erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Dominik Brodowski und Felix Freiling

Transnationale Cyberkriminalität vs. nationale Strafverfolgung: Mögliche Auswege aus einem grundsätzlichen Dilemma

Cyberkriminalität wird nicht selten über Landesgrenzen hinweg begangen und stellt daher ein transnationales Phänomen dar. Die Strafverfolgung hingegen wird grundsätzlich von den Nationalstaaten betrieben und ist daher im Ausgangspunkt an nationalstaatliche Regelungen gebunden. Dieser Beitrag möchte durch einen skizzenhaften Problemaufriss zum Nachdenken über dieses grundsätzliche Dilemma anregen.

Das Problem

Das Internet stellt eine Kommunikationsinfrastruktur zur Verfügung, mit deren Hilfe sich Computer und Personen auf sehr einfache Art und Weise weltweit vernetzen können. Interaktive Webseiten wie Blogs und soziale Medien sowie ein transnational ausgerichteter E-Commerce erzeugen bei vielen Menschen den Eindruck eines Raumes grenzenloser Kommunikationsfreiheit. Dass mit dem Internet nationalstaatliche Grenzen jedoch nicht verschwunden sind, merkt man spätestens dann, wenn man selbst Opfer von Cyberkriminalität geworden ist – etwa durch betrügerische Nutzung gestohlener Kreditkarteninformationen oder dadurch, dass man seinen eigenen Rechner nach einer Infektion mit erpresserischer Ransomware freikaufen muss.

Die digitale Schattenwirtschaft agiert professionell, arbeitsteilig und seriösen Schätzungen zufolge (Anderson et al., 2013) mit großem ökonomischen Gewinn. Bei aller Notwendigkeit, die technischen Ursachen von Cyberkriminalität zu verstehen und diesen entgegenzuwirken (Brodowski & Freiling, 2011, S. 81 ff.), erfordert das soziale Problem von Cyberkriminalität auch eine (straf)rechtliche Antwort. Diese wird aber dadurch erschwert, dass Cyberkriminalität nicht vor den Grenzen der Nationalstaaten halt macht.

Auch wenn man das Internet aus technischer wie aus soziologischer Sicht als *virtuellen Cyberspace* verstehen kann, so nimmt jedes Verhalten im Internet seinen Ursprung in einem menschlichen Verhalten und lässt sich daher auf einen physischen Ort zurückführen. Neben diesem *Handlungsort* gibt es noch eine Fülle weiterer Anknüpfungspunkte dafür, dass das materielle Strafrecht eines bestimmten Nationalstaats anwendbar ist. Daher ist ein transnationales, kriminelles Verhalten im Regelfall nach dem Recht mehrerer Staaten strafbar. Das grundlegende Problem, das dieser Artikel beleuchten möchte, entsteht nun in der Vielzahl von Fällen, in denen die Strafverfolgungsbehörden in einem Staat A eine Straftat verfolgen wollen (und dürfen), dabei jedoch auf Ermittlungen in einem anderen Staat B angewiesen sind, um diese Straftat erfolgreich aufzuklären und um den oder die Straftäter wegen dieser Straftat zu verurteilen.

In all diesen Konstellationen sind die Strafverfolgungsbehörden im Staat A nämlich im Ausgangspunkt dadurch eingeschränkt, dass sie nur in diesem Staat – aber nicht im Staat B – tätig werden dürfen, ohne die Souveränität des anderen Staates zu verletzen und möglicherweise eine Straftat nach dem Strafrecht des Staates B zu begehen. Ein Beispiel hierzu aus der analogen Welt: Wenn ein Polizist aus dem Staat A ohne entsprechende Befugnis des Staates B auf dessen Staatsgebiet einen Verdächtigen festnimmt und auf verschlungenen Pfaden nach A verbringt, so wird dies zum einen zu erheblichen diplomatischen Verwicklungen führen. Da Entführungen in wohl allen Staaten strafbar sind, wird sich zum anderen der Polizist im Staat B wegen der nach dortigem Recht rechtswidrigen Entführung des Verdächtigen strafrechtlich verantworten müssen.

