Zeichnung: Jens Heise

Staatliche Internet-Kriminalität im gemeinsamen Europa

von Dieter Deiseroth

Zur Strafbarkeit der Ausspähung des E-Mail-Verkehrs von deutschen Staatsangehörigen durch den italienischen Geheimdienst SISMI nach deutschem Recht

I. Mögliche Tathandlungen von SISMI-Agenten/-Bediensteten

Den italienischen Justizbehörden und insbesondere dem dortigen Obersten Richterrat („Consiglio Superiore della Magistratura" – CSM)[1] liegen Erkenntnisse vor, dass u.a. der E-Mail-Verkehr der europäischen Richterorganisation MEDEL durch Bedienstete des italienischen Militär-Geheimdienstes SISMI[2] ausspioniert worden ist. Mitglieder von MEDEL sind in Deutschland die Gruppe der in der Gewerkschaft Ver.di organisierten Richterinnen und Richter sowie die „Neue Richtervereinigung" (NRV).

Zwischen 2001 und 2006 soll SISMI ausweislich des vom CSM einstimmig verabschiedeten Untersuchungsberichts vom 4.7.2007[3] und der darin in Bezug genommenen Einzeldokumente mehr als 200 Richterinnen und Richter in Italien und in zwölf weiteren europäischen Ländern beschattet, ihre Computer und ihren E-Mail-Verkehr kontrolliert sowie ihnen teilweise auch gezielte Fehlinformationen zugespielt haben.[4] Zu den 47 italienischen Opfern sollen vor allem jene Mailänder Staatsanwälte gehören, die Verfahren gegen den Ex-Ministerpräsidenten Silvio Berlusconi eröffneten und vom SISMI-Geheimdienst als „regierungsfeindlich" eingestuft wurden. Zielobjekte von SISMI sollen auch zwei Staatsanwälte gewesen sein, die Strafverfahren gegen jenes CIA-Kommando betreiben, dem die Verschleppung des ägyptischen Predigers Abu Omar vorgeworfen wird, sowie Staatsanwalt Antonio Ingroia, der über die Querverbindungen zwischen Mafia und Politik in Italien ermittelte. Ferner sollen von den Bespitzelungsaktionen unter anderem das langjährige Vorstandsmitglied von MEDEL, Edmondo Bruti Liberati, und zahlreiche Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte betroffen sein, die als Delegierte, als Funktionsträger oder als sonstige Aktive von MEDEL vor allem über das Internet untereinander kommuniziert haben. Die Einzelheiten ergeben sich aus der fünfseitigen Entschließung des CSM vom 4.7.2007.[5]

Diese geheimdienstlichen Aktivitäten, von denen möglicherweise auch deutsche Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte als Teilnehmer am MEDEL-internen E-Mail-Verkehr und an Veranstaltungen betroffen sind, werfen die Frage auf, ob und unter welchen Voraussetzungen deutsche Strafverfolgungsbehörden diesbezügliche strafrechtliche Ermittlungen einleiten könnten. Bundesjustizministerin Brigitte Zypries hat zwischenzeitlich die deutsche Botschaft in Rom sowie ihren italienischen Amtskollegen um Unterrichtung über die Vorfälle gebeten.[6]

II. Zuständigkeit der deutschen Strafverfolgungsbehörden

Die örtliche und damit auch die internationale Zuständigkeit der deutschen Strafverfolgungsbehörden richtet sich gemäß § 143 Abs.1 GVG nach der örtlichen Zuständigkeit des entsprechenden Gerichts. Dessen Zuständigkeit ist in den Vorschriften der §§ 7–9 StPO geregelt.
Nach § 7 StPO ist das Gericht zuständig, „in dessen Bezirk die Straftat be-

gangen ist“. Damit stellt das Gesetz für die Bestimmung der Zuständigkeit der deutschen Strafverfolgungsbehörden nach §§ 7 StPO, 143 Abs.1 GVG auf den Tatort im Sinne der Vorschriften der §§ 3 ff StGB ab.[7]

Gemäß § 3 StGB gilt das deutsche Strafrecht für Taten, die im Inland begangen werden. Diese Bestimmung wird durch § 9 StGB näher konkretisiert, wonach eine Tat an jedem Ort begangen ist, an dem der Täter gehandelt hat („Handlungsort“) oder an dem der zum gesetzlichen Straftatbestand gehörende Handlungserfolg eingetreten ist („Erfolgsort“), also der Ort, an dem sich die Gefahr verwirklicht, deren Vermeidung Zweck der betreffenden Strafvorschrift ist. Wenn sich z.B. ein Hacker aus Deutschland rechtswidrig über Computer in Italien in einen Computer in den USA einwählt, so sind nach dem Territorialprinzip, das die Geltung des innerstaatlichen Strafrechts auf die im Inland begangenen Taten beschränkt, möglicherweise sowohl (auf der Grundlage von § 3 StGB) das deutsche als auch, nach Maßgabe der dortigen Bestimmungen, das italienische und das amerikanische Strafrecht[8] anwendbar.[9] Dabei ist die Bestimmung des „Erfolgsortes“ bei Distanz-, insbesondere Internet-Delikten sehr schwierig und demzufolge bislang auch nicht hinreichend geklärt.[10] Bei einem mittels einer Datenübertragung begangenen Delikt besteht ein inländischer Tatort i.S.v. § 3 StGB nur dann, wenn der „Taterfolg“, z.B. die Verletzung der durch § 202a StGB geschützten Rechtssphäre einer Person an der Integrität ihrer persönlichen digitalen Daten, im Inland eintritt.
Für Taten, die *im Ausland* gegen einen Deutschen begangen wurden, gilt das deutsche Strafrecht, „wenn die Tat am Tatort mit Strafe bedroht ist“ (§ 7 Abs. 1 StGB). Eine Strafverfolgung von im Ausland (z.B. Italien) begangenen Handlungen italienischer SISMI-Bediensteter durch deutsche Strafermittlungsbehörden setzt mithin zunächst voraus, dass ein(e) deutsche(r) Staatsbürger(in) Tatopfer ist. Ob dies im Hinblick auf die Ausspähung des E-Mail-Verkehrs zwischen deutschen Staatsangehörigen und Mitgliedern der europäischen Richtergewerkschaft MEDEL der Fall war, kann nur durch entsprechende Ermittlungen vor allem der Strafverfolgungsorgane festgestellt werden. Ferner muss im Hinblick auf § 7 Abs. 1 StGB (Tatort im Ausland; Tatopfer deutsche Staatsangehörige) die Tathandlung in Italien „mit Strafe bedroht“ sein. „Mit Strafe bedroht“ bedeutet nach der ständigen Rechtsprechung des BGH, dass das Tatortrecht „unter irgendeinem rechtlichen Gesichtspunkt“ eine Strafbarkeit der Tat vorsieht.[11] Die „völlige Übereinstimmung der Straftatbestände und ihrer Anwendung in der Praxis“ ist nicht erforderlich. Ein solcher Fall dürfte hier vorliegen. Denn in Italien ist – ebenso wie in Deutschland (vgl. dazu nachfolgend Abschnitt III.) – das Ausspähen von Daten ein Straftatbestand.[12] Dabei ist es unerheblich, ob die Strafbarkeit im Ausland im dortigen Strafgesetzbuch oder in strafrechtlichen Nebengesetzen ihren Niederschlag gefunden hat.

Allerdings steht mit der Subsumtion eines strafrechtlich relevanten Sachverhalts unter einen entsprechenden (ausländischen) Straftatbestand noch nicht fest, dass die Tat am Tatort (hier: Italien) tatsächlich strafbar ist. Insbesondere ist denkbar, dass das Tatortrecht Gegennormen enthält, die die Strafbarkeit des Verhaltens im Hinblick auf besondere weitere Umstände, die zum Zeitpunkt der Tat vorliegen, in dem konkreten Fall ausschließen. Es kommt insoweit auf die „sachlich-rechtliche Lage“ an, so dass Rechtfertigungs- und Entschuldigungsgründe des Tatortrechts beachtlich sind.[13] Im vorliegenden Falle ist nicht ersichtlich, dass sich SISMI-Bedienstete hinsichtlich des Ausspähens von Daten italienischer und deutscher Staatsangehöriger auf eine gesetzliche Befugnisnorm und damit einen Rechtfertigungsgrund stützen konnten. Insoweit wird auf die nachfolgenden Ausführungen in Abschnitt III.1.2 verwiesen.

III. Strafbarkeit des Ausspähens von Daten nach deutschem Recht

1. § 202a StGB

1.1 Tatgegenstand

Durch die Vorschrift des § 202a StGB[14] werden alle „Daten“, also durch Zeichen codierte Informationen, geschützt, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Dazu gehören jedenfalls die digitalen Daten, die im E-Mail-Verkehr zwischen Personen erstellt, ausgetauscht und gespeichert werden. Dabei spielt es keine Rolle, ob die Speicherung oder Übermittlung der Daten für persönliche Zwecke (z.B. im Rahmen gewerkschaftlicher Aktivitäten) oder im Zusammenhang mit der Wahrnehmung dienstlicher Aufgaben erfolgt.

Tatopfer: Deutsche
Tatort: Italien

„Gespeichert“ sind Daten, wenn sie zum Zweck ihrer Weiterverwendung erfasst, aufgenommen oder aufbewahrt sind. Eine „Übermittlung“ von Daten liegt vor, wenn Daten weitergeleitet werden, insbesondere im online-Verkehr von Rechner zu Rechner, sei es innerhalb eines Netzwerkes, sei es über Fernmeldewege. Der Begriff erfasst auch Handlungen, die auf Daten während eines Übermittlungsvorganges zugreifen.

Weitere Tatbestandsvoraussetzung ist, dass die Daten nicht für eine Nutzung durch den darauf zugreifenden Täter bestimmt sind. Die Entscheidung über die Bestimmung obliegt allein der Person, der die Rechtsmacht über die Daten zusteht. Im E-Mail-Verkehr ist dies in der Regel jedenfalls diejenige Person, die die Daten erstellt, übermittelt und speichert, nicht aber der darauf zugreifende Geheimdienst.
Die Daten müssen ferner, soll der Tatbestand des § 202a StGB erfüllt sein, gegen unberechtigten Zugang besonders gesichert sein. Das Merkmal des Zugangs umfasst jede technische oder physische Einwirkungsmöglichkeit auf Datenspeicher ebenso wie den physischen oder digitalen Zugang zum System und Sicherungsbereich. Eine besondere Sicherung gegen unberechtigten Zugang besteht bei Daten, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der „Geheimhaltung“ oder Abschirmung vor unbefugtem Zugriff dokumentiert hat.[15] Dies kann sowohl durch mechanische Mittel also auch durch software- oder hardware-integrierte Si-

cherungen erfolgen, die allerdings nicht den erhöhten Sicherungsgrad des § 9 BDSG erfüllen müssen. Eine besondere Sicherung gegen unberechtigten Zugang im Sinne des § 202a StGB besteht jedenfalls dann, wenn vom Berechtigten Datenverschlüsselungen oder Passwörter eingesetzt werden.[16] Das ist beim E-Mail-Verkehr bei der Verwendung von Passwörtern, die den Zugang zur Internet-Verbindung eröffnen bzw. versperren, regelmäßig der Fall.

1.2 Tathandlung

Die Tathandlung besteht nach § 202a Abs. 1 StGB darin, dass der Täter sich oder einem anderen die Daten unter Überwindung der Sicherung verschafft. Für die Strafbarkeit gem. § 202a StGB ist es unerheblich, ob die verschafften Daten Geheimnisse darstellen. Auch ist es nicht erforderlich, dass Daten verändert, zerstört oder an dritte Personen weitergegeben werden. Vielmehr sind bereits das – durch die Sicherung dokumentierte – formelle Geheimhaltungsinteresse des Netzteilnehmers und die Integrität seines Computersystems geschützt. Der Tatbestand wird jedenfalls etwa bei Infizierung mit sog. Trojanischen Pferden („Trojaner")[17] oder ähnlicher Software verwirklicht, also beim Einsatz versteckter Programme zur Erlangung von Informationen über Vorgänge und zum Ausspähen von Daten. Ein Sich-Verschaffen ist auch dann gegeben, wenn der Täter durch täuschende Einwirkung auf den Berechtigten diesen veranlasst, Daten irrtümlich selbst zu übermitteln, z.B. durch täuschende Datenabfrage beim sog. „password fishing".

Streitig ist zwar, ob bereits das Hacking in der Form eines („bloßen") unberechtigten Eindringens in fremde Dateien oder Datenübermittlungsvorgänge den Tatbestand des § 202a StGB erfüllt.[18] Da aber auch das Überwinden von Software-Sicherungen zum „Selbstzweck" des Eindringens regelmäßig die Entschlüsselung oder die Kenntnisnahme von Programmdateien voraussetzt[19] und da ohnehin ein erfolgreiches Eindringen ohne Kenntnisnahme der gesicherten Zieldateien jedenfalls bei einem Ausspionieren zu nachrichtendienstlichen Zwecken fern liegend ist, dürfte bei einem Ausspähen von im E-Mail-Verkehr zwischen Richterinnen und Richtern, Staatsanwältinnen und Staatsanwälten (privat oder dienstlich) angefallenen Daten eine von § 202a Abs. 1 StGB erfasste Tathandlung vorliegen. Diese sich bereits aus ihrem Wortlaut ergebende Auslegung der Vorschrift entspricht auch dem erkennbaren normativen Zweck der Regelung, die vom Berechtigten abgegrenzte Geheim- und Privatsphäre gegen das in der Regel heimliche, für den Betroffenen vielfach nicht erkennbare sowie nach erstmaligem „Knacken" der Zugangssicherung beliebig oft wiederholbare Eindringen in diese Sphäre zu verhindern.

Zusammenfassung

Der Beitrag untersucht die Strafbarkeit der Maßnahmen, die der italienische Geheimdienst zwischen 2001 und 2006 gegen 203 Richter und Staatsanwälte aus Italien und Europa durchgeführt hat. Darunter sind sicherlich auch Deutsche, die z.B. an Medelnet teilgenommen haben.
Das deutsche Strafrecht gilt nicht nur für Inlandstaten, sondern auch für solche, bei denen das Tatopfer die deutsche Staatsangehörigkeit hatte und die Tathandlung im Handlungsland mit Strafe bedroht ist (§ 9 StGB).
Die Voraussetzungen des § 202 a StGB (Ausspähen von Daten) liegen vor. Das Verhalten des Geheimdienstes war illegal. Allerdings ist nach § 205 StGB die Stellung eines Strafantrags erforderlich.
In Betracht kommt weiter ein Verstoß gegen § 44 Abs. 2 BDSG.
Im Rahmen von Eurojust und EJN könnte eine effektive Strafverfolgung im europäischen Kontext erfolgen.

Keine Rechtsgrundlage in Deutschland und Italien

Für die Tatbestandsverwirklichung erfordert § 202a StGB des Weiteren, dass der Täter unbefugt gehandelt hat.
Im vorliegenden Fall ist eine Befugnis des italienischen Geheimdienstes SISMI zum Ausspähen des E-Mail-Verkehrs von (deutschen) Richterinnen und Richtern, Staatsanwältinnen und Staatsanwälten im Hinblick auf ihre Mitgliedschaft oder ihre Aktivitäten in der Europäischen Richtergewerkschaft MEDEL weder nach – worauf es für die Strafbarkeit nach § 202a StGB ankommt – deutschem noch nach italienischem Recht ersichtlich.

Die Aufgaben von SISMI sind im Gesetz Nr. 801 vom 24.10.1977[20] festgelegt. In Art. 4 heißt es dazu, dass er zuständig ist für „alle Informations- und Sicherheitsaufgaben zur militärischen Verteidigung der Unabhängigkeit und Integrität des (italienischen) Staates gegen jede Gefahr, Bedrohung oder Aggression" sowie für „die mit diesen Zielen verbundene Gegenspionage." Das Nähere bestimmt der Verteidigungsminister, dem SISMI untersteht, auf der Grundlage der Direktiven und Anordnungen des Ministerpräsidenten. Spezielle Befugnisnormen enthält das Gesetz Nr. 801 nicht.
Es wäre aufschlussreich, aufgrund der erwähnten Aufklärungsversuche der Bundesjustizministerin bei ihrem italienischen Amtskollegen sowie in einem strafrechtlichen Ermittlungsverfahren die „offizielle" Rechtfertigung für die SISMI-Aktivitäten zu erfahren.

Soweit sich die SISMI-Bediensteten eine Einwilligung der betroffenen Personen zur Einsicht in die Daten durch Täuschung erschlichen haben sollten, würde eine solche nicht ausreichen, um eine Befugnis zum Ausspähen der Daten zu begründen.[21]
Gegenwärtig ist jedenfalls nicht erkennbar, dass die Ausspähung des E-Mail-Verkehrs von Mitgliedern der Richtergewerkschaft MEDEL im Hinblick auf die Wahrnehmung dieser im Gesetz normierten spezifisch militärischen Aufgabenzuweisung geeignet und erforderlich (gewesen) sein sollte, auch wenn man die Weite und Unbestimmtheit der ge-

setzlichen Aufgabenzuweisung in Rechnung stellt.
Damit dürfte jedenfalls der hinreichende Verdacht eines besonders schweren Eingriffs in das sowohl durch die Verfassung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als auch durch die Europäische Menschenrechtskonvention besonders geschützte Grundrecht auf informationelle Selbstbestimmung vorliegen, der die Aufnahme von strafrechtlichen Ermittlungen rechtfertigt.

Strafverfolgung nur auf Antrag

Zur Tatbegehung ist zumindest bedingter Vorsatz erforderlich. Davon dürfte hier auszugehen sein, da die fehlende Befugnis relativ klar erkennbar war und das in Rede stehende Handeln der SISMI-Bediensteten sogar ziel- und zweckgerichtet erfolgt sein dürfte. Dies legt jedenfalls die in der Entschließung des CSM vom 4.7.2007 erfolgte Wiedergabe der Motive und der Rechtfertigung der SISMI-Operationen nahe. Dass die SISMI-Bediensteten in einem Verbotsirrtum gehandelt haben könnten, ist nicht ersichtlich. Ein solcher wäre jedenfalls bei Einholung qualifizierten Rechtsrates vermeidbar gewesen.

1.3 Strafantrag

Nach § 205 StGB ist für die Strafverfolgung ein Strafantrag des durch die Tathandlung Verletzten erforderlich. Die deutsche Staatsanwaltschaft kann mithin nur dann tätig werden, wenn betroffene deutsche Staatsangehörige einen solchen Strafantrag stellen. Dieser Antrag ist gem. § 77b StGB innerhalb von drei Monaten nach Kenntnis der Tat und der Person des Täters zu stellen. Wenn ein Netzteilnehmer von einem Fall des Hackings betroffen wird, muss er sich deswegen innerhalb dieser Frist entscheiden, ob er – z.B. mit dem Ziel einer Durchsuchung beim Angreifer – Strafantrag stellen will.

2. Datenschutzrechtliche Regelungen

Das in Rede stehende Handeln von SISMI-Bediensteten kann unter bestimmten Voraussetzungen auch nach dem Bundesdatenschutzgesetz (BDSG) strafbar sein und in Deutschland nach Maßgabe der oben unter II. behandelten Grundsätze verfolgt werden. Strafbar macht sich nach § 44 Abs. 1 BDSG,

„(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht."

Die von § 44 Abs. 1 BDSG in Bezug genommene Vorschrift des § 43 Abs. 2 BDSG erfasst u.a. die nachfolgenden Handlungen:

„(2) ..., wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. ...
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. ... oder
6. ....."

Allerdings dürfte es im Sinne des § 44 Abs. 1 BDSG kaum der Fall oder jedenfalls nur schwer nachweisbar sein, dass die SISMI-Operationen gegen Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte vorsätzlich „gegen Entgelt" oder „in der Absicht" vorgenommen wurden, um „einen anderen zu schädigen". Das hängt vom Ergebnis der Ermittlungen ab.[22]

Zu beachten ist aber in jedem Falle, dass nach § 44 Abs. 2 BDSG die Tat nur auf Antrag verfolgt wird. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Aufsichtsbehörde.

3. Nach § 95 des Telekomunikationsgesetzes (TKG) wird auch derjenige bestraft, der entgegen § 86 Satz 1 oder 2 TKG „eine Nachricht abhört oder den Inhalt einer Nachricht oder die Tatsache ihres Empfangs einem anderen mitteilt."
Die in Bezug genommene Vorschrift des § 86 TKG hat folgenden Wortlaut:

„Mit einer Funkanlage dürfen Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden. Der Inhalt solcher Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 85 besteht, anderen nicht mitgeteilt werden. § 85 Abs. 4 gilt entsprechend. Das Recht, Funkaussendungen zu empfangen, die für die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, sowie das Abhören und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt."

IV. Nationale Grenzen von Ermittlungshandlungen

Sind bei Vorliegen der dargelegten Voraussetzungen das deutsche materielle Strafrecht anwendbar und auch die deutschen Strafverfolgungsbehörden für die Verfolgung einer Straftat zuständig, können die deutschen Strafverfolgungsbehörden nach den Regeln des geltenden Völkerrechts allerdings grundsätzlich nur auf dem deutschen Staatsgebiet tätig werden. Ermittlungsmaßnahmen deutscher Strafverfolgungsorgane im Ausland würden die Hoheitsrechte des fremden Staates verletzen. Ein deutscher Polizeibeamter oder Staatsanwalt kann somit nicht einfach ins Ausland fahren und dort ermitteln. Ebenso wenig ist den deutschen Behörden in der Regel die Durchsuchung z.B. einer italienischen Datenbank erlaubt, in der in strafbarer Weise Daten (hinsichtlich deutscher Staatsangehöriger) gespeichert worden sind. Eine solche Durchsuchung setzt vielmehr grundsätzlich ein Tätigwerden der italienischen Strafverfolgungsbehörden im Wege der Amts- oder Rechtshilfe[23] voraus, soweit nicht spezielle zwischenstaatliche Abkommen[24] oder EU-Regelungen[25] eingreifen. Zwangsmaßnahmen können von den Ermittlungsbehörden daher grundsätzlich nur auf dem eigenen Staatsgebiet vorgenommen werden; bei Ermittlungen im Ausland gelten dagegen die ausländischen Rechtsgrundlagen in Verbindung mit den einschlägigen Nor-

men über die internationale Amts- und Rechtshilfe.

V. Europarechtliche Dimensionen (Eurojust und EJN)

Käme es im Fall der hier in Rede stehenden Aktivitäten von SISMI-Bediensteten zur Aufnahme von Ermittlungsmaßnahmen deutscher Strafverfolgungsbehörden, könnte sich daraus auch eine Bewährungsprobe für die Effektivität der polizeilichen und justiziellen Zusammenarbeit innerhalb der Europäischen Union und zwischen ihren Mitgliedstaaten ergeben.

Im Jahre 2002 ist Eurojust als Organ der EU[26] mit eigener Rechtspersönlichkeit errichtet worden. Eurojust ist eine unabhängige EU-Behörde (Sitz in Den Haag) und gehört zum Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (sogenannte „dritte Säule"). Jeder Mitgliedstaat muss ein nationales Mitglied benennen, das die Eigenschaft eines Staatsanwalts, Richters oder Polizeibeamten mit gleichwertigen Befugnissen besitzt. Die nationalen Mitglieder unterliegen hinsichtlich ihres Status dem nationalen Recht des Mitgliedstaates, der sie benannt hat. Außerdem legt jeder Mitgliedstaat die Dauer des Mandats des nationalen Vertreters sowie die ihm übertragenen justiziellen Befugnisse fest.

Die Arbeit von Eurojust wird von der des Europäischen Justiziellen Netzes ergänzt. Das Europäische Justizielle Netz (EJN) ist ein 1998 von der Europäischen Union gegründetes „Netz justizieller Kontaktstellen zwischen den Mitgliedstaaten", das insbesondere für eine bessere Abwicklung von Rechtshilfeersuchen sorgen soll. Im Gegensatz zu Eurojust verfügt das Europäische Justizielle Netz nicht über eine zentrale Organisation; die verantwortlichen Beamten der nationalen Kontaktstellen in den Mitgliedstaaten kommen nur gelegentlich zu gemeinsamen Sitzungen beim Generalsekretariat des Rates der Europäischen Union zusammen. Die Strafverfolgungsbehörden können sich des EJN bei allen Arten schwerwiegender Straftaten bedienen, um die Durchführung ihrer Rechtshilfeersuchen zu erleichtern. Eurojust ist für Ermittlungen und Strafverfolgungsmaßnahmen im Bereich der schweren Kriminalität zuständig, wenn – wie im vorliegenden Fall – mindestens zwei Mitgliedstaaten betroffen sind. Diese EU-Einrichtung soll (1.) die Koordinierung zwischen den zuständigen Behörden der Mitgliedstaaten fördern sowie (2.) die internationale Rechtshilfe und die Erledigung von Auslieferungsersuchen erleichtern.

Der Zuständigkeitsbereich von Eurojust erstreckt sich u.a. auf die Kriminalitätsformen und Straftaten, die in die Zuständigkeit von Europol fallen. Dazu zählt (neben Terrorismus, Drogen- und Menschenhandel, Geldfälschungen und Geldwäsche) u.a. auch – im vorliegenden Falle einschlägig – die Computerkriminalität. Eurojust kann seine Aufgaben über eines oder mehrere nationale Mitglieder oder als Kollegium wahrnehmen. So kann Eurojust die Behörden der betroffenen Mitgliedstaaten auffordern, Ermittlungen zu führen oder die Strafverfolgung aufzunehmen sowie ein gemeinsames Ermittlungsteam einzusetzen. Es bleibt abzuwarten, ob sich die Strafermittlungsbehörden im vorliegenden Fall dieser EU-Mechanismen (Eurojust und EJN) sowie Europol bedienen werden sowie ob und ggf. in welcher Weise diese dabei ihre Leistungsfähigkeit unter Beweis stellen werden.[27]

Der Autor:

Dr. Dieter Deiseroth ist Richter am BVerwG und Mitglied der wissenschaftlichen Beiräte der Humanistischen Union, von IALANA und IPPNW.

Anmerkungen

1 Der CSM ist das oberste Selbstverwaltungsorgan der italienischen Justiz (für die Laufbahn[en] der RichterInnen und StaatsanwältInnen). Dem zur Gewährleistung der Unabhängigkeit der ital. Justiz unmittelbar durch die ital. Verfassung (vgl. Art. 104, 105, 106 und 107) eingerichteten Gremium gehören unter dem Vorsitz des italienischen Staatspräsidenten kraft ihres Amtes die Präsidenten des Kassationsgerichtshofes und der italienischen Generalstaatsanwaltschaft am Kassationsgerichtshof sowie 16 von den Richtern/Staatsanwälten Italiens („magistrati") und 8 vom italienischen Parlament (aus dem Kreis der Anwälte und Rechtsprofessoren) gewählte Vertreter an. Nähere Informationen dazu auf der Homepage des CSM unter: http://www.csm.it/

2 SISMI war in den vergangenen Jahren wiederholt in die öffentliche Kritik geraten. Die Vorwürfe betrafen u.a. seine Mitwirkung an der Erstellung von gefälschten Beweismitteln für die US-Regierung über den angeblichen Erwerb von Uran durch das Saddam-Hussein-Regime in Nigeria („Nigergate"), illegale Abhöraktionen im Bereich der italienischen Telecom sowie seine Beteiligung an der Entführung des Muslim-Predigers Abu Omar durch CIA-Bedienstete. SISMI-Direktor General Nicoló Pollari ist im November 2006 durch die Prodi-Regierung von seinem Posten abgelöst und durch Admiral Branciforte ersetzt worden. Pollari wurde zwischenzeitlich wegen seiner möglichen Beteiligung an der Abu Omar-Entführung zusammen mit 26 CIA-Agenten vor einem Mailänder Strafgericht angeklagt. Aufgrund eines vor kurzem vom ital. Parlament beschlossenen Änderungsgesetzes wird SISMI künftig seine Tätigkeiten unter der Bezeichnung „AISE" („Agenzia informazioni e sicurezza esterna" – Agentur für Informationen und äußere Sicherheit) fortführen. Der ital. Inlands-Geheimdienst SISDE trägt künftig die Bezeichnung AISI („Agenzia informazioni e sicurezza interna"), vgl. dazu u.a. FAZ v. 3.8.2007

3 Beschluss der Plenarversammlung des CSM vom 4.7.2007 auf Vorschlag seines Ersten Ausschusses („– 461/RR/2006 – Delibera del Comitato di Presidenza in data 7 novembre 2006 con la quale è stata autorizata l'apertura presso la Prima Commissione di una practica a tutela dei magistrati che, come riferiscono notizie di stampa, sarebbero stati oggetto di informative e di osservazione ad opera di appartenenti o collaboratori del servizio di informazione militare")

4 Vgl. u.a. Stellungnahmen der ital. Richtervereinigung „Associazione Nazionale Magistrati" vom 18.7.2007, der franz. Richtergewerkschaft „Syndicat de la Magistrature" vom 27.7.2007 sowie der in der Gewerkschaft Ver.di organisierten RichterInnen und Richter vom 16.7.2007 und der NRV

5 Auszüge in dt. Sprache im Beitrag von Strecker, in diesem Heft, S. 113

6 Vgl. dazu Südd. Zeitung vom 21.7.2007 und vom 10.8.2007 sowie Frankfurter Rundschau vom 4.8.2007

7 Vgl. dazu Meyer-Goßner, StPO, 50. Aufl. 2007, § 7 Rn. 2. Andere Gerichtsstände im Inland, die z.B. an den inländischen

Wohnsitz oder bei dessen Fehlen an den gewöhnlichen Aufenthalt oder letzten Wohnsitz des Beschuldigten oder den Ort der Ergreifung des Täters anknüpfen, ergeben sich aus den Regelungen der §§ 8 ff StPO

[8] Bei Kommunikationsvorgängen zwischen Nicht-Amerikanern im Ausland ist stets zu bedenken, dass vor allem Internet-Telefonate und internationale E-Mails oft über Großrechner laufen, die in den USA stehen. Es ist für einen Zugriff auf E-Mail-Korrespondenz schon deshalb nicht erforderlich, dass Absender oder Empfänger in den USA leben bzw. dort die E-Mails versenden oder empfangen. Daran knüpft das jüngst vom US-Kongress verabschiedete Gesetz an, das US-Geheimdiensten weitgehend erlaubt, Telefonate und E-Mail-Verkehr zwischen Ausländern (weltweit) abzufangen und auszuwerten, vgl. dazu Südd. Zeitung v. 6.8.2007, S. 8

[9] Bericht der Arbeitsgruppe Zugangs- und Nutzungsregelungen für die bayerischen Hochschulnetze. Bayerisches Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst. München. RB-Nr. 05/97/02. Februar 1997; in: http://www.rz.uni-wuerzburg.de/netzbericht/Abschnitt 7.3.2.a

[10] Vgl. dazu die Nachweise u.a. bei Tröndle/Fischer, a.a.O., § 9 Rn. 5 ff

[11] Vgl. u.a. BGHSt 2, 160 f; NJW 1954, 1086; BGHSt 27, 5 ff; Scholten, Das Erfordernis der Tatortstrafbarkeit in § 7 StGB, 1993, 132 ff; Tröndle/Fischer, a.a.O., § 7 Rn. 7 und 9 m.w.N.

[12] Die Strafbestimmung(en) zum Schutz digitaler Daten wurden durch das Gesetz No. 547 vom 23.12.1993 (G. U. n. 305 del 30 Dicembre 1993) in das ital. StGB (Codice Penale – CP –) eingefügt und stellen u.a. das unbefugte/missbräuchliche Eindringen in ein digitales Informationssystem (accesso abusivo ad un sistema informatico; vgl. Art. 615-ter. CP) sowie das unbefugte/missbräuchliche Aufspüren und Nutzen von Passwörtern (detenzione e diffusione abusiva di password e codici d'accesso; vgl. Art.615-quater. CP) und die Verletzung der digitalen Kommunikationsfreiheit (intercettazione di comunicazioni informatich telematiche; vgl. Art. 617-quater. CP) unter Strafe. Auf die Einzelheiten der ital. strafrechtlichen Regelungen kann hier nicht näher eingegangen werden.

[13] Vgl. dazu die Nachweise bei Scholten, a.a.O., 145 ff, zur Rspr. des BGH und von Obergerichten

[14] Die im Hinblick auf das Verfassungsgebot des „nullum crimen/nulla poena sine lege" notwendige Geltung des Straftatbestandes des § 202a StGB („Ausspähen von Daten") ist für den Tatzeitraum zu bejahen. Denn die Vorschrift ist durch Art. 1 Nr. 7 des 1986 in Kraft getretenen 2. WiKG (BGBl. I 721) und damit bereits vor den hier in Rede stehenden in den Jahren 2001–2006 erfolgten SISMI-Aktivitäten in das deutsche Strafgesetzbuch eingefügt worden. Vgl. Bühler, MDR 1987, 448 ff

[15] Vgl. dazu u.a. Bühler, MDR 1987, 453

[16] Tröndle/Fischer, a.a.O., § 202a Rn. 8

[17] Zu den technischen Grundlagen vgl. u.a. Markus Hansen, Andreas Pfitzmann: Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, DRiZ (August-Heft) 2007, S. 225 ff.

[18] Diese Unklarheit soll in Umsetzung des Übereinkommens des Europarats über Computerkriminalität sowie des Rahmenbeschlusses 2005/222/JI des EU-Rates vom 24.2.2005 über Angriffe auf Informationssysteme demnächst durch das Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (vgl. Entwurf der Bundesregierung vom 20.9.2006) bereinigt werden.

[19] Vgl. dazu Bühler, MDR 1987, 452; Tröndle/Fischer, a.a.O. § 202a Rn. 11 f m.w.N.

[20] „Istituzioni e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto die Stato", vgl. http://www.serviziinformazionesicurezza.gov.it/pdcweb.nsf/pagine/sismi (7.8.07)

[21] Für Eingriffe von Strafverfolgungsbehörden kommen in Deutschland § 94 StPO sowie § 100a ff StPO in Betracht. Die heimliche Durchsuchung der im Computer eines Beschuldigten gespeicherten Dateien mit Hilfe eines Programms, das ohne Wissen des Betroffenen aufgespielt wurde (verdeckte „Online-Durchsuchung"), ist nach der jüngsten Rechtsprechung des Bundesgerichtshofs wegen fehlender Ermächtigungsgrundlage unzulässig; BGH, Beschluss vom 31.1.2007 (Az StB 18/06).

[22] Auf die Frage, ob die SISMI-Aktivitäten im Übrigen mit datenschutzrechtlichen Vorschriften vereinbar waren, kann hier nicht näher eingegangen werden.

[23] Vgl. dazu die Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt) v. 18.9.1984 i.d.F. v. 1.7.1994, abgedr. u.a. bei Piller-Herrmann, Justizverwaltungsvorschriften, Loseblatt-Textsammlung, unter 2 f

[24] Vgl. dazu die Zusammenstellung bei Schomburg, NJW 2005, 3264

[25] Vgl. dazu das am 23.8.2005 in Kraft getretene Übereinkommen von 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union sowie das dt. Gesetz vom 22.7.2005, verkündet am 27.7.2005, BGBl II, Nr. 16, S. 650, Inkrafttreten am 28.7.2005; vgl. zu den Gesetzgebungsmaterialien BT-Drs. 15/4232 und 15/4233; allgemein vgl. Meyer-Goßner, StPO, a.a.O., Einl. 214 ff

[26] Vgl. hierzu den Beschluss des EU-Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität

[27] In dem Bericht der EU-Kommission vom 6. Juli 2004 „Rechtliche Umsetzung des Beschlusses des Rates vom 28. Februar 2002 über die Einrichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität" wurde seinerzeit eine sehr enttäuschende Bilanz der Arbeit von Eurojust (bis zum damaligen Stichtag 30.9.2003) gezogen. Die EU-Kommission bezweifelte damals, dass die in den Mitgliedstaaten geltenden Rechtsvorschriften ausreichend sind, um den Eurojust-Beschluss in vollem Umfang wirksam werden zu lassen und daraus ein effizientes Instrument zu machen. Daher hat sie alle Mitgliedstaaten aufgefordert, für eine rasche und vollständige Umsetzung des Beschlusses zu sorgen und ihnen folgende Maßnahmen empfohlen: Klärung einiger wesentlicher Punkte durch Verfassen von Leitlinien oder eines Rundschreibens, auch wenn nicht unbedingt Legislativmaßnahmen erforderlich sind; Gewährleistung eines hinreichend zügigen Informationsflusses; Übertragung der erforderlichen justiziellen und/oder Ermittlungsbefugnisse an die nationalen Eurojust-Mitglieder.

Und so sehen Richtergehälter in USA aus – wer sollte da nicht neidisch werden?
http://www.ncsconline.org/WC/Publications/KIS_JudComJudSal010107Pub.pdf