



Zertifikatsprogramm - Z402

# Computerstrafprozessrecht

- Cyberkriminalität und die Grundlagen des Strafprozessrechts
- Ermittlungsmaßnahmen I: Allgemeiner Teil
- Ermittlungsmaßnahmen II: Offene Ermittlungsmethoden
- Ermittlungsmaßnahmen III: Verdeckte Ermittlungsmethoden
- Beweisführung und Beweisverwertung – der Einsatz von Informationstechnik im Strafprozess

Dr. Christoph Burchard, LL.M (NYU)

Dominik Brodowski, LL.M (UPenn)

# Modul

## Computerstrafprozessrecht

---

Studienbrief 1: Cyberkriminalität und die Grundlagen  
des Strafprozessrechts

---

Autoren:

Dr. Christoph Burchard, LL.M (NYU)

Dominik Brodowski, LL.M (UPenn)

Prof. Dr. Joachim Vogel †

---

1. Auflage

© 2014 Bei Copyrightfragen wenden Sie sich bitte an Dr. Christoph Burchard,  
Lehrstuhl für Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht (ehedem  
Prof. Dr. Joachim Vogel)  
Ludwig-Maximilians-Universität München  
Professor-Huber-Platz 2  
80539 München

1. Auflage (1. August 2014)

Didaktische und redaktionelle Bearbeitung:

Der Studienbrief wurde redaktionell überarbeitet. Besonderer Dank gilt Alexander Castle für die Unterstützung bei der Überarbeitung des Manuskripts.

Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Verfasser unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

## Inhaltsverzeichnis

<b>Einleitung zu den Studienbriefen .....</b>	<b>5</b>
I.    Abkürzungen der Randsymbole und Farbcodierungen .....	5
II.   Zu den Autoren.....	6
III.  Modullehrziele.....	7
<b>Studienbrief 1 Cyberkriminalität und die Grundlagen des Strafprozessrechts .....</b>	<b>9</b>
1.1  Lernergebnisse .....	9
1.2  Advance Organizer.....	9
1.3  Aufgaben und Zwecke des Strafprozessrechts, Einordnung in das System der Strafrechtspflege.....	9
1.4  Abgrenzung zum Polizei- und Geheimdienstrecht.....	10
1.5  Rechtsquellen, Auslegung von Computerstrafprozessrecht.....	10
1.6  Akteure .....	11
1.6.1  Gerichte .....	11
1.6.2  Strafverfolgungsbehörden .....	12
1.6.3  Der Beschuldigte und sein Verteidiger .....	13
1.6.4  Opfer.....	14
1.6.5  Zeugen und Sachverständige .....	14
1.6.6  Private Dritte .....	15
1.7  Voraussetzungen eines Strafprozesses .....	16
1.8  Ablauf.....	17
1.8.1  Ermittlungsverfahren.....	17
1.8.2  Zwischenverfahren.....	19
1.8.3  Hauptverfahren .....	20
1.8.4  Rechtsmittelverfahren .....	21
1.8.5  Rechtskraft und Strafvollstreckung.....	21
1.8.6  Sonderformen.....	21
1.9  Prinzipien .....	22
1.9.1  Wahrheitsfindung .....	23
1.9.2  Unschuldsvermutung.....	23
1.9.3  In dubio pro reo .....	23
1.9.4  Prinzipien bezüglich der Anklageerhebung.....	24
1.9.5  Öffentlichkeit.....	24
1.9.6  Verzögerungsverbot, Beschleunigungsgebot.....	24
1.9.7  Verhältnismäßigkeitsprinzip .....	24
1.9.8  Grundsatz des fairen Verfahrens („fair trial“), Waffengleichheit .....	24
1.10 Zusammenfassung.....	25
1.11 Übungen .....	26
<b>Verzeichnisse .....</b>	<b>27</b>
I.    Kontrollaufgaben.....	27

II. Literatur.....27

## Einleitung zu den Studienbriefen

### I. Abkürzungen der Randsymbole und Farbcodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Merksatz	M
Quelltext	Q
Übung	Ü

## II. Zu den Autoren



Dominik Brodowski studierte – nach einem Abstecher zur Luft- und Raumfahrttechnik an der Technischen Universität München – Jura an der Juristischen Fakultät der Eberhard-Karls-Universität Tübingen und an der University of Pennsylvania Law School. Neben seinem Dissertationsprojekt – den Grenzbereich zwischen Polizei- und Strafprozessrecht betreffend – begleitet er derzeit als Wissenschaftlicher Angestellter an der Juristischen Fakultät der Ludwig-Maximilians-Universität München schwerpunktmäßig aktuelle europäische Strafrechtsetzungsprozesse sowie den Kernbereich des Straf- und Strafprozessrechts, einschließlich seiner verfassungsrechtlichen und internationalen Überformungen. In seiner Freizeit ist Dominik Brodowski u. a. an der Weiterentwicklung des Betriebssystem-Kernels von Linux™ beteiligt und hat dabei etwa die Unterstützung von Stromspartechniken maßgeblich verbessert.



Prof. Dr. Joachim Vogel (RiOLG) † studierte Rechtswissenschaft