Es liegt somit eine Souveränitätskollision vor: Einerseits gehört es zu den Kernaufgaben eines souveränen Staates, seine Staatsgewalt in seinem eigenen Staatsgebiet auszuüben – und damit für den Staat A, sein materielles Strafrecht durchzusetzen und hierdurch auch die Restitution der durch die Straftat Geschädigten zu unterstützen. Andererseits aber bedeutet staatliche Souveränität auch, den Staat und die im Staatsgebiet ansässigen Personen vor einer Machtausübung anderer Staaten zu schützen – und damit für den Staat B, seine Bürger sowohl davor zu schützen, dass sie selbst in den Staat A verschleppt werden, als auch davor, dass ihre Daten in den Staat A transferiert werden.

Welche Wege kann man prinzipiell einschlagen, um dem (jedenfalls in etlichen Fällen legitimen) Schutzbedürfnis der Nutzer Rechnung zu tragen – und damit etwa deutsche Nutzer vor einem zu weitreichenden Datentransfer in die USA zu schützen – und gleichzeitig den Schutzanspruch der Staaten – und damit die transnationale Durchsetzung von Strafnormen – nicht vollständig zu verraten? Wir skizzieren drei mögliche Alternativen.

Alternative 1: Transnationale Kooperation gegen Cyberkriminalität

Die Praxis behilft sich bislang vor allem mit einer Kooperation der nationalen Kriminaljustizsysteme (Brodowski & Freiling, 2011, S. 173 ff.). Stimmt nämlich der Staat B der Durchführung einer Strafverfolgungsmaßnahme in seinem Staatsgebiet zu oder führt der Staat B eine Strafverfolgungsmaßnahme auf Ersuchen des Staates A durch, so liegt keine Souveränitätsverletzung des Staates B vor. Kann das der Strafverfolgung zugrundeliegende Verhalten auch durch den Staat B verfolgt werden, so wird oftmals in beiden Staaten A und B ein Ermittlungsverfahren gegen den oder die Verdächtigen eingeleitet. Beide Staaten nehmen dann in ihrem jeweiligen Staatsgebiet die erforderlichen Ermittlungen vor und tauschen sich regelmäßig über die gewonnenen Erkenntnisse aus. Auch auf diesem Wege sogenannter Spiegelverfahren oder Parallelermittlungen treten somit keine Souveränitätsverletzungen auf.

Solche formellen und informellen Kooperationen sollen durch eine Vielzahl von Instrumenten, die teils spezifisch die Verfolgung von Cyberkriminalität betreffen, beschleunigt und erleichtert werden. So ist exemplarisch zu verweisen auf internationale Übereinkommen wie die sogenannte *Cybercrime Convention* (Übereinkommen über Computerkriminalität, 2001), auf die (noch in nationales Recht umzusetzende) Europäische Ermittlungsanordnung der EU (Richtlinie 2014/41/EU, 2014), auf rund um die Uhr erreichbare Kontaktstellen bei den Polizeien, aber auch auf die Etablierung sehr erfolgreicher informeller wissenschaftlicher und organisatorischer Kooperationen, etwa im Bereich der Internet-Beschwerdestellen und bei der Bekämpfung von Botnetzen.

Dennoch stoßen diese Kooperationsmodelle in vielen Fällen an ihre Grenzen: So dauert insbesondere die förmliche Rechtshilfe in Strafsachen oft recht lange – während sich die gesuchten Daten schnell vom Staat B in einen weiteren Staat C transferieren oder löschen lassen. Faktisch stellt sich nicht selten das Problem, dass es schwierig herauszufinden ist, in welchem Staat die gesuchten Daten tatsächlich gespeichert sind. Schließlich bedeutet die Involvierung mehrerer Kriminaljustizsysteme auch einen erheblichen Ressourcenaufwand. Und nicht immer ist ein Staat – etwa wegen des Ressourcenaufwands oder wegen einer anderen Bewertung, ob das Verhalten tatsächlich verfolgenswert ist – überhaupt bereit, einem anderen Staat Hilfe zur dortigen Strafverfolgung zu leisten.

