Dr. Lorenz Franck

Herausgabe von Passwörtern und der nemo-tenetur-Grundsatz

Ermittlungsbehörden sind gegen moderne Verschlüsselungsverfahren weitgehend machtlos. In verschiedenen nationalen Rechten existieren daher Ansätze, den Inhaber des Schlüssels zur Kooperation zu zwingen. Der nachfolgende Beitrag identifiziert die Pflicht zur Herausgabe von Passwörtern als Fremdkörper im System des Beweismittelrechts und als nicht zu rechtfertigende Grundrechtsverletzung. Dies hindert den deutschen Gesetzgeber an der Einführung derartiger Maßnahmen und hat Auswirkungen auf die Verwertbarkeit von im Ausland gewonnenen Ermittlungsergebnissen.

I. Einführung

„Rubber hose cryptanalysis" heißt im Englischen die Gewinnung von kryptographischen Schlüsseln durch schiere Gewalt gegen den Schlüsselinhaber[1]. In rechtliche Formen gegossen bedeutet dies, dass Angeklagte oder Zeugen durch obrigkeitliche Sanktionen – in der Regel Haft oder Geldstrafen – zur Aufgabe von Verschlüsselungspasswörtern bewegt werden sollen. In einigen Staaten[2] existieren bereits entsprechende Vorgehensweisen.

II. Rechtsvergleichender Überblick

1. USA

Die US-amerikanische Bill of Rights schützt grundsätzlich vor Selbstbelastungen im Strafprozess. Die entsprechende Passage im fünften Verfassungszusatz lautet: *„No person […] shall be compelled in any criminal case to be a witness against himself […]."* Die Passwortherausgabe gilt als geschützte Aussage in diesem Sinne. Dennoch haben sich die Gerichte bereits mehrfach mit dem Zwang zur Entschlüsselung befasst und die rechtlichen Vorgaben konkretisiert.

In *United States of America v. Rogozin*[3] erfragten Beamte das Passwort, ohne auf die sog. Miranda-Rechte hinzuweisen. Der mit der Sache befasste US District Court of Western New York verwarf daher sämtliche erlangten Beweismittel.

In der Sache *Grand Jury Subpoena to Sebastien Boucher*[4] entschied der US District Court von Vermont, dass seitens des Angeklagten zwar nicht das Passwort selbst, wohl aber

1 Zur Begriffsgeschichte siehe groups.google.com/forum/#!msg/sci.crypt/RjpbAJNfLd0/DSZ5EJTzDsUJ.

2 Die unter II. getroffene Aufzählung ist keineswegs abschließend.

3 09-cr-379, 2010 WL 4628520 vom 16. November 2010. Vergleiche auch United States v. Kirschner, 09-MC-50872, 2010 WL 1257355 vom 30. März 2010.

4 2:06-mj-91, 2009 WL 424718 vom 19. Februar 2009. Zu den Besonderheiten des Falles gehörte unter anderem, dass Grenzbeamte die Dateiinhalte teilweise bereits auf dem Bildschirm gesehen hatten.

die Inhalte der verschlüsselten Festplatte herausgegeben werden mussten. Der US Disctrict Court von Colorado entschied in *United States of America v. Ramona Camelia Fricosu*[5] nach demselben Schema. Diesen beiden Fällen war allerdings gemein, dass die Ermittlungsbehörden bereits gesicherte Erkenntnisse darüber besaßen, dass sich belastendes Beweismaterial auf den Datenträgern befand.

Anders lag dies wiederum in der Entscheidung *United States of America v. John Doe*[6] des Court of Appeals, Eleventh Circuit. Hier war unklar, ob bzw. welche Daten in den vorgefundenen verschlüsselten Containern gespeichert waren. Das Gericht gelangte zu der Überzeugung, dass bereits die Entschlüsselung an sich als Aussage im Sinne des fünften Verfassungszusatzes gewertet werden müsse und erklärte die Entschlüsselungsanordnung für rechtswidrig.

Wie mit verschlüsselten Datenträgern in Zukunft umgegangen werden soll, ist unter amerikanischen Juristen weiterhin umstritten[7]. Teilweise werden geeignete Vorkehrungen gefordert, die einen gestuften Zwang zur Entschlüsselung[8] ermöglichen. Bei konsequenter Weigerung wird sogar eine Schuldvermutung vorgeschlagen[9].

