die Verletzung des Amtsgeheimnisses in ihrer Privatsphäre tangiert wird.[8] Die Universität hat als öffentlich-rechtliche Anstalt gar keine Privatsphäre und kann damit auch nicht Geschädigte einer Amtsgeheimnisverletzung sein. Die an der Wahrung des Amtsgeheimnisses bestehenden öffentlichen Interessen werden von der Staatsanwaltschaft vertreten.[9]

Die Universität ist in den vorliegenden Strafverfahren Anzeigeerstatterin. Auch daraus kann sie keine Parteistellung ableiten. Ein Anzeigeerstatter ist nur insoweit Verfahrensbeteiligter, als er in seinen Rechten unmittelbar betroffen ist, und zwar in dem Umfang, wie es zur Wahrung der Betroffenheit erforderlich ist (Art. 105 Abs. 2 StPO). Die Betroffenheit muss nicht nur faktisch sein, sondern unmittelbar, z.B. durch eine angeordnete Zwangsmassnahme. Zwangsmassnahmen der Staatsanwaltschaft gegen ein öffentliches Organ wie die Universität sind jedoch nicht zulässig (siehe dazu unten, Ziffer 6.1).

Der Universität kommt in den Strafuntersuchungen somit weder eine Parteistellung noch eine andere besondere Rolle zu.

5.2 Bearbeiten von Telefon- und E-Mail-Verkehrsdaten von Mitarbeitenden und Studierenden durch die Universität

Zur Erfüllung ihrer Aufgaben stehen den Mitarbeitenden am Arbeitsplatz die notwendigen Betriebsmittel zur Verfügung. Dazu gehören regelmässig auch Telefon und E-Mail. Die Universität verwaltet als Arbeitgeberin im Rahmen der betriebsinternen Organisation die entsprechenden Geräte und Anschlüsse.

---

6 Basler Kommentar (BSK) StPO-MAZZUCCHELLI/POSTIZZI, Art. 115 Rz 39.
7 BGE 120 Ia 220, E. 3b.
8 Donatsch/Hansjakob/Lieber, Kommentar StPO, Art. 115 Rz 2.
9 BSK StPO-MAZZUCCHELLI/POSTIZZI, Art. 115 Rz 40.

Die Studierenden verfügen nicht über einen zugeteilten Arbeitsplatz; sie können allenfalls – soweit vorhanden – öffentliche Telefonanschlüsse oder Informatikgeräte nutzen. Bei der Nutzung des persönlichen E-Mail-Kontos[10] fallen personenbezogene Daten (E-Mail-Verkehrsdaten, E-Mail-Inhalte) auf den Mail-Servern der Universität an.

Die bei der Nutzung von Informatik- und Kommunikationsmitteln anfallenden Verkehrsdaten dürfen im Rahmen der gesetzlichen Grundlagen aufbewahrt und weiter bearbeitet werden.

- Telefon-Verkehrsdaten

Die Aufzeichnung der Telefon-Verkehrsdaten erfolgt gemäss Angaben der Universität zum Zweck des Nachvollzugs interner Verrechnungen und der Statistik. Die Telefon-Verkehrsdaten werden während mindestens sechs und höchstens zwölf Monaten gespeichert.
In Bezug auf die Nutzung und die Überwachung des Telefon-Verkehrs bestehen – soweit ersichtlich – keine besonderen universitätsinternen Regelungen. Somit gilt § 75 der Vollzugsverordnung zum Personalgesetz (VVO PG, LS 177.111), wonach die private Nutzung von Telekommunikationsmitteln in einem angemessenen Umfang (in zeitlicher Hinsicht als auch bezüglich anfallende Telefongebühren) gestattet bzw. im darüber hinausgehenden Umfang zu vergüten ist.

- E-Mail-Verkehrsdaten

Die Nutzung der Informatikmittel und deren Überwachung werden im Reglement der Universitätsleitung über den Einsatz von Informatikmitteln an der Universität Zürich vom 27. Oktober 2006 (REIM) geregelt. Die Verordnung über die Nutzung von Internet und E-Mail des Kantons (LS 177.115) kommt deshalb nicht direkt zur Anwendung. Gemäss REIM ist die Nutzung von E-Mail zu privaten, nicht-kommerziellen Zwecken grundsätzlich gestattet, soweit diese in geringem Rahmen geschieht (§ 8 Abs. 2 REIM). Es besteht keine Möglichkeit, E-Mail als privat zu bezeichnen (§ 13 Abs. 2 REIM). Zweck der Überwachung ist primär die Erkennung von Missbrauch durch Dritte, das heisst Nicht-Universitätsangehörige (vgl. § 2 Abs. 1 REIM), sowie die Ressourcenplanung (§ 13 Abs. 1 REIM). Die Verfolgung weiterer Zwecke wird aufgrund der Formulierung in § 13 Abs. 1 REIM vorbehalten. Aus § 15 REIM ist ersichtlich, dass auch die Verhinderung von Missbräuchen durch Mitarbeitende erfasst wird. Als Missbrauch gilt die Verletzung von Bestimmungen des REIM oder anderer universitärer Reglemente durch den Einsatz oder die Benutzung von Informatikmitteln (§ 14 Abs. 1 REIM). Eine nicht abschliessende Aufzählung von Missbrauchstatbeständen enthält § 14 Abs. 2 REIM. Der E-Mail-Verkehr und die Internetnutzung

[10] Mit der Immatrikulation wird den Studierenden ein persönliches UniAccess-Konto mit entsprechender E-Mail-Box zugeteilt, welches wöchentlich zu konsultieren ist. Informationen, welche das Studium betreffen, gelten als verbindlich zugestellt, sobald sie von der UniAccess-Mailbox abrufbar sind (§ 14 Verordnung über die Zulassung zum Studium an der Universität Zürich, VZS).

werden protokolliert. Voraussetzung für eine personenbezogene Auswertung von E-Mail-Daten ist ein konkreter Verdacht auf Missbrauch sowie die vorgängige Abmahnung des Betroffenen durch den Vorgesetzten (§ 15 Abs. 1 und 2 REIM). Gemäss Auskunft der Universität Zürich werden E-Mail-Verkehrsdaten sechs Monate plus drei Wochen aufbewahrt.