Auch eine Verlagerung der Verfolgung von Cyberkriminalität auf eine supranationale Instanz – etwa auf einen internationalen Gerichtshof oder ein internationales Tribunal zur Verfolgung von Cybercrime (Schjolberg, 2014) – wäre mit der Schwierigkeit verbunden, dass erst ein Konsens gefunden werden müsste, welches Verhalten überhaupt strafbar sein soll. Zudem wäre eine solche zentrale Institution mit der Quantität an Cyberkriminalität schlicht überfordert und auf die Zusammenarbeit mit den (in ihren Befugnissen unverändert auf ihr Territorium begrenzten) Nationalstaaten angewiesen (Safferling, 2012, S. 262). Ohnehin erscheint eine globale Einigung auf eine zentrale Strafverfolgung – die nicht einmal in Bezug auf schwerste Verbrechen gegen die Menschheit erzielt werden konnte – mit territorial nicht begrenzten Ermittlungskompetenzen politisch schlicht als nicht durchsetzbar.

Alternative 2: Reduktion des Schutzversprechens der Nationalstaaten

Eine zweite Alternative besteht darin, das Schutzversprechen des Staates gegenüber seinen Bürgern einzuschränken. Bezogen auf den Schutz vor Cyberkriminalität beschreibt dies den Zustand, den viele Nutzer derzeit im Internet faktisch erleben. Denn nicht selten merken Nutzer gar nicht, dass sie Opfer von Cyberkriminalität geworden sind; die Strafverfolgungsbehörden sind aus den genannten Gründen nicht selten bei der Verfolgung von Delikten dann ohnmächtig, wenn die Spur der Täter eine Staatsgrenze überquert.

Man kann nun argumentieren, dass man aus der Not – also der Hilflosigkeit von Nutzern und Behörden – dadurch eine Tugend macht, dass man öffentlich feststellt, dass für bestimmte Tätigkeiten und Vorkommnisse keinerlei staatlicher Schutz übernommen wird. In Analogie zu den Reisewarnungen des Auswärtigen Amtes könnte beispielsweise das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) Webseiten oder Netzbereiche als *unsicher* einstufen und Schutzpflichten des Staates gegenüber seinen Bürgern einschränken, sollte man sich trotzdem auf diese Seiten bewegen. Dies hätte sicherlich einen nicht vernachlässigbaren Effekt auf das Verhalten von Nutzern, die bestimmte Online-Dienstleistungen und Websites meiden und sich beim Surfen im Netz anders verhalten würden. Ein solches Vorgehen hätte also durchaus ein präventives Potenzial.

Dennoch sprechen verschiedene, gewichtige Gründe gegen ein solches Vorgehen. Ein erster Grund liegt sicherlich in den ökonomischen Einschränkungen, die die Veränderung des Nutzerverhaltens nach sich ziehen würde, bis hin zu einer generellen *Abkehr vom Netz,* was auch viele Effizienzmaßnahmen in der öffentlichen Verwaltung (E-Government) konterkarieren würde. Viel schlimmer: Durch einen solchen Ansatz würde der Nationalstaat teilweise auf die Durchsetzung des Rechts auf eigenem Boden verzichten; das Internet würde tatsächlich mehr und mehr zu einem *rechtsfreien* Raum werden. Dies käme einer Kapitulation des Strafrechts vor dem Problem transnationaler Cyberkriminalität gleich – ein grundsätzlicher *Dammbruch*, dessen Folgen unabsehbar wären.

In anderer Hinsicht sind jedoch Reduktionen des Schutzversprechens verbreitet – namentlich insoweit, als ein Staat B sein Versprechen zurücknimmt, seine Bürger vor transnationalen Eingriffen des Staates A zu schützen. Das ist beispielsweise faktisch in der Ohnmacht der europäischen Politik gegenüber der Netzüberwachung durch US-amerikanische Geheimdienste zu ver-

zeichnen. Völkervertraglich spiegelt sich dieser Lösungsansatz in einer Erlaubnis wider, die sich die Vertragsstaaten der *Cybercrime Convention* eingeräumt haben: Demzufolge darf ein Vertragsstaat A auch online auf Computerdaten zugreifen, die sich im Vertragsstaat B befinden, wenn A „die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten … [an A] weiterzugeben" (Übereinkommen über Computerkriminalität, 2001).