2. Vereinigtes Königreich

Seit Oktober 2007 ist im Vereinigten Königreich der sog. „Regulation of Investigatory Powers Act 2000" (RIPA) in Kraft[10]. Gemäß Part III, Sections 49 ff. RIPA können Personen angewiesen werden, verschlüsselte Inhalte lesbar zu machen bzw. den entsprechenden Schlüssel direkt herauszugeben[11]. Nach Part III, Section 53 RIPA drohen bei Zuwiderhandlung in Fällen nationaler Sicherheit bis zu fünf Jahre Haft, ebenso in Fällen von child indecency, in allen anderen Fällen zwei Jahre Haft. Die ersten Verurteilungen wurden bereits ausgesprochen. Eine Berufung der Betroffenen auf die Selbstbelastungsfreiheit (privilege of self-incrimination) sowie das Recht auf ein faires Verfahren nach Art. 6 MRK wurden seitens des Supreme Court of Judicature verneint[12]. Zur Begründung führten die Richter an, das Passwort besäße eine vom bloßen Willen des Beschuldigten losgelöste eigenständige Existenz, vergleichbar mit Blut-, Urin- und Gewebeproben. Zugleich sei der Schlüssel selbst nicht belastend, sondern lediglich die verschlüsselten Inhalte[13].

3. Frankreich

In Frankreich gilt das Gesetz 2001-1062 vom 15. November 2001 betreffend die Sicherheit im Alltag (Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne)[14]. Der darin enthaltene Art. 30 fügte einige neue Regelungen in den Code de procédure pénal (C.P.P.) ein. Gemäß den neu geschaffenen Artt. 230-1 ff. C.P.P. kann anlässlich eines Strafverfahrens jede Person gezwungen werden, Kryptoschlüssel bzw. Passwörter an die Ermittlungsbehörden herausgzugeben. Bei Zuwiderhandlung drohen drei Jahre Haft und 45.000 € Strafe. Hätte durch die Herausgabe ein Verbrechen verhindert werden können, steigt die maximale Strafdrohung auf fünf Jahre und 75.000 €.

4. Niederlande

Bereits 1998 war versucht worden, den Verdächtigen einer Straftat per Gesetz einer Entschlüsselungsanordnung zu unterwerfen. Wegen zahlreicher Proteste wurde der Vorschlag jedoch zurückgezogen[15]. Das niederländische Ministerium für Sicherheit und Justiz (Ministerie van Veiligheid en Justitie) hat Anfang Mai 2013 einen neuerlichen Gesetzentwurf vorgestellt. Darin ist geplant, dem Verdächtigen einen strafbewehrten „decryptiebevel" zu erteilen[16]. Der Vorstoß stützt sich dabei gezielt auf die Rechtslage in Frankreich und im Vereinigten Königreich[17]. Zwar sind sich die Verfasser des Entwurfs bewusst, welche Bedeutung der nemo-tenetur-Grundsatz auch im niederländischen Strafprozessrecht besitzt, gehen aber davon aus, dass es sich dabei keineswegs um ein absolutes Recht handelt[18].

Bert-Jaap Koops von der Universität Tilburg kommt in einem aktuellen Gutachten zu dem Schluss, dass ein Entschlüsselungsbefehl jedenfalls nicht vollkommen unvereinbar mit dem nemo-tenetur-Grundsatz sei[19]. Noch im Jahr 2000 gelangte *Koops* zum klar entgegengesetzten Ergebnis[20]. Die weitere Entwicklung in den Niederlanden gilt es zu beobachten.

5 10-cr-00509-REB-02 vom 23. Januar 2012. Fricosu hatte im Verfahren zugegeben, dass belastendes Material auf ihrem Computer enthalten war.

6 3:11-mc-00041-LAC vom 23. Februar 2012. Zusammenfassung der Entscheidung auch bei Lengyel, ZD-Aktuell 2012, 02832.

7 Betreffend Nutzerpasswörtern für Webdienste siehe etwa Morrison, Passwords, Arkansas Law Review 2012, 133 ff.

8 McGregor, Vanderbilt Journal of Entertainment and Technology Law 2010, 581, 608.

9 Siehe etwa Larkin, Vanderbilt Journal of Entertainment and Technology Law 2012, 253, 276 f. Larkin bestreitet indes bereits, dass die Passwortherausgabe Aussagecharakter besitzt, a.a.O, 270.