Zusammenfassend lässt sich festhalten, dass für das Bearbeiten von Telefon- und E-Mail-Verkehrsdaten durch die Universität Rechtsgrundlagen für folgende Bearbeitungszwecke bestehen:

- das technische Herstellen von Verbindungen,
- das interne Verrechnen von Telefongesprächen,
- die (nicht personenbezogene) Statistik,
- die (nicht personenbezogene) Systemüberwachung hinsichtlich Betriebsstabilität, Performance und Sicherheit,
- das Feststellen und Ahnden von Missbräuchen bei konkretem Verdacht nach vorgängiger Abmahnung.[11]

5.3 Auswertung der Telefon-Verkehrsdaten

5.3.1 Massgebliche Ereignisse (Sachverhalt)

Im vorliegenden Fall hatte die Staatsanwaltschaft von der Universität die Herausgabe der Telefon-Verkehrsdaten aller Telefonanschlüsse des Medizinhistorischen Instituts via die Fernmeldedienstanbieterin der Universität für einen konkret bestimmten Zeitraum von 9 Tagen verlangt. Kurz darauf dehnte sie das Begehren auf sämtliche Mobil- und Festnetzanschlüsse der Universität über einen Zeitraum von 9 Monaten aus. Aus den von der Universität im Rahmen der Kontrolle eingereichten Unterlagen ergibt sich, dass in der Zwischenzeit Kontakte zwischen der Universität und der Staatsanwaltschaft stattgefunden hatten, in dessen Rahmen die Universität die Staatsanwaltschaft darüber informierte, dass sie über die Telefon-Verkehrsdaten aller Anschlüsse selber verfüge. Ob die Universität von sich aus der Staatsanwaltschaft dieses Vorgehen vorschlug, lässt sich nicht abschliessend belegen, da dem Datenschutzbeauftragten zu den geführten Gesprächen keine Unterlagen zur Verfügung stehen. Diese Möglichkeit ist aber auch nicht auszuschliessen. Auf jeden Fall kam die Universität der Aufforderung der Staatsanwaltschaft nach, indem sie sämtliche Anschlüsse dahingehend überprüfte, ob im gewünschten Zeitraum von 9 Monaten Verbindungen mit bestimmten Telefonnummern stattgefunden hatten. Zu einem späteren Zeitpunkt nahm die Universität zwei weitere Male vergleichbare

[11] Missbrauch ist auch bei der Telefonie möglich. Insbesondere wenn die Nutzung den angemessenen Umfang übersteigt, stellt dies einen Missbrauch dar. Der Arbeitgeber darf in diesem Fall bei konkretem Verdacht und nach vorgängiger Abmahnung Auswertungen vornehmen.

Auswertungen über andere Zeiträume bzw. andere angerufene Telefonnummern vor.

Die Universität verfügt über rund 9‘300 Festnetzanschlüsse und hat rund 1‘800 Mobilanschlüsse abonniert. Darüber hinaus sind externe Stellen (z.B. Staatsarchiv) und assoziierte Institute (z.B. Europa Institut Zürich) in das Telefon-Netzwerk der Universität integriert. Die Auswertungen, welche die Universität vorgenommen hat, erfolgten über sämtliche Anschlüsse.

Die Universität beschäftigt rund 8‘400 Mitarbeitende.[12] Weiter betroffen ist eine unbestimmte Zahl von Mitarbeitenden von externen Stellen und assoziierten Instituten.

5.3.2 Rechtliche Beurteilung

Ziel der Auswertung war es, diejenigen Anschlüsse zu identifizieren, von denen bestimmte Telefonnummern angerufen worden waren. Diese Auswertung erfolgte im Hinblick darauf, Personen zu finden, die möglicherweise eine Straftat (Amtsgeheimnisverletzung) begangen haben. Dadurch hat die Universität eine Auswertung nach Methoden der Rasterfahndung durchgeführt.

Die Rasterfahndung ist ein polizeiliches bzw. strafprozessuales Instrument, um computergestützt in Datenbeständen nach unbestimmten Personen zu suchen, die bestimmte Kriterien erfüllen. Ziel ist, die Gruppe der zu überprüfenden Personen einzuschränken, da es im Gegensatz zu einer konventionellen Fahndung keine bekannte Zielperson gibt. Rasterfahndungen sind den Strafverfolgungsbehörden vorbehalten und unterliegen den Voraussetzungen des anwendbaren Polizei- und Strafprozessrechts. Für Rasterfahndungen in den Telefon-Verkehrsdaten verfügt die Universität über keine Rechtsgrundlagen.

Selbst wenn Rechtsgrundlagen für ein solches Vorgehen gegeben wären, würde es offensichtlich an der Verhältnismässigkeit fehlen. Dies allein schon aufgrund der Tatsache, dass die Staatsanwaltschaft ursprünglich nur nach den Telefon-Verkehrsdaten des Medizinhistorischen Instituts über einen kurzen Zeitraum fragte. Offensichtlich hätte es genügt, in einem ersten Schritt diese Daten auszuwerten. Es war nicht erforderlich, Daten von rund 11‘000 Telefonanschlüssen von rund 8‘400 Mitarbeitenden der Universität sowie von einer unbestimmten Anzahl von Mitarbeitenden externer Stellen und assoziierter Institute über einen Zeitraum von 9 Monaten auszuwerten. Es wurde nicht die mildeste Massnahme gewählt.

[12] Quelle: Statistische Angaben der Universität für das Jahr 2013 (publiziert www.uzh.ch, eingesehen am 15. Juni 2014).