Nach Auffassung des Schweizerischen Bundesgerichts sind auf dieser Grundlage ausländische E-Mail-Provider befugt, die E-Mails ihrer Kunden an schweizerische Strafverfolgungsbehörden auszuhändigen, soweit diese Provider – wie üblich – in ihren Allgemeinen Geschäftsbedingungen (dem „Kleingedruckten") einen entsprechenden Kooperationsvorbehalt aufgenommen haben (Schweiz. BGer, Urt. v. 14.1.2015, 1B_344/2014, 2015). Das bedeutet eine Privatisierung der Strafrechtspflege, da nicht länger die Nationalstaaten, sondern nunmehr Internetprovider über einen transnationalen Datentransfer zu Strafverfolgungszwecken entscheiden. Noch weiter geht die Auffassung der US-amerikanischen Regierung in einem noch anhängigen Gerichtsverfahren gegenüber Microsoft, die von einer Pflicht zur Kooperation spricht (Microsoft v. USA, 2nd Cir, 14-2985-CV, pending). Und bemerkenswert ist eine vergiftete Klausel in einem aktuellen US-amerikanischen Gesetzesvorhaben, das Ausländern (rudimentären) Rechtsschutz in Datenschutzfragen vor amerikanischen Gerichten einräumt: Sollte nämlich ein ausländischer Staat einem strafverfolgungsbezogenen Datenaustausch eines Internetproviders mit US-amerikanischen Behörden entgegentreten – mit anderen Worten: sollte dieser Staat seinen Souveränitätsanspruch geltend machen –, verlören sämtliche Bürger dieses Staates diese Rechtsschutzmöglichkeiten wieder (Judicial Redress Act, 2015). Doch auch in Deutschland sind Stimmen in der Rechtswissenschaft zu hören, die vertreten, dass man den durch Strafverfolgungsbehörden erzwungenen Zugriff technisch nicht von einem freiwilligen Zugriff des berechtigten Nutzers unterscheiden kann. Solange sich daher der Polizist nicht ins Ausland begebe, sondern auf Daten nur *online* – etwa auf der (insoweit zweifelhaften (Brodowski & Eisenmenger, 2014)) Grundlage des § 110 Abs. 3 StPO – zugreife, werde die Souveränität des ausländischen Staates nicht verletzt (Wicker, 2013; Zerbes & El-Ghazi, 2015).

Zwar hat dieser Lösungsansatz einer Souveränitätsreduktion den Charme, dass er ressourcenschonend eine transnationale Verfolgung von Cyberkriminalität erleichtert. Dennoch sind auch hier etliche Gefahren zu erkennen. So sind die Möglichkeiten, sich effektiv gegen strafrechtliche Vorwürfe zu verteidigen, im transnationalen Kontext noch immer stark eingeschränkt. Besonders bedrohlich ist eine solche Souveränitätsreduktion im Internet jedenfalls dann, wenn sich nicht nur demokratische Rechtsstaaten auf diese berufen und Unrechtsregime global tätige Internetdienstleister in die Pflicht nehmen, sie bei einer illegitimen Strafverfolgung (z. B. gegen Regimekritiker) zu unterstützen.

Alternative 3: Nationale Netze mit Grenzkontrollen

Eine dritte Alternative besteht darin, die Internationalität des Internets einzuschränken, also nationale oder regionale Netze zu schaffen und diese an den Grenzen intensiv zu kontrollieren. Man würde beispielsweise deutsche Netzanbieter dazu verpflichten, ihre Netzinfrastruktur vollständig auf deutschem Territorium zu betreiben und an den Übergangsstellen ins Ausland eine aufwändige Überwachungsinfrastruktur bereitzustellen, die Straftaten einschränken und die Rückverfolgung von Straftätern erleichtern soll. Es gibt durchaus verschiedene Vorbilder für ein solches Vorgehen (Lee & Liu, 2012; Clayton, Murdoch & Watson, 2006; Ensafi et al., 2015) – auch wenn dort die Motivation mitnichten darin besteht, die eigenen Einwohner vor internationaler Cyberkriminalität zu schützen.