10 Online unter www.legislation.gov.uk/ukpga/2000/23/contents.

11 Auch Gercke sieht hierin einen eklatanten Verstoß gegen das nemo-tenetur-Prinzip, ders., MMR 2008, 291, 298.

12 No. [2008] EWCA Crim 2177 vom 9. Oktober 2008, www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html.

13 No. [2008] EWCA Crim 2177 vom 9. Oktober 2008, Rn. 20. Das Gericht bezog sich unmittelbar auf die Entscheidung des EGMR in der Sache Saunders v. United Kingdom vom 17. Dezember 1996, Case Number 43/1994/490/572. In der EGMR-Entscheidung wurde ein Verstoß gegen Art. 6 MRK bei Preisgabe von Gedankeninhalten aber gerade bejaht.

14 Online unter www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052.

15 Koops, Commanding Decryption and the Privilege Against Self-Incrimination, Nachdruck aus Breur/Kommer/Nijboer/Reijntjes (Hrsg.), New trends in criminal investigation and evidence, Bd. II, S. 431-445, Antwerpen/Groningen/Oxford 2000, nunmehr S. 2, online unter arno.uvt.nl/show.cgi?fid=5724.

16 Memorie van toelichting wetsvoorstel versterking aanpak computercriminaliteit, S. 52 ff., online unter www.rijksoverheid.nl/ministeries/venj/documenten-en-publicaties/kamerstukken/2013/05/02/memorie-van-toelichting-wetsvoorstel-versterking-aanpak-computercriminaliteit.html.

17 Memorie (Fn. 16), S. 55 f.

18 Memorie (Fn. 16), S. 57 mit Verweis auf mehrere strafprozessuale Normen, die den Verdächtigen von Mitwirkungspflichten ausnehmen.

19 Koops, Het decryptiebevel en het nemo-teneturbeginsel, 2012, S. 104 f., online unter www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/11/28/het-decryptiebevel-en-het-nemo-tenurbeginsel.html [sic!].

20 Koops, Commanding Decryption 2000 (Fn. 15), S. 12.

III. Rechtslage in Deutschland

1. Nemo tenetur se ipsum accusare

Die Freiheit, sich nicht selbst bezichtigen zu müssen, hat eine längere Geschichte[21]. Als tradierter Verfahrensgrundsatz kann nemo-tenetur heute auf ganz unterschiedliche Weise hergeleitet werden[22].

Einfachgesetzlich ergibt sich das Prinzip zunächst aus Art. 14 III lit. g) des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR)[23], der 1973 von Deutschland ratifiziert wurde und seitdem als Bundesrecht gilt. Außerdem gehört die Selbstbelastungsfreiheit nach allgemeiner Lesart sowie der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zum Kerngehalt des Rechts auf ein faires Verfahren nach Art. 6 I S. 1 MRK[24], welche bereits 1952 von Deutschland ratifiziert wurde. Ausformungen des nemo-tenetur-Prinzips finden sich sodann in mehreren strafprozessualen Vorschriften (§§ 55 I, 115 III, 163a III S. 2 und IV S. 2, 136 I S. 2, 243 IV S. 1 StPO). Aus dem der StPO zugrundeliegenden Akkusations- und Inquisitionsprinzip sowie der Unschuldsvermutung lässt sich ebenfalls ein Schweigerecht des Beschuldigten ableiten.

In verfassungsrechtlicher Hinsicht wird gleichsam eine Fülle von Ankerpunkten angeboten[25]. Die Rechtsprechung legt sich insoweit nicht fest[26].

Denkbar ist zunächst die Anknüpfung an den Schutz der Menschenwürde in Art. 1 I GG[27]. Die Menschenwürde ist stets dann betroffen, wenn der Mensch zum Objekt eines staatlichen Verfahrens herabgewürdigt wird[28]. Der Anwendungsbereich der Objektformel sollte bezüglich des nemo-tenetur-Satzes nicht zu vorschnell verneint werden[29]. Zwar verbürgt die Selbstbelastungsfreiheit gerade ein Recht zur Passivität, doch macht es einen gewichtigen Unterschied, ob das Objekt staatlichen Handelns gewissermaßen unverrückbar oder aber frei beweglich ist.

Art. 2 I GG verbürgt die freie Entfaltung der Persönlichkeit, die durch einen Aussagezwang beschnitten würde. Art. 2 II S. 2 GG schützt die Freiheit als solche, welche durch eine strafrechtliche Verurteilung entzogen werden kann. Das Allgemeine Persönlichkeitsrecht, die informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kommen als Kompositgrundrechte nach den Art. 1 I, 2 I GG in Betracht.

Art. 4 I Var. 2 GG schützt die Freiheit des Gewissens, also die freie Entscheidung für oder gegen ein Geständnis. Das in Art. 20 III GG niedergelegte Rechtsstaatsprinzip verpflichtet die staatlichen Organe zur Durchführung eines fairen Verfahrens. Die Gewährung rechtlichen Gehörs nach Art. 103 I GG führt dazu, dass der Angeklagte gehört werden muss, im Umkehrschluss aber auch schweigen darf[30].

Die unklare verfassungsrechtliche Herleitung deutet darauf hin, dass es sich beim nemo-tenetur-Grundsatz um eine notwendige Prämisse des Strafprozesses handelt. Entsprechende Anknüpfungspunkte durchziehen das gesamte Verfassungs- und Prozessrecht. Insofern ist nicht weniger, sondern mehr Grundrechtsschutz für den Betroffenen angezeigt[31].

Belastet sich ein Beschuldigter selbst, ohne zuvor gemäß § 136 I S. 2 StPO über sein Schweigerecht belehrt worden zu sein, greift ein Beweisverwertungsverbot. Auch ein Grundrechtsverstoß führt in aller Regel zu einem Verwertungsverbot. Nach dem sog. „Gemeinschuldner-Beschluss" des BVerfG ist eine Selbstbelastung zwar zulässig, aber strafrechtlich nicht verwertbar, wenn sich eine Aussagepflicht aus spezialgesetzlichen Vorschriften ergibt, die ihrerseits nicht zu einer strafrechtlichen Verurteilung beitragen sollen[32].

2. Entschlüsselungsbefehl de lege lata

In Deutschland verstößt der Entschlüsselungsbefehl nach allgemeiner Meinung gegen den nemo-tenetur-Grundsatz[33]. Dies gilt sowohl für die Herausgabe des Passworts als auch für die Lesbarmachung verschlüsselter Inhalte ohne Preisgabe des Passworts an die Behörden.

Weder Beschuldigte noch Zeugen (§ 55 I StPO) müssen sich nach hiesigem Recht durch eine Aussage selbst inkriminieren[34]. Nach der Rechtsprechung des BGH ist der Beschuldigte frei, „selbst darüber zu befinden, ob er an der Aufklärung des Sachverhalts aktiv mitwirken will oder nicht"[35]. Gemeint sind also nicht allein geständige Einlassungen, sondern jedes aktive Tun.

Verschriftlichte Passwortlisten (und soweit erforderlich auch die entsprechende Software[36]) unterliegen freilich der Beschlagnahme[37]. Zeugen, die nicht nach den §§ 52 ff.

21 Möller, JR 2005, 314, 315; Rüping, JR 1974, 135, 136 ff.

22 Grundlegend Bunzel, Erkenntnisgewinn aus konzelierten Daten, 2011, S. 153 ff.

23 Hierzu Gollwitzer, Menschenrechte im Strafverfahren. EMRK und IPBPR, 2005, S. 420 ff.

24 Gollwitzer, Menschenrechte 2005 (Fn. 22), S. 421 m.w.N.; Meyer-Ladewig, Europäische Menschenrechtskonvention, 3. Aufl., 2011, Art. 6 Rn. 131. Vgl. auch EGMR, Saunders v. United Kingdom vom 17. Dezember 1996, Case Number 43/1994/490/572.

25 Gollwitzer, Menschenrechte 2005 (Fn. 22), S. 421 f.; Möller, 314, 317 ff.; Verrel, NStZ 1997, 361, 364 f.

26 Siehe BVerfG NStZ 1995, 555 f.

27 So die wohl h.M., vgl. Gollwitzer, Menschenrechte 2005 (Fn. 22), S. 421; Verrel, NStZ 1997, 361, 364.

28 Grundlegend Dürig, AöR 81 (1956), 117, 127 f.

29 Anders Möller, JR 2005, 314, 317.

30 Möller, JR 2005, 314, 318.

31 Gegen die verfassungsrechtliche Überbetonung Verrel, NStZ 1997, 361, 364.

32 BVerfG NJW 1981, 1431, 1432 betreffend Auskunftspflichten nach der Konkursordnung.

33 Brodowski/Freiling, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 133; Bunzel, Erkenntnisgewinn aus konzelierten Daten, 2011, S. 410; Cornelius in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, 2. Aufl., 2006, Rn. 406; Eisenberg, Beweisrecht der StPO, 7. Aufl., 2011, Rnn. 2325 f.; Gerhards, (Grund-)Recht auf Verschlüsselung?, Baden-Baden 2010, S. 294 ff.; Nack in: Hannich (Hrsg.), Karlsruher Kommentar zur StPO, 6. Aufl., 2008, § 94 Rn. 4.

34 Zur „Belohnung" der Selbstanzeige im Steuerrecht siehe Kopf/Szalai, NJ 2010, 363 ff.

35 BGH NJW 1994, 1807, 1808.

36 LG Trier NStZ 2004, 223.

37 Nack, in: Karlsruher Kommentar (Fn. 33), § 94 Rn. 4; Park, Handbuch Durchsuchung und Beschlagnahme, 2. Aufl., 2009, Rn. 772.

StPO privilegiert sind, müssen ebenfalls bei der Entschlüsselung beschlagnahmter Datenträger mitwirken[38].

Nach § 113 I S. 2 TKG können darüber hinaus Telekommunikationsunternehmen verpflichtet werden, Zugangsdaten für Endgeräte und Online-Speicher ihrer Kunden offenzulegen[39]. Dies bezieht sich insbesondere auf PINs und PUKs für SIM-Karten. Während PIN-Codes seitens des Kunden frei änderbar sind, werden die PUKs fest voreingestellt. Sonstige Fälle der Passwortermittlung existieren im deutschen Strafverfahren nicht, die übrigen Mitwirkungspflichten – etwa bei ärztlichen Untersuchungen, Durchsuchungen oder Beschlagnahmen – sind damit nicht vergleichbar, da hierbei lediglich Duldungspflichten, nicht aber aktive Handlungspflichten bestehen.

3. Verwertbarkeit ausländischer Ermittlungsergebnisse und Vollstreckbarkeit ausländischer Urteile

Wird nun ein Beschuldigter im Ausland dazu gezwungen, sein Passwort zu offenbaren, stellt sich die Frage, inwieweit das gewonnene Beweismaterial in Deutschland in einen Prozess eingeführt werden darf. Eine klare Regelung zur Beweisverwertung bei Verletzung individueller Rechte fehlt[40]. Die etwaige Lösung auf Ebene der Beweiswürdigung oder aber der Strafzumessung wirkt in keiner Weise befriedigend[41]. Gerade wegen der gesteigerten Grundrechtsrelevanz (die Artt. 1 I und 4 I Var. 2 GG werden immerhin vorbehaltlos gewährleistet), bedarf es eines umfassenden Beweisverwertungsverbotes bei Verletzung des nemo-tenetur-Prinzips[42].

Das Verwertungsverbot bezieht sich dabei einerseits auf den Umstand, dass dem Beschuldigten das konkrete Passwort überhaupt bekannt war, andererseits freilich auf die verschlüsselten Inhalte. Eine Fernwirkung hinsichtlich weitergehender Ermittlungsergebnisse wird nach hiesiger Rechtsprechung eher selten angenommen. Sie dürfte aber jedenfalls dann anzunehmen sein, wenn es sich bei dem herausgegebenen Passwort gerade um den Hauptzugang zu einem Passwortmanagement-System handelt oder wenn ein und dasselbe Passwort mehrfach für unterschiedliche Zwecke verwendet wurde.

Gemäß der §§ 48 ff. IRG können ausländische Strafurteile im Inland vollstreckt werden. Nach § 49 I Nr. 2 IRG ist zuvor genau zu prüfen, ob im vorangegangenen Verfahren völkerrechtliche Mindeststandards wie diejenigen der MRK oder des IPbpR eingehalten wurden[43]. Ein Urteil, das unter Verstoß gegen den nemo-tenetur-Satz zustande gekommen ist, genügt diesen Anforderungen nicht. Ein dahingehendes Rechtshilfeersuchen wäre abzulehnen.

4. Aspekte eines etwaigen Gesetzgebungsverfahrens

Angesichts der Gesetzeslage im Vereinigten Königreich wurden bereits Befürchtungen geäußert, auch in Deutschland könnten eines Tages vergleichbare Regelungen eingeführt werden[44]. Verfassungsrechtliche Vorgaben hindern den nationalen Gesetzgeber allerdings, den Entschlüsselungsbefehl gesetzlich festzuschreiben[45].

Nicht nur, dass es für eine Einschränkung von Prozessgrundrechten einer genauen Prüfung der Verhältnismäßigkeit der Mittel bedarf[46]. Der zumindest flankierende Schutz durch die Menschenwürdegarantie lässt die Abwägung eindeutig zugunsten des Beschuldigten tendieren. Insbesondere die Herleitung des nemo-tenetur-Grundsatzes aus den Artt. 1 I und 20 III GG schützen vor übereilter Grundrechtsbeschneidung, da diese Vorschriften von der sog. Ewigkeitsgarantie des Art. 79 III GG erfasst sind. Der Entschlüsselungsbefehl ist daher mit dem deutschen Grundgesetz gänzlich inkompatibel.

IV. Fazit

Die Einführung eines Entschlüsselungsbefehls mag für die Ermittlungsbehörden reizvoll wirken, doch ist dies von Verfassungs wegen unzulässig. Der nemo-tenetur-Grundsatz ist charakteristisch und symptomatisch für unsere Justizgrundrechte. Etwaigen Bestrebungen, die Selbstbelastungsfreiheit zu beschränken, ist nicht nur in technischer Hinsicht (Stichwort: plausible deniability47) zu begegnen, sondern gerade auch auf juristischer Ebene die Stirn zu bieten. Im Ausland durch Verletzung von nemo tenetur gewonnene Beweismittel sind in Deutschland daher nicht vor Gericht verwendbar. Insgesamt ist der IT-Sicherheit im Land mehr gedient, wenn eine breite Akzeptanz von Verschlüsselungslösungen geschaffen wird, anstelle die bestehenden Möglichkeiten rechtlich zu beschneiden.

38 Eisenberg, StPO (Fn. 33), Rn. 2325; Nack in: Karlsruher Kommentar (Fn. 33), § 94 Rn. 4.

39 Seit der Entscheidung des BVerfG NJW 1012, 1419 f. bedarf es einer fachrechtlichen Ermächtigungsgrundlage für das Auskunftsersuchen.

40 Gless, JR 2008, 317, 325.

41 Zu den unterschiedlichen Lösungsansätzen Gless, JR 2008, 317, 324.

42 Ebenso Böse, ZStW 114 (2002), 148, 169 ff.; wohl auch Gless, JR 2008, 317, 326.

43 OLG Koblenz, Beschl. vom 30. November 2010, Az.: 1 Ws 541/10.

44 Vetter, England. Gefängnis für verschwiegenes Passwort, law blog vom 6. Oktober 2010, online unter www.lawblog.de/index.php/archives/2010/10/06/england-gefangnis-fur-verschwiegenes-passwort/.

45 So auch Gerhards, (Grund-)Recht auf Verschlüsselung?, Baden-Baden 2010, S. 299 ff.

46 Eingehend zur verfassungsrechtlichen Rechtfertigung Bunzel, Erkenntnisgewinn aus konzelierten Daten, 2011, S. 204 ff.

47 Siehe etwa www.truecrypt.org/docs/plausible-deniability.

Dr. iur. Lorenz Franck
Seit 2013 Rechtsassessor. Bis 2011 wissenschaftlicher Mitarbeiter an der Universität zu Köln, zugleich Forschungstätigkeit zum interdisziplinären Zusammenwirken von Juristen und Naturwissenschaftlern. Danach Rechtsreferendar beim Landgericht Köln. In dieser Funktion Stationen unter anderem bei der Staatsanwaltschaft Köln (Abteilung für Computer- und Internetkriminalität), dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Referat III, Arbeitnehmer- und Sozialdatenschutz) in Bonn sowie der Gesellschaft für Datenschutz und Datensicherheit e.V. in Bonn.