5.3.3 Exkurs: Rasterfahndung durch die Staatsanwaltschaft

Ob eine Rasterfahndung durch die Staatsanwaltschaft verhältnismässig wäre, muss an dieser Stelle nicht abschliessend beurteilt werden. Immerhin sind diesbezüglich folgende Aspekte zu berücksichtigen:

Gemäss Art. 273 StPO kann die Staatsanwaltschaft Auskunft betreffend Verkehrs- und Rechnungsdaten bzw. Teilnehmeridentifikation verlangen, sofern der dringende Verdacht besteht, ein Verbrechen oder Vergehen oder eine Übertretung nach Art. 179^{septies} StGB sei begangen worden und die Voraussetzungen nach Art. 269 Abs. 1 lit. b und c StPO erfüllt sind. Art. 269 Abs. 1 lit. b und c StPO verlangen, dass die Schwere der Straftat die Überwachung rechtfertigt und die bisherigen Untersuchungshandlungen erfolglos geblieben sind bzw. die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden.

Gemäss bundesgerichtlicher Rechtsprechung regelt Art. 273 StPO die Überwachung des Anschlusses einer bestimmten Person (Tatverdächtiger oder Dritter; vgl. Art. 270 lit. b StPO). Von Art. 273 StPO nicht ausdrücklich erfasst ist dagegen ein Antennensuchlauf im Rahmen einer Rasterfahndung bei unbekannter Täterschaft. Rasterfahndungen sind daher unter strengeren Voraussetzungen zulässig: Der Tatverdacht muss sich auf ein Verbrechen beziehen, die Gesuchten müssen bei noch unbekannter Täterschaft individualisierbar sein, die Subsidiarität der Überwachung muss gewahrt werden (ultima ratio der Untersuchungsanstrengungen) und die verdächtige Schnittmenge der abgeglichenen Verkehrs- und Rechnungsdaten muss voraussichtlich klein sein, das heisst, dass sich das Ergebnis voraussichtlich auf einige wenige Verdächtige bezieht.[13]

Die Auswertung der Telefon-Verkehrsdaten der Universität bzw. eines aufgrund von weiteren Kriterien eingeschränkten Kreises von Mitarbeitenden ist mit der Erhebung von Verkehrsdaten betreffend eine tatverdächtige Person bzw. eine Drittperson, deren Anschluss die tatverdächtige Person benutzt oder die der tatverdächtigen Person Nachrichten übermittelt haben könnte, nicht vergleichbar. Im relevanten Zeitpunkt gab es – soweit ersichtlich – weder eine tatverdächtige Person noch richtete sich die Auswertung der Telefon-Verkehrsdaten gegen eine bestimmte Drittperson. Das Vorgehen entspricht vielmehr einer Rasterfahndung gegen eine unbekannte Täterschaft.

Die durch die bundesgerichtliche Rechtsprechung entwickelten Voraussetzungen einer Rasterfahndung sind vorliegend nicht erfüllt: Die Verletzung des Amtsgeheimnisses ist ein Vergehen und nicht ein Verbrechen (Art. 320 i.V.m. 10 Abs. 3 StGB). Soll entgegen der bundesgerichtlichen Rechtsprechung am Wortlaut von Art. 273 Abs. 1 StPO festgehalten werden, wonach auch der Verdacht eines Vergehens zur Anordnung einer Verkehrsdatenerhebung genügt, muss es sich zumindest um eine

[13] BGE 137 IV 340, Erw. 6.1.

schwere Form der Amtsgeheimnisverletzung handeln (Art. 273 Abs. 1 i.V.m. 269 Abs. 1 lit. b StPO). Ob dies vorliegend erfüllt ist, ist fraglich. Insbesondere betreffend den Akademischen Bericht 2011 des Medizinhistorischen Instituts und Museums ist festzuhalten, dass dieser auf der Datenbank Akademische Berichte ab dem 4. Mai 2012 aufgeschaltet und für rund 1'400 Personen[14], welche ein Log-in besitzen, zugänglich war. Des Weiteren müssen die Gesuchten durch die Rasterfahndung individualisierbar sein, was bei persönlich zuordenbaren Festnetz- und Mobilanschlüssen sowie bei Sammelanschlüssen, deren Nutzer bestimmbar sind, zu bejahen ist. Sodann ist die Subsidiarität der Verkehrsdatenerhebung im Sinne einer ultima ratio vorliegend wohl nicht gegeben. Aus den Unterlagen ist ersichtlich, dass die Staatsanwaltschaft nach der Vornahme erster Abklärungen die Universität um die Herausgabe der Telefon-Verkehrsdaten des Medizinhistorischen Instituts für den Zeitraum 8.-16. September 2012 gebeten hat. Welche anderweitigen Untersuchungshandlungen bereits vorgenommen wurden, ist nicht ersichtlich. Aufgrund der Zeitdauer zwischen der Eingangsbestätigung der Strafanzeige (28. September 2012) und der Aufforderung zur Verkehrsdatenerhebung (4. Oktober 2012) bzw. der Rasterfahndung (9. Oktober 2012) ist jedoch davon auszugehen, dass die Untersuchung noch nicht weit fortgeschritten war. Bei der Rasterfahndung im April 2013 erging die Aufforderung zur Erhebung der Telefon-Verkehrsdaten gar mit dem ersten Schreiben der Staatsanwaltschaft an die Universität in der betreffenden Angelegenheit. Das letzte Erfordernis der voraussichtlich geringen Anzahl Verdächtiger als Resultat der Rasterfahndung wäre vorliegend als erfüllt zu betrachten, sofern sich diese auf einen aufgrund weiterer Kriterien eingeschränkten Kreis von Mitarbeitenden der Universität beschränkt hätte.

Auch für Auswertungen durch die Staatsanwaltschaft, wie sie effektiv die Universität vorgenommen hat, sind die Voraussetzungen einer Rasterfahndung nicht erfüllt.

5.3.4 Auswertung von Telefon-Verkehrsdaten externer Stellen und assoziierter Institute

Die Universität hat auch Auswertungen der Telefon-Verkehrsdaten von externen Stellen (z.B. Staatsarchiv) sowie von assoziierten Instituten[15] (z.B. Europa Institut Zürich) vorgenommen, die in das Telefon-Netzwerk der Universität integriert sind. Betroffen ist eine unbekannte Zahl Mitarbeitende dieser externen Stellen und assoziierten Institute.