Zwar ist bereits viel über nationale Netze diskutiert worden, etwa unter dem Stichwort „Entnetzung" (Gaycken & Karger, 2011) oder im Kontext von *Internetfiltern,* welche den Zugriff auf Kinderpornografie erschweren sollten (Sieber, 2009). Neuen Auftrieb hat diese Diskussion durch ein aktuelles Urteil des EuGH erhalten, das – auch im Kontext der Snowden-Enthüllungen – den Transfer personenbezogener Daten aus der EU in die USA jedenfalls erschwert hat (EuGH, Urt. v. 6.10.2015, C-362/14, 2015).

Drei Gründe sprechen aber zuvörderst gegen eine solche Lösung. Der erste ist ökonomischer Natur, denn nationale Netze sind aus betriebswirtschaftlicher Sicht schwer zu legitimieren. Die großen internationalen Internet-Carrier können sehr viel effizienter die globalen Datenströme abwickeln, wenn sie unabhängig von geographischen Grenzen agieren können. Durch die Medien wird zwar suggeriert, dass ein Großteil des Netzverkehrs in hierarchischer Form über zentrale Internetknoten wie den DE-CIX in Frankfurt abgewickelt wird. Die tatsächliche Vernetzungsstruktur im Internet ist jedoch

Was kann man tun?

Das Internet ist genauso tückisch wie die reale Welt:

- Nepper, Schlepper, Bauernfänger (jetzt weltweit)

Mindeststandard an technischem Schutz

- Virenschutz aktuell halten (auch die kostenlosen Programme sind gut)
- Betriebssystem und Anwendungen aktuell halten (automatische Updates)

Wichtiger noch: Medienkompetenz – drei Regeln

1. Bleiben Sie misstrauisch
   - Es ist naiv zu glauben, im Internet gibt es alles umsonst
   - Woher weiß ich, wer am anderen Ende der Leitung sitzt?
2. Im Zweifel auf Funktionalität verzichten
   - Neue Features bedeuten oft neue Probleme
   - Fremde Software birgt neue Gefahren
3. Erstatten Sie Anzeige oder beschweren Sie sich!
   - Online-Anzeige bei Ihrer Polizei
   - Internet-Beschwerdestelle

Felix Freiling, 2015

durch komplexe und in ihrer Gänze auch nicht öffentlich bekannte Peering-Vereinbarungen zwischen den Netzanbietern gegeben, die gemäß betriebswirtschaftlichen Erwägungen geschlossen werden.

Der zweite Grund ist technischer und rechtlicher Natur, denn es ist nicht einmal in Ansätzen klar, wie man effektive Grenzkontrollen in einem national aufgeteilten Internet realisieren könnte. Das im Zuge der Flüchtlingskrise wieder ins öffentliche Bewusstsein gedrungene realweltliche Analogon, also physische Kontrollen an den Grenzübergängen, erscheint vom Erfolgspotenzial her geradezu traumhaft gut: Zwar mag die Entdeckungsgefahr für Schmuggler oder Schleuser bei physischen Grenzkontrollen gering erscheinen, doch setzen sie sich immer einem nicht vernachlässigbaren Ergreifungsrisiko aus. Im Vergleich hierzu sind digitale Grenzkontrollen durch automatisierte kryptographische Verschleierungstechniken verhältnismäßig einfach zu überwinden. Eine effektive Kontrolle an den Außengrenzen des Netzes wäre vermutlich nur flankiert durch eine umfassende innerstaatliche Netzüberwachung wirksam, welche die Kontrolle von Endgeräten einschließen müsste. Die dadurch notwendigen Grundrechtseingriffe wären um mehrere Größenordnungen gravierender als jene, die im Kontext der Vorratsdatenspeicherung diskutiert wurden und werden.

Drittens würde die Regulierungsmacht der Nationalstaaten über das Internet – beziehungsweise über die dann entstehenden Inter*netze* – gestärkt, was insbesondere in Unrechtsregimes der liberalisierenden Kraft des Netzes Einhalt gebieten würde.

Fazit

Kriminalität überwindet seit jeher räumliche Grenzen: Sei es, dass Waren ü ber Staatsgrenzen hinweg geschmuggelt werden; sei es, dass Täter über Staatsgrenzen fliehen. Die zunehmende Vernetzung und räumliche Entgrenzung der Informationstechnologie führt daher im Ausgangspunkt nur zu einer Intensivierung bekannter Phänomene, namentlich der Frage, wie eine Strafnorm auch über Staatsgrenzen hinaus durchgesetzt werden kann – und wann solch einer transnationalen Strafverfolgung entgegenzutreten ist.

Dieser Beitrag hat drei mögliche Wege aufgezeigt, wie dieser Problemlage grundsätzlich begegnet werden könnte. Alle drei Wege sind jedoch mit erheblichen rechtsstaatlichen und teils auch rechtspraktischen Gefahren verbunden; alle drei Wege sind nicht hinreichend erfolgversprechend; auf allen drei Wegen gerät die nationalstaatliche Souveränität zunehmend an faktische Grenzen. In jedem Falle aber muss ein Mehr an transnationaler Strafverfolgung auch mit einem Mehr an Schutz für den Einzelnen vor illegitimer Strafverfolgung verbunden werden. Denn nur eine legitime, am Schutz von Grund- und Menschenrechten orientierte ausländische Strafverfolgung kann eine hinreichende Rechtfertigung dafür bieten, dass ein Staat seine Bürger – und deren Daten – einer ausländischen Strafverfolgung preisgeben darf.

Danksagung

Wir danken Christoph Safferling und Christian Rückert für deren wertvolle Anmerkungen zu einem Entwurf dieses Beitrags. Dieser Beitrag ist teilweise im Rahmen des BMBF-geförderten Projekts „Open Competence Center for Cyber Security – OpenC3S“ entstanden.

Referenzen

Anderson, R. et al. (2013). Measuring the cost of cybercrime. In R. Böhme (Hrsg.), *The economics of information security and privacy – WEIS 2012: 11th annual workshop on the economics of information security* (S. 265–300). Berlin: Springer.

Brodowski, D. & Eisenmenger, F. (2014). Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden. Sachliche und zeitliche Reichweite der „kleinen Online-Durchsuchung“ nach § 110 Abs. 3 StPO. *ZD,* 119–126.

Brodowski, D. & Freiling, F. C. (2011). *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft.* Berlin: Forschungsforum Öffentliche Sicherheit.

Clayton, R., Murdoch, S. J. & Watson, R. N. M. (2006). Ignoring the great firewall of China. In G. Danezis & P. Golle (Hrsg.), *Privacy enhancing technologies.* LNCS Bd. 4258 (S. 20–35). Berlin: Springer.

Ensafi, R. et al. (2015, April). Analyzing the great firewall of China over space and time. *Proceedings on Privacy Enhancing Technologies, 2015* (1), 61–76.

EuGH, Urteil v. 6.10.2015, C-362/14.

Gaycken, S. & Karger, M. (2011). Entnetzung statt Vernetzung. Paradigmenwechsel bei der IT-Sicherheit. *MMR,* 3–8.

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, United States District Court (SDNY) Memorandum and Order of 25 April 2014, 13-Mag-2814, upheld by Order of the United States District Court (SDNY) of 11 August 2014. Appeal (pending): Microsoft Corporation v. United States of America United States Court of Appeals (2nd Cir) 14-2985-CV.

Judicial Redress Act of 2015. H.R. 1428, 114th Congress; S. 1600, 114th Congress.

Lee, J.-A. & Liu, C.-Y. (2012). Forbidden city enclosed by the great firewall: The law and power of internet filtering in China. *Minnesota Journal of Law, Science & Technology, 13,* 125–152.

Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen. ABlEU 2014 L 130 v. 1.5.2014, S. 1–36.

Safferling, C. (2012). *International Criminal Procedure.* Oxford: OUP.

Schjolberg, S. (2014). *The History of Cybercrime, 1976-2014.* Norderstedt: Books on Demand.

Schweizerisches Bundesgericht, Urteil v. 14.1.2015, 1B_344/2014.

Sieber, U. (2009). Sperrverpflichtungen gegen Kinderpornografie im Internet. *JZ,* 653–662.

Übereinkommen über Computerkriminalität v. 23.11.2001. ETS Nr. 185.

Wicker, M. (2013). Durchsuchung in der Cloud. Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden. *MMR,* 765–769.

Zerbes, I. & El-Ghazi, M. (2015). Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung. *NStZ,* 425–433.

Informationen zu den Autoren Dr. Dominik Brodowski und Prof. Dr. Felix Freiling finden Sie auf Seite 26.