

Cybercrime und Recht

Rechtliche Aspekte der Kriminalität im Cyberspace und Ermittlungsmethoden waren Schwerpunkte beim Symposium der wissenschaftlichen Interessengemeinschaft IT-LAW.AT.

Phishing, unberechtigte Behebungen von Bargeld an Bankomaten und Bestellbetrug im Internet waren Schwerpunkte des Referats von DI MMMag. Michael Tolstiuik, Richter am Landesgericht für Strafsachen Wien.

Beim Phishing, dem Passwort-Fischen, kundenschaftet der Täter einen Zugangscodes aus. Auch wenn es nicht zu einem betrügerischen Datenverarbeitungsmissbrauch (§ 148a StGB) kommt, hat der Täter durch ein Abfangen, entsprechende Absicht vorausgesetzt, in vielen Fällen den Tatbestand des § 119a StGB (Missbräuchliches Abfangen von Daten) erfüllt. Hat der Täter den Zugangscodes (etwa die TAN) dadurch erlangt, dass das Opfer auf eine gefälschte Website umgeleitet wurde, dann hat er durch diese Tat handlung ein Computerprogramm hergestellt oder besitzen, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung der Delikte nach den §§ 119a und 148a StGB geschaffen oder adaptiert worden ist, und damit von der objektiven Tatseite her den Tatbestand des § 126c StGB (Missbrauch von Computerprogrammen oder Zugangsdaten) verwirklicht. Ist in weiterer Folge die vom Vorsatz umfasste Vermögensschädigung tatsächlich eingetreten, ist der Tatbestand des § 148a StGB erfüllt. Die dazu führenden Vorbereitungshandlungen gehen dann in diesem Delikt auf.

Wenn Kredit- oder Bankomat-Karten ge- oder verfälscht oder gestohlene Karten verwendet werden, kommen die Strafbestimmungen



Waltraud Kotschy: Datenschutzrechtliche Grenzen bei der Ermittlung und Auswertung von Verdachtsdaten.

über unbare Zahlungsmittel (§§ 241a bis 241f StGB) zum Tragen.

Der Tatbestand der Geldwäscherei (§ 165 StGB) sowie die diesbezüglichen strafprozessualen Verfolgungsmöglichkeiten (§ 116 StPO; Auskunft über Bankkonten und Bankgeschäfte) wurden mit 1. Juli 2010 (BGBl I 2010/38) wesentlich geändert. Neben einer Erweiterung des Vortatenkataloges umfasst die Geldwäscherei nunmehr auch die Eigengeldwäsche, die bisher als straflose Nachtat angesehen wurde. Begründet wurde diese Verschärfung mit der

Aufwendung zusätzlicher krimineller Energie – aus dem Blickwinkel, dass der Zweck der Geldwäschereibestimmung die Unverwertbarkeit kriminell kontaminierten Vermögens ist (RV 673 BlgNR 24. GP).

Die Novellierung des § 116 StPO geht ebenfalls auf eine Kritik bei der Länderüberprüfung Österreichs durch die *Financial Action Task Force (FATF)* zurück, bei der Österreich Mitglied ist. Im Bericht vom 26. Juni 2009 wurden die österreichischen Regelungen für eine Auskunft über Bankkonten und Bankgeschäfte als zu

restriktiv bezeichnet, was die Möglichkeit der Strafverfolgungsbehörden zur Ausforschung von Vermögen krimineller Herkunft erschwere. Der eingeschränkte Zugang zu Bankinformationen verzögere die internationale Zusammenarbeit. Dies war laut Tolstiuik insofern der Fall, als nach § 116 StPO aF. die Auskunft über Bankkonten und Bankgeschäfte nur zulässig war, wenn sie zur Aufklärung eines Verbrechens oder Vergehens, das in die Zuständigkeit des Landesgerichtes gefallen ist. Die Masse der „Ebay-Betrugsfälle“ mit einer Schadenssumme von unter 3.000 Euro konnte daher nicht auf dem Weg einer Kontenöffnung verfolgt werden. In Rechts-hilfverfahren hat sich die Praxis mit einem Rückgriff auf Art. 51 SDÜ beholfen und dadurch eine Kontenöffnung ermöglicht (OLG Wien vom 19.5.2008, 23 Bs 140/08v).

Nach der nunmehrigen Rechtslage ist die Auskunft über Bankkonten und Bankgeschäfte auch bei vorsätzlich begangenen Straftaten zulässig, die in die Zuständigkeit der Bezirksgerichte fallen. Die Auskunft ist durch die Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen. Eine Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen (§ 110 Abs. 2 StPO). Über eine Beschlagnahme hat das Gericht auf Antrag der Staatsanwaltschaft oder einer von der Sicherstellung betroffenen Person unverzüglich zu entscheiden (§ 115 Abs. 2 StPO). Eine Durchbrechung des Bankge-

IT-LAW.AT

Informationsrecht

Der Verein *IT-LAW.AT* wurde 2001 von Absolventen des postgradualen Universitätslehrgangs für Informationsrecht und Rechtsinformation gegründet. Ziel des Vereins ist die Bereitstellung einer Plattform für Interessierte im Bereich Informationsrecht und

Rechtsinformation zum Zweck der Kooperation und des Wissens- und Informationsaustausches auf hohem fachlichem Niveau.

Beim *IT-LAW.AT*-Symposium am 18. Oktober 2010 im Festsaal der Diplomatischen Akademie in Wien nahmen 50 Interessierte teil.

<http://www.it-law.at>



Nothmüller Michael
HAUSTECHNIK

Planung - Verkauf - Vermietung - Wartung
Klima-, Entfeuchtungs-, Kältegeräte, Wärmepumpen

2521 Trumau Fax & Tel.: 02253/9158
Am Pflanzsteig 10 Mobiltel.: 0664/3812515
E-Mail: nothmichael@aon.at



Binder

St. Andrä-Wördern

office@adeg-binder.at - www.adeg-binder.at

Hauptgeschäft: Hauptstraße 23 3423 Wördern 02242 / 32287, Fax -21
Filiale: Tullner Straße 30a 3423 St. Andrä 02242 / 33820-20, Fax -21

Wo Sie auch wohnen, der Weg wird sich lohnen!



Baumpflege Kreitl

Gutachten - Baumpflege - Baumrodung
Konzepte und Problemlösungen für Baumbestände
Wurzelstockentfernung - Windbruchbeseitigung
Gefahr in Verzug-Bäume - Ersatzpflanzungen

2281 Raasdorf, Die Marchfelderstraße 12
Tel.: 0664 / 886 20 930
Internet: www.kreitl.at

MALEN
BESCHICHTEN
KORROSIONSSCHUTZ



ASPETTENSTR. 48
2380 PERCHTOLDSDORF
TEL: 01/890 38 31 • FAX: 01/890 38 30
E-MAIL: INFO@MABEKO.AT

**MABEKO, MALEN – BESCHICHTEN –
KORROSIONSSCHUTZ GMBH**

Malermeister
Ernst Klingelbrunner jun.

3441 Baumgarten/Tullnerfeld
Hauptstraße 92
Tel. + Fax: 02274 / 7085



Prof. Wolfgang Brandstetter: Tendenz zu einem „Fishing for Evidence“.

heimnisses könnte die Beschlagnahme von Überwachungsfotos von Videokameras im Bereich von Geldausgabeautomaten darstellen. Hiezu hat der OGH mit Urteil vom 13.12.2007, 12 Os 100/07h, auf Grund einer Nichtigkeitsbeschwerde der Generalprokuratur ausgeführt, dass derartige Fotos schon deshalb nicht unter das Bankgeheimnis fallen, weil § 38 Abs. 1 BWG nur solche Informationen erfasst, die den zur Geheimhaltung Verpflichteten ausschließlich aufgrund der Geschäftsverbindung mit Kunden oder aufgrund einer Großkreditmeldung (§ 75 Abs. 3 BWG) anvertraut oder zugänglich gemacht worden sind. Jedenfalls nicht dazu zählen unabhängig von der tatsächlichen Durchführung einer Transaktion angefertigte Bilder von Personen, die sich im Bereich eines Bankomaten aufhalten.

Kommunikationsgeheimnis. Rechtsproblemen, die sich bei der Ausforschung der Nutzer von IP-Adressen ergeben, ist Mag. Peter Gildemeister der Oberstaatsanwaltschaft Wien nachgegangen. An grundrechtlichen Schranken sind das Fernmeldegeheimnis (Art. 10a StGG) sowie § 1 des Datenschutzgesetzes zu beachten. Bereits aus § 7 Abs. 2 DSGVO



Karin Mair: Gerichtsfeste Datenermittlung und Auswertung durch Private.

ergebe sich die Zulässigkeit der Übermittlung personenbezogener Daten an eine gesetzlich und damit unter Einhaltung des Verhältnismäßigkeitsgebots vorgehende Strafverfolgungsbehörde.

Nach Art. 10a StGG darf das Fernmeldegeheimnis nicht verletzt werden. Ausnahmen von dieser Bestimmung sind nur auf Grund eines richterlichen Befehles zulässig.

Diese durch BGBl 1974/8 in das Staatsgrundgesetz aus 1867 eingefügte und am 1. Jänner 1975 in Kraft getretene Verfassungsbestimmung konnte Entwicklungen wie Internet und Mobilkommunikation noch nicht erfassen. Nach heutigen Begriffen waren damals Inhaltsdaten einer Kommunikation gemeint.

Auf einfachgesetzlicher Ebene legt § 93 Abs. 1 TKG 2003 fest, dass dem in den Absätzen 3 und 4 inhaltlich näher beschriebenen Kommunikationsgeheimnis die Inhalts-, Verkehrs- und Standortdaten unterliegen. Inhaltsdaten betreffen die Inhalte übertragener Nachrichten (§ 92 Abs. 3 Z 5 TKG); Verkehrsdaten sind Daten, die zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden (§ 92 Abs. 3

Z 4 TKG). Standortdaten sind Daten, die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben (§ 92 Abs. 3 Z 6 TKG).

Gildemeister verglich das Verhältnis zwischen Fernmelde- und Kommunikationsgeheimnis mit zwei konzentrischen Kreisen, von denen das Fernmeldegeheimnis der engere ist. Das Kommunikationsgeheimnis als solches ist vom Richtervorbehalt nicht umfasst.

In einem nach der StPO geführten Strafverfahren wird in das Kommunikationsgeheimnis eingegriffen. Unter „Auskunft über Daten einer Nachrichtenübermittlung“ versteht § 134 Z 2 StPO die Erteilung einer Auskunft über Verkehrsdaten, Zugangsdaten und Standortdaten. „Überwachung von Nachrichten“ ist, nach der Definition des § 134 Z 3 StPO, das Ermitteln des Inhalts von Nachrichten, die ausgetauscht oder weitergeleitet werden – also während des Kommunikationsvorgangs. Nach dessen Abschluss kommt nur mehr Sicherstellung in Betracht.

Beide Maßnahmen sind nur zur Aufklärung einer vorsätzlich begangenen Straftat zulässig, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, und stehen unter Richtervorbehalt. Wird der Antrag des Staatsanwalts vom Gericht bewilligt, wendet sich die Polizei an den Provider.

IP-Adressen. Die in § 93 Abs. 1 nicht angeführten Stammdaten (§ 92 Abs. 3 Z 3 TKG) unterliegen nicht dem Kommunikationsgeheimnis. Als Daten über Familien- und Vorname, Wohnadresse und Teilnehmernummer sind sie mit einem öffentlichen Telefonverzeichnis vergleichbar.



Prof. Hannes Tretter: Spannungsfeld zwischen Ermittlungsmethoden und Grundrechten.

Nicht anzuwenden sind gemäß § 103 Abs. 4 TKG Beschränkungen über die zulässige Verwendung, Auswertung und Übermittlung gegenüber Ersuchen der Gerichte, die sich auf die Aufklärung und Verfolgung einer bestimmten Straftat beziehen. Unter „Gericht“ sind auch die Staatsanwaltschaften zu verstehen, das wurde mittlerweile durch die Rechtsprechung der Oberlandesgerichte klargestellt. Es genügt ein formloses Ersuchen der Staatsanwaltschaft an den Betreiber, die hinter einer Teilnehmernummer stehenden Daten einer physischen Person bekannt zu geben. Wird die Auskunft verweigert, kommen Sicherstellung, Zeugeneinvernahme oder Beugestrafen in Betracht.

Wenn die IP-Adresse eines Teilnehmers an einer Kommunikation bereits bekannt ist, handelt es sich nach dem Urteil des OGH vom 26.7.2005, 11 Os 57/05z, um eine Stammdatenabfrage – gleichgültig, ob eine statische oder dynamische IP-Adresse vorliegt. Eine „Auskunft über Daten einer Nachrichtenübermittlung“, die der Bewilligung durch den Richter bedürfen würde, würde nur dann vorliegen, wenn eine noch nicht bekannte IP-Adresse ermit-

telt werden sollte. Bei Kommunikationsvorgängen im Internet, beispielsweise bei Betrügereien, werden aber regelmäßig die IP-Adressen freiwillig übermittelt.

Das Urteil des OGH vom 14.7.2009, 4 Ob 41/09x, stehe laut Gildemeister der Auffassung nicht entgegen, dass auch bei dynamischen IP-Adressen die Anfrage nach der dahinter stehenden Person eine Stammdatenabfrage ist. Das Urteil sagt lediglich aus, dass dem Privatankläger nach dem Urheberrechtsgesetz ein privatrechtlicher Anspruch an den Provider auf Herausgabe dieser Daten nicht zusteht. Unberührt bleiben die Bestimmungen der Strafprozessordnung durch die Bestimmungen des TKG über Kommunikationsgeheimnis und Datenschutz (§ 92 Abs. 2 TKG).

Dass Internet-Provider bei Anfragen von Staatsanwaltschaften, wer der Inhaber einer bestimmten IP-Adresse ist, die Herausgabe der Stammdaten verweigern, beruhe laut Gildemeister auf einem Missverständnis. Als „Zeugen“ für seine Rechtsmeinung, dass bei diesen Anfragen kein Richtervorbehalt besteht, führte er die – verfassungsgerichtlich bereits mehrfach (VfGH Zlen G 29/08, 30/08, 147/08,

31/08, 35/08) überprüfte – Bestimmung des § 53 Abs. 3a des Sicherheitspolizeigesetzes an, wonach die Sicherheitsbehörden berechtigt sind, von Betreibern öffentlicher Telekommunikationsdienste unter anderem (Z 3) Auskunft über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, zu verlangen, wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen.

Eine andere Rechtsauffassung zu vertreten, würde bedeuten, dass die Masse der Betrugsfälle im Internet (Ware wird bezahlt, aber nicht geliefert), nicht mit Hilfe der bekannten IP-Adressen verfolgt werden könnte, weil die Schadenssummen in der Regel unter 3.000 Euro liegen und die Tat (lediglich) mit Freiheitsstrafe bis zu sechs Monaten bedroht ist (§ 146 StGB), somit die Voraussetzungen des § 135 Abs 2 StPO nicht vorliegen.

Grundrechtsschutz. Auf strafrechtliche und sicherheitspolizeiliche Ermittlungsmethoden im Spannungsfeld zu den Grundrechten ging a. o. Univ.-Prof. Dr. Hannes Tretter, Leiter des Ludwig Boltzmann Institutes für Menschenrechte, ein. Straftaten unter Einsatz elektronischer Datenverarbeitung sind etwa der widerrechtliche Zugriff auf Computersysteme, Computerbetrügereien und -sabotage, Urheberrechtsverletzungen und Software-Piraterie oder der Missbrauch elektronischer Plattformen wie etwa des Online-Bankings oder von Versteigerungsplattformen. Das Netz wird als Medium



IT-Law-Tagung: Richter Michael Tolstiu, Rechtsanwältin Isabell Lichtenstrasser, Staatsanwalt Peter Gildemeister.

zur Verabredung, Vorbereitung und zum Aufruf von Straftaten eingesetzt, von der organisierten Kriminalität zum Menschen-, Organ-, Waffen- und Suchtgifthandel sowie zur Geldwäsche verwendet, und bildet die logistische Struktur für politisch und religiös motivierten Terrorismus, zu Gewaltaufrufen, Verhetzung, Rassismus und Fremdenfeindlichkeit. Über das Netz erfolgen Verabredungen zu Kannibalismus und Satanismus, zu verpönten Sexualpraktiken wie Pädophilie und Sodomie; Kinderpornografie wird verbreitet. Im Internet denunziert und „an den Pranger gestellt“ zu werden, kann zu einer Art „bürgerlichem Tod“ führen.

Dennoch müssten sich Ermittlungsmethoden an den Grundrechten orientieren. Selbst bei geforderter Geheimhaltung effektiver präventiver Maßnahmen müsse nach der Rechtsprechung des EGMR die nachträgliche Informationspflicht wegen des Rechts auf eine wirksame Beschwerde gemäß Art. 13 EMRK gewährleistet sein, ebenso bei Ermittlung des Täters und des Tatorts das Recht auf ein faires Verfahren nach Art. 6 EMRK. Bei der Beschlagnahme von Computern sei es sein Problem, dass die Un-

tersuchungen oft erst nach Monaten abgeschlossen seien. Die Unmöglichkeit, Geschäftsdaten zu verwenden, könne den finanziellen oder wirtschaftlichen Ruin des Besitzers bedeuten, was die Frage der Verhältnismäßigkeit im Hinblick auf das Eigentumsrecht oder zur Freiheit der Berufsausübung aufwerfe. Diese Auswirkungen müssten mitbedacht werden.

Ein ähnliches Problem ergebe sich beim Einfrieren von Konten von Personen, die ohne jede Anhörung auf eine diesbezügliche Liste gesetzt werden (EuGH-Urteil *Yusuf und Kadi*). Ferner bestünden in der EU Pläne, zur Verhinderung von Terroranschlägen und Straftaten alle im öffentlichen Raum installierten Videosysteme zusammenzuschließen und mit Datenbanken zu kombinieren.

Zu fordern sei die Entwicklung von der virtuellen Welt angepassten Regelungen, die Eingriffe in die Grundrechte nur unter äußerst restriktiven Voraussetzungen zum Schutz höherrangiger Rechtsgüter zulassen würden. Es müssten, wie dies das deutsche Bundesverfassungsgericht im Urteil zur Online-Durchsuchung ausgeführt habe, ein konkreter Tatverdacht oder eine konkrete Gefahr für Le-

ben, körperliche Integrität oder Freiheit eines Menschen oder gegen Güter der Allgemeinheit vorliegen, die die Existenz des Staates und der Menschen berühren. Verdachtslose oder verdachtsschwache Präventivmaßnahmen, die die Allgemeinheit belasten, müssten zurückgedrängt werden. Es gelte, trotz aller legitimen Maßnahmen zur Bekämpfung von Kriminalität in Ausnahmesituationen wie dem eines Terrorakts, nicht Ausnahmeregelungen zu schaffen, die die Gefahr mit sich bringen würden, „bis zur Normalität perpetuiert zu werden“.

Auch Univ.-Prof. Dr. Wolfgang Brandstetter von der Wirtschaftsuniversität Wien hat die Tendenz zu einem „Fishing for Evidence“ festgestellt, dass also durch Einsatz immer weiterer Überwachungsmaßnahmen möglichst viele Daten gewonnen werden sollen, um in einem Anlassfall ausgewertet werden zu können. Zwangsmaßnahmen in Wirtschaftsstrafverfahren wie die Beschlagnahme von Computern würden aus Sicht eines Verteidigers weiters das Problem aufwerfen, dass damit auch der Zugang zu Anwaltskorrespondenz eröffnet werde. Hinzuweisen sei auf das Gebot der Verhältnis-

mäßigkeit nach § 5 StPO: Die Maßnahmen müssten im öffentlichen Interesse liegen, geeignet und erforderlich sein und in einem angemessenen Verhältnis zum Gewicht der Straftat, zum Grad des Verdachts und zum angestrebten Erfolg stehen.

Dr. Waltraud Kotschy zeigte die datenschutzrechtlichen Grenzen der Ermittlung und Auswertung von Verdachtsdaten auf. Mag. Karin Mair von *Deloitte Forensic & Dispute Services GmbH*, Wien (www.deloitte.at), bot Einblicke in die Vorgangsweise privater Beratungsunternehmen, die mit der Aufklärung von Verdachts- oder Anlassfällen beauftragt werden, insbesondere, wie auf gerichtsfeste Weise Daten ermittelt und ausgewertet werden.

Themen der anschließenden Podiumsdiskussion zusammen mit Justizministerin Mag. Claudia Bandion-Ortner waren die Bekämpfung des Terrorismus und in diesem Zusammenhang die in parlamentarischer Beratung stehende Regierungsvorlage des Terrorismuspräventionsgesetzes 2010 (RV 674 Bg- NR 25.GP); die Bekämpfung der Kinderpornografie, Vorratsdatenspeicherung und die Kleinkriminalität im Internet („Internet-Abzocke“).

Kurt Hickisch