---

[14] Diese Angabe entstammt einem Memo, das in der Universität im Rahmen der Strafuntersuchung am 19. Oktober 2012 intern erstellt und dem Datenschutzbeauftragten anlässlich der Sachverhaltsabklärungen eingereicht wurde.

[15] Assoziierte Institute sind wissenschaftlich tätige und rechtlich selbstständige Institutionen, die mit der Universität aufgrund gegenseitiger Interessen durch eine Vereinbarung verbunden sind; § 1 des Reglements für Assoziierte Institute der Universität Zürich vom 19. Dezember 2005.

Das Bearbeiten von Telefon- bzw. E-Mail-Verkehrsdaten durch die Universität erfolgt in diesen Fällen im Auftrag des jeweiligen Dritten. Datenbearbeitungen im Auftrag unterstehen spezifischen Regelungen. Ist der Auftraggeber ein öffentliches Organ des Kantons Zürich, sind §§ 6 IDG in Verbindung mit 25 IDV (Verordnung über die Information und den Datenschutz, LS 170.41) massgebend. Ist der Auftraggeber eine Privatperson, ist Art. 10a des Bundesgesetzes über den Datenschutz (DSG) massgebend.

Die assoziierten Institute der Universität sind rechtlich selbstständige Institutionen. Auf Mitarbeitende von assoziierten Instituten, welche in den von der Universität zur Verfügung gestellten Räumlichkeiten arbeiten, sind die Bestimmungen betreffend Drittmittelanstellungen des Reglements über Drittmittel an der Universität analog anzuwenden. Abweichende Anstellungsbedingungen bedürfen der Genehmigung durch die Universitätsleitung (§§ 1 und 6 des Reglements für Assoziierte Institute der Universität Zürich). Mitarbeitende von assoziierten Instituten sind somit nicht an der Universität angestellt; die Universität verlangt lediglich die Einhaltung bestimmter Anstellungsbedingungen. Die assoziierten Institute sind deshalb – wie andere externe Stellen – als Dritte zu betrachten, in deren Auftrag die Universität gewisse Dienstleistungen erbringt (z.B. Telefonie oder E-Mail-Kommunikation).

Im vorliegenden Fall ist die Universität Auftragnehmerin. Sie erbringt Telefonie- und E-Mail-Dienstleistungen für die genannten Institutionen und handelt in deren Auftrag. Somit darf sie jegliche Auswertungen der Verkehrsdaten auch nur gestützt auf einen entsprechenden Auftrag vornehmen. Dieser kann sich entweder aus der vertraglichen Vereinbarung ergeben oder im Einzelfall erteilt werden. Der Datenschutzbeauftragte geht davon aus, dass für die fraglichen Auswertungen weder vertragliche Bestimmungen bestehen noch der Universität Aufträge erteilt wurden. Jedenfalls hat die Universität diesbezüglich keine Unterlagen vorgelegt. Ob im vorliegenden Sachverhalt eine entsprechende Vereinbarung bzw. ein entsprechender Auftrag für eine Auswertung überhaupt zulässig wäre, kann offen gelassen werden. Soweit die Universität ohne Auftrag der externen Stellen und assoziierten Institute Auswertungen vorgenommen und Daten weitergegeben hat, hat sie sich allenfalls nach § 40 IDG strafbar gemacht.

5.4 Auswertung der E-Mail-Verkehrsdaten

5.4.1 Massgebliche Ereignisse (Sachverhalt)

In ähnlicher Weise wie bei den Telefon-Verkehrsdaten wertete die Universität auch zweimal den E-Mail-Verkehr sämtlicher universitärer E-Mail-Adressen auf Verbindungen mit genau bezeichneten E-Mail-Adressen bzw. E-Mail-Domains über einen Zeitraum von rund zweieinhalb Monaten aus. Von der Auswertung betroffen waren Angehörige der Universität (Mitarbeitende sowie Studierende) sowie Dritte, deren E-Mail-Verkehr über das Netzwerk der Universität läuft (z.B. Zentralbibliothek).

Während bei der Auswertung der Telefon-Verkehrsdaten rund 8‘400 Mitarbeitende der Universität sowie eine unbestimmte Anzahl Personen externer Stellen und assoziierter Institute betroffen waren, kommen in diesem Fall rund 26‘000 Studierende[16] hinzu, deren E-Mail-Verkehr ebenfalls über Domains der Universität läuft.

Die Universität konnte dem Datenschutzbeauftragten keine Angaben betreffend die Zahl der herausgegebenen E-Mail-Verkehrsdaten bzw. die von der Rasterfahndung betroffenen Personen machen. Grund hierfür sei, dass eine E-Mail mindestens zwei Datensätze (je einen für Absender und Empfänger) generiere. Bei E-Mails mit mehreren Empfängern («an», «cc» und «bcc») würden entsprechend mehr Datensätze erzeugt. Des Weiteren führte die Universität aus, dass es technisch nicht möglich sei, zwischen E-Mail-Verkehrsdaten von E-Mails von Angehörigen der Universität und von Nicht-Universitätsangehörigen zu unterscheiden. Dies lässt vermuten, dass es auch nicht möglich ist, zwischen E-Mail-Verkehrsdaten von Mitarbeitenden und von Studierenden zu unterscheiden. Dennoch lässt sich eine ungefähre Grösse der Anzahl von den Auswertungen betroffener Personen ermitteln. Aufgrund von der Universität publizierten Zahlen lässt sich die Anzahl betroffener Angehöriger der Universität ungefähr bei 8‘400 Mitarbeiten und ca. 26‘000 Studierende beziffern. Hinzu kommen Mitarbeitende von externen Stellen und assoziierten Instituten.

5.4.2 Rechtliche Beurteilung

Der Sachverhalt unterscheidet sich von der Auswertung der Telefon-Verkehrsdaten lediglich in quantitativer Hinsicht. Der Zeitraum, für den die Auswertungen erfolgten, war etwas kürzer, dafür war die Anzahl der von den Auswertungen betroffener Personen (erheblich) grösser. Die rechtliche Beurteilung deckt sich deshalb mit derjenigen von Ziffer 5.3.2 betreffend Telefon-Verkehrsdaten. Auch für die vorgenommene Auswertung des E-Mail-Verkehrs bestehen keine rechtlichen Grundlagen. Insbesondere bietet auch das REIM keine Rechtsgrundlage für eine Rasterfahndung oder für eine anlassbezogene Auswertung sämtlicher E-Mail-Verkehrsdaten aller Mitarbeitender und Studierender der Universität sowie externer Dritter.

5.4.3 Auswertung von E-Mail-Verkehrsdaten externer Stellen und assoziierter Institute

In Bezug auf die Auswertung der E-Mail-Verkehrsdaten externer Dritter und assoziierter Institute gilt das in Ziffer 5.3.4 Dargelegte sinngemäss.

[16] Quelle: Statistische Angaben der Universität für das Jahr 2013 (publiziert www.uzh.ch, eingesehen am 15. Juni 2014).

6 Beurteilung der Bekanntgabe von Personendaten durch die Universität an die Staatsanwaltschaft

6.1 Amts- und Rechtshilfe durch ein öffentliches Organ im Rahmen einer Strafuntersuchung

Die Strafprozessordnung (StPO) regelt die Beweismittel und die Zwangsmassnahmen. Die Universität hat – wie oben, Ziffer 5.1, dargelegt – keine besondere Stellung im Verfahren. Sie ist eine öffentlich-rechtliche Anstalt, die eine Strafanzeige erstattet hat. Im Rahmen der Einreichung der Anzeige darf sie gestützt auf § 167 des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess (GOG, LS 211.1) Daten von Tatverdächtigen und allenfalls weiteren Beteiligten (z.B. in Frage kommende Zeugen oder Auskunftspersonen) weitergeben.

Für die Beweismittelbeschaffung bei anderen Behörden sieht die StPO den Rechtshilfeweg vor: Die Behörden des Bundes und der Kantone sind zur Rechtshilfe an die Strafverfolgungsbehörden verpflichtet, wenn Straftaten nach Bundesrecht in Anwendung der StPO verfolgt und beurteilt werden (Art. 44 StPO). Der Behördenbegriff ist weit auszulegen. Davon erfasst werden auch öffentlich-rechtliche Anstalten wie die Universität.[17] Vorliegend erfolgten die Datenherausgaben in Zusammenhang mit einem Verfahren wegen Amtsgeheimnisverletzung, also einer Straftat nach Bundesrecht (Art. 320 StGB). Somit kommen die Rechtshilfebestimmungen zur Anwendung.

Unter den Begriff der Rechtshilfe fällt jede Massnahme, um die eine Behörde im Rahmen ihrer Zuständigkeit in einem Strafverfahren ersucht (Art. 43 Abs. 4 StPO). Rechtshilfemassnahmen stellen beispielsweise Gesuche um Herausgabe von internen Berichten, Protokollen oder Notizen, um Erteilung von Auskünften oder Übermitteln von Akten und Beweismitteln oder um Entbindung vom Amtsgeheimnis zwecks Einvernahme eines Amtsträgers als Zeuge dar.[18]

Die Leistung von Rechtshilfe ist jedoch keine uneingeschränkte Pflicht. Stehen überwiegende öffentliche oder private Interessen oder rechtliche Bestimmungen wie das Berufsgeheimnis entgegen, kann die ersuchte Behörde die Rechtshilfe einschränken oder verweigern.[19] Im Konfliktfall entscheidet – bei Behörden des gleichen Kantons – die Beschwerdeinstanz dieses Kantons endgültig (Art. 48 Abs. 2 StPO), vorliegend das Obergericht des Kantons Zürich (§ 49 GOG). Gegen eine Einschränkung oder Verweigerung der Rechtshilfe können keine prozessualen

[17] BSK StPO-SCHMITT, Art. 44 Rz 3.
[18] BSK StPO-SCHMITT, Art. 43 Rz 15 mit weiteren Nachweisen.
[19] BSK StPO-SCHMITT, Art. 44 Rz 6; vgl. auch Art. 194 Abs. 2 StPO betreffend Beizug von Akten anderer Verfahren.

Zwangsmassnahmen ergriffen werden.[20] Eine Beschlagnahme von Behördenakten ist beispielsweise nicht zulässig.[21]

Für die Datenbekanntgaben der Universität an die Staatsanwaltschaft bestehen demnach gesetzliche Grundlagen; es handelt sich um Rechtsgrundlagen im Sinne von §§ 16 und 17 IDG.

Zu prüfen bleibt, ob die Bekanntgaben der Daten geeignet und erforderlich waren, sich insbesondere auf den notwendigen Umfang beschränkten und keine überwiegenden öffentlichen oder privaten Interessen entgegenstanden.

6.2 Herausgabe der Telefon-Verkehrsdaten

6.2.1 Massgebliche Ereignisse (Sachverhalt)

Die Staatsanwaltschaft verlangte die Verkehrsdaten sämtlicher Telefonanschlüsse des Medizinhistorischen Instituts für einen Zeitraum von 9 Tagen heraus. Die Universität teilte der Staatsanwaltschaft mit, dass sie die Daten sämtlicher universitätsinterner Anschlüsse selber erheben könne. Daraufhin verlangte die Staatsanwaltschaft die Verkehrsdaten sämtlicher Mobil- und Festnetzanschlüsse der Universität, von denen in einem Zeitraum von 9 Monaten Verbindungen mit bestimmten, von ihr vorgegebenen Telefonnummern erfolgten. Die Universität nahm die verlangte Auswertung vor und lieferte der Staatsanwaltschaft die Resultate. Später erfolgten zwei analoge Begehren. Die Universität nahm auch diese Auswertungen vor und gab die Resultate der Staatsanwaltschaft heraus.

6.2.2 Rechtliche Beurteilung

Wie bereits oben, Ziffer 5.3.2, dargelegt, erfolgten die Auswertungen durch die Universität ohne gesetzliche Grundlage.

Für eine Bekanntgabe bestehen hingegen – wie oben, Ziffer 6.1 ausgeführt – Rechtsgrundlagen in Art. 43 f. StPO.

Es lässt sich weiter feststellen, dass nur diejenigen Daten herausgegeben wurden, bei denen effektiv Verbindungen von Anschlüssen der Universität zu den fraglichen Telefonnummern hergestellt worden waren. Damit wurden die Daten umfangmässig auf das Erforderliche begrenzt.

Betreffend jene Telefon-Verkehrsdaten, welche für die Strafuntersuchung als erforderlich zu qualifizieren sind, wäre vor deren Herausgabe an die Staatsanwaltschaft

[20] BSK StPO-SCHMITT, Art. 43 Rz 11.
[21] BSK StPO-BOMMER/GOLDSCHMIED, Vor Art. 263-268 Rz 3.

jedoch eine Interessenabwägung vorzunehmen und zu prüfen gewesen, ob der Herausgabe überwiegende öffentliche oder private Interessen entgegenstanden.

Ein privates Interesse liegt insbesondere im Schutz der Privatsphäre Dritter (§ 23 Abs. 3 IDG), mithin der Angehörigen der Universität. Die Universität hat ihren Mitarbeitenden gegenüber eine Fürsorgepflicht. Sie hat persönlichkeitsverletzende Handlungen zu unterlassen sowie dafür zu sorgen, dass Dritte die Persönlichkeit der Mitarbeitenden nicht verletzen.

Die Auswertung der Telefon-Verkehrsdaten sämtlicher rund 11‘000 Telefonanschlüsse von rund 8‘400 Mitarbeitenden der Universität sowie einer unbestimmten Anzahl von Mitarbeitenden externer Stellen und assoziierter Institute über einen Zeitraum von 9 Monaten greift übermässig in die Persönlichkeit der Betroffenen ein. Wie oben, Ziffer 5.3.2 bzw. 5.3.4 festgehalten, ist sie nicht rechtmässig. Auch wenn die Herausgabe schliesslich „nur“ Daten von einigen Dutzend Personen umfasst, steht aufgrund der widerrechtlichen Datenbeschaffung (Auswertungen) im vorliegenden Fall ein überwiegendes privates Interesse der von der Bekanntgabe betroffenen Personen entgegen.

6.3 Herausgabe der E-Mail-Verkehrsdaten

6.3.1 Massgebliche Ereignisse (Sachverhalt)

Die Staatsanwaltschaft ersuchte die Universität um den Abgleich des E-Mail-Verkehrs sämtlicher universitärer E-Mail-Adressen auf Verbindungen mit genau bezeichneten E-Mail-Adressen bzw. E-Mail-Domains. In der Folge wertete die Universität den E-Mail-Verkehr sämtlicher über das Netzwerk der Universität verkehrenden E-Mails für einen Zeitraum von rund zweieinhalb Monaten aus und gab das Resultat der Staatsanwaltschaft heraus. Später erfolgte ein zur ersten Anfrage analoges Begehren. Die Universität nahm auch diese Auswertung vor und übergab der Staatsanwaltschaft das Resultat.

6.3.2 Rechtliche Beurteilung

Die Universität hat sämtliche bei ihr vorhandenen E-Mail-Verkehrsdaten auf Verbindungen mit bestimmten E-Mail-Adressen bzw. -Domains innerhalb eines von der Staatsanwaltschaft vorgegebenen Zeitraums überprüft. Das Vorgehen ist dasselbe wie bei der Auswertung der Telefon-Verkehrsdaten.

Für die Beurteilung der Frage, ob die Herausgabe dieser Daten an die Staatsanwaltschaft zulässig war, kann daher auf die Ausführungen in Ziffer 6.2.2 verwiesen werden. Die Fragen der Erforderlichkeit und der Abwägung mit entgegenstehenden Interessen sind analog jener betreffend die Herausgabe der Telefon-Verkehrsdaten zu beurteilen.

6.4 Herausgabe von E-Mail-Inhalten

6.4.1 Massgebliche Ereignisse (Sachverhalt)

Die Staatsanwaltschaft ersuchte die Universität um die Herausgabe von zwölf E-Mail-Inhalten. Die Universität übermittelte der Staatsanwaltschaft sechs E-Mail-Inhalte. Später ersuchte die Staatsanwaltschaft die Universität erneut um die Herausgabe von 43 E-Mail-Inhalten, unter anderem auch von Mitarbeitenden der Zentralbibliothek. Die Universität teilte der Staatsanwaltschaft mit, dass die Zentralbibliothek über eine eigene Rechtspersönlichkeit verfüge, weshalb die entsprechenden E-Mail-Inhalte bei dieser erhältlich zu machen seien. Sie lieferte der Staatsanwaltschaft fünfzehn E-Mail-Inhalte, welche sieben Mitarbeitende der Universität betrafen.

6.4.2 Rechtliche Beurteilung

Die von der Staatsanwaltschaft angeforderten E-Mail-Inhalte stützen sich auf die von der Universität durchgeführten Auswertungen der E-Mail-Verkehrsdaten. Diese erfolgten ohne Rechtsgrundlage.

Für die Beurteilung der Frage, ob die Herausgabe dieser Daten an die Staatsanwaltschaft zulässig war, kann daher auf die Ausführungen in Ziffer 6.2.2 verwiesen werden. Die Fragen der Erforderlichkeit und der Abwägung mit entgegenstehenden Interessen sind analog jener betreffend die Herausgabe der Telefon-Verkehrsdaten zu beurteilen.

6.5 Einsicht in drei E-Mail-Boxen und Herausgabe von zwei E-Mail-Box-Kopien

6.5.1 Massgebliche Ereignisse (Sachverhalt)

Die Universität gewährte einem von der Staatsanwaltschaft beigezogenen Sachverständigen vor Ort Einblick in drei E-Mail-Boxen. Betroffen waren drei Mitarbeitende des Medizinhistorischen Instituts. Die Universität lieferte dem betreffenden Sachverständigen auf Anweisung des Staatsanwalts eine Kopie von zwei der drei E-Mail-Boxen (Momentaufnahme per Stichtag).

6.5.2 Rechtliche Beurteilung

Gemäss Auskunft der Universität erfolgte die Einsichtnahme in drei E-Mail-Boxen und anschliessende Herausgabe von zwei E-Mail-Box-Kopien im Hinblick auf die Aufhebung einer Zwangsmassnahme. Betroffen sind drei Mitarbeitende des Medizinhistorischen Instituts. Dem Datenschutzbeauftragten liegen keine weiteren Informationen über die Umstände der Bekanntgabe der Inhalte der betroffenen E-Mail-

Boxen vor. Immerhin lässt sich sagen, dass die Einsichtnahme in bzw. die Herausgabe von E-Mail-Boxen drei bestimmte Personen aus dem Medizinhistorischen Institut und damit das spezifische Umfeld der Straftat betrafen. Somit ist von einer konkreten Verdachtslage auszugehen. Ob für die weiteren Untersuchungen die Herausgabe der gesamten E-Mailboxen erforderlich war, kann jedoch nicht abschliessend beurteilt werden. Die Umstände sprechen dafür, dass die Bekanntgabe rechtmässig war.

6.5.3 Exkurs: Beizug eines Sachverständigen

Die Staatsanwaltschaft hat für die Einsichtnahme in die E-Mail-Boxen bzw. die darauf folgende Herausgabe einen Sachverständigen beigezogen. Ein solcher Beizug ist im Rahmen von Art. 182 ff. StPO zulässig. Der beigezogene Sachverständige darf Personendaten im Rahmen des Sachverständigenauftrags bearbeiten (Art. 184 StPO und § 6 IDG). Vorliegend gibt es keine Anhaltspunkte, dass die Datenbearbeitungen des Sachverständigen nicht korrekt erfolgten.

6.6 Herausgabe der Datenbank Akademische Berichte inklusive Zugriffslogs

6.6.1 Massgebliche Ereignisse (Sachverhalt)

Die Universität übergab dem von der Staatsanwaltschaft beigezogenen Sachverständigen eine Kopie der Datenbank Akademische Berichte inklusive Zugriffslogs.

6.6.2 Rechtliche Beurteilung

Der Akademische Bericht 2011 des Medizinhistorischen Instituts und Museums war ab dem 4. Mai 2012 auf der Datenbank Akademische Berichte für die rund 1‘400 Personen, welche über ein Log-in verfügen, abrufbar. Die Datenbekanntgabe betrifft somit einen der Berichte, welche Objekt der möglichen Amtsgeheimnisverletzung bilden.

Dem Datenschutzbeauftragten ist nicht bekannt, welche Personen von der Herausgabe der Zugriffslogs betroffen sind. Insbesondere ist unklar, ob lediglich die Logprotokolle betreffend die erfolgten Zugriffe auf den Akademischen Bericht 2011 des Medizinhistorischen Instituts und Museums oder betreffend sämtliche in der Datenbank abrufbaren Akademischen Berichte herausgegeben wurden. Die dem Datenschutzbeauftragten zur Verfügung stehenden Unterlagen enthalten keine Anhaltspunkte, dass nur die Logprotokolle der Zugriffe auf die Datenbank Akademische Berichte herausgegeben wurden. Vielmehr ist anzunehmen, dass die Logprotokolle sämtlicher Zugriffe auf alle in der Datenbank vorhandenen Dokumente herausgegeben wurden.

Darüber hinaus lässt sich die Frage stellen, ob ein Bericht, der ab 4. Mai 2012 für rund 1‘400 Personen abrufbar war, als geheim im Sinne von Art. 320 StGB gelten kann. Dies ist jedoch eine materiell-strafrechtliche Frage, die vom zuständigen Strafgericht zu beantworten ist.

Sofern von der Datenbekanntgabe lediglich Personen betroffen wären, welche Zugriff auf den Akademischen Bericht 2011 des Medizinhistorischen Instituts und Museums genommen haben und der fragliche Zeitraum begrenzt ist, könnte die Datenbekanntgabe als verhältnismässig erachtet werden. Es ist jedoch nirgends ersichtlich, dass die Herausgabe der Logprotokolle begrenzt wurde; vielmehr wurde wohl die gesamte Datenbank Akademische Berichte mit allen Zugriffslogs herausgegeben. Diese Herausgabe erscheint unverhältnismässig.

6.7 Herausgabe von vier Wohnadressen

6.7.1 Massgebliche Ereignisse (Sachverhalt)

Die Staatsanwaltschaft beauftragte die Kantonspolizei mit der Einvernahme genau bezeichneter Personen als Auskunftspersonen. Die Universität erhielt eine Ausfertigung der Verfügung. Sie gab der Kantonspolizei die Wohnadressen von drei Mitarbeitenden der Universität sowie einer Person, welche am Europa Institut Zürich angestellt ist, bekannt.

6.7.2 Rechtliche Beurteilung

Die Herausgabe der Wohnadressen von namentlich bezeichneten Mitarbeitenden der Universität anlässlich eines Strafverfahrens an die Strafverfolgungsorgane ist verhältnismässig. Rechtsgrundlagen sind die oben, Ziffer 6.1 erwähnten Bestimmungen über die Rechtshilfe von Behörden.
Betreffend die Herausgabe der Wohnadresse des Mitarbeitenden des Europa Instituts Zürich hätte dieses über die Herausgabe entscheiden müssen.

6.8 Sicherheit der Übermittlung bei einer Datenbekanntgabe

Die Datenbekanntgaben erfolgten durch verschiedene Übermittlungsmethoden: per Post, durch persönliche Übergabe und per E-Mail.

Öffentliche Organe sind verpflichtet, Informationen durch angemessene technische und organisatorische Massnahmen zu schützen. Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik (§ 7 IDG).
Massnahmen der Informationssicherheit sind in sämtlichen Phasen des Bearbeitens von Personendaten zu treffen, mithin auch bei deren Bekanntgabe.

- Bei der persönlichen Übergabe an eine zum Empfang der Daten berechtigte Person sind keine besonderen Massnahmen zu treffen. Es ist sicherzustellen, dass der richtige Datenträger an einen berechtigten Empfänger übergeben wird und dass die übermittelnde und die empfangende Personen jeweils auf ihrem Transportweg geeignete Massnahmen zum Schutz vor Verlust treffen.
- Bei der Übermittlung per Post sind – je nach Inhalt – unter Umständen zusätzliche Massnahmen wie Zustellung gegen Rückschein, Einschreiben usw. zu treffen. Allenfalls ist anstelle der Post der Weg der persönlichen Übergabe zu wählen.
- Bei der Übermittlung per E-Mail sind sensible Daten immer zu verschlüsseln. Personendaten, welche der Staatsanwaltschaft im Rahmen eines Strafverfahrens herausgegeben werden, sind besondere, d.h. sensible Personendaten (§ 3 [Abs. 4] lit. a Ziff. 4 IDG). Teilweise erfolgte die Übermittlung sensibler Daten per E-Mail unverschlüsselt; dies verstösst gegen § 7 IDG.

7 Ergebnisse

Der beschriebene Sachverhalt und dessen rechtliche Beurteilung führen zu folgenden Ergebnissen:

- Die Auswertungen der Telefon-Verkehrsdaten durch die Universität waren rechtswidrig.
- Die Auswertungen der E-Mail-Verkehrsdaten durch die Universität waren rechtswidrig.
- Den Herausgaben der ausgewerteten Telefon- und E-Mail-Verkehrsdaten durch die Universität an die Staatsanwaltschaft standen überwiegende private Interessen der Betroffenen entgegen; sie waren rechtswidrig.
- Die Herausgaben von Daten betreffend externer Stellen und assoziierter Institute durch die Universität waren rechtswidrig.
- Den Herausgaben von Inhalten von E-Mails durch die Universität standen überwiegende private Interessen der Betroffenen entgegen; sie waren rechtswidrig.
- Die Rechtmässigkeit des Gewährens von Einsicht in und der Herausgabe von E-Mail-Boxen durch die Universität kann nicht abschliessend beurteilt werden.
- Die Herausgabe der Datenbank Akademische Berichte samt deren Zugriffslogs durch die Universität kann nicht abschliessend beurteilt werden. Es bestehen Anhaltspunkte, dass die Herausgabe nicht verhältnismässig und somit rechtswidrig war.
- Die Herausgabe von Wohnadressen durch die Universität war rechtmässig. Über die Herausgabe der Wohnadresse eines Mitarbeitenden des Europa-Instituts hätte allerdings dieses entscheiden müssen.
- Für die Übermittlung von Daten per E-Mail durch die Universität wurden, soweit sie unverschlüsselt erfolgte, keine angemessenen Sicherheitsmassnahmen getroffen.

Über diese Ergebnisse hinaus macht der Datenschutzbeauftragte folgende Feststellungen:

- Universitätsinterne Organisation

Die Herausgaben von Daten erfolgten durch unterschiedliche Dienste bzw. Abteilungen der Universität, wobei teilweise in Absprache bzw. auf Instruktion, teilweise autonom gehandelt wurde. Es ist offen, ob organisatorische Regelungen, Freigabeverfahren, Informations- und Eskalationswege u.dgl. für den Fall bestehen, dass im Rahmen eines Strafverfahrens Anfragen der Strafverfolgungsbehörden an die Universität gelangen. Diese Aspekte wurden im Rahmen der Kontrolle nicht näher überprüft.
Es stellt sich grundsätzlich die Frage, welche Stellen in solche Vorgänge wie einzubeziehen sind und wen universitätsintern die Verantwortung für die Datenbearbeitungen und Datenbekanntgaben trifft. Soweit dies nicht geregelt ist, empfiehlt es sich, diesbezügliche organisatorische Regelungen zu treffen. Dabei ist auch festzulegen, wie die Rechtmässigkeit von Datenbekanntgaben geprüft und die Interessenabwägung vorgenommen wird.

- Transparenz der Vorgänge für die Betroffenen

Die von der Universität vorgenommenen Auswertungen und Datenbekanntgaben betreffen Tausende von Universitätsangehörigen (Mitarbeitende und Studierende) sowie Dritte, die bezüglich Telefon- und E-Mail-Dienstleistungen vertraglich der Universität angeschlossen sind. Aufgrund der gesetzlichen und vertraglichen Treue- und Fürsorgepflichten der Universität im Verhältnis zu ihren Angehörigen als auch zu den externen Stellen ist es angezeigt, dass die Universität die Betroffenen von sich aus auf geeignete Weise über die Datenbearbeitungen und Datenbekanntgaben informiert.

8 Schlussbesprechung und weiteres Vorgehen

Der vorliegende Bericht wurde mit der Universität Zürich am 27. Juni 2014 besprochen. An der Besprechung nahmen teil:

- Universität: Prof. Dr. Michael Hengartner, Rektor, Prof. Dr. Andrea Schenker-Wicki, Prorektorin Rechts- und Wirtschaftswissenschaften, Dr. Rita Stöckli, Stellvertretende Generalsekretärin, Beat Müller, Stellvertretender Leiter Kommunikation, Sven Akeret, Leiter Rechtsdienst, und Nadia Steiner, Mitarbeiterin Rechtsdienst.
- Datenschutzbeauftragter: Dr. Bruno Baeriswyl, Datenschutzbeauftragter, und Marco Fey, Abteilungsleiter.

Die Universität erstattet dem Datenschutzbeauftragten **bis 30. November 2014** Bericht über Massnahmen, die sie getroffen hat, um inskünftig bei vergleichbaren Situationen die gesetzeskonforme Datenbearbeitung und Datenbekanntgabe sicherzustellen.

Der vorliegende Bericht wird durch den Datenschutzbeauftragten veröffentlicht.

Zürich, 3. Juli 2014

Datenschutzbeauftragter des Kantons Zürich

Der Beauftragte

Dr. Bruno Baeriswyl

Verteiler:
- Universität Zürich, Rektor (2 Exemplare)
- Universitätsrat, Präsidentin (1 Exemplar)

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
Fax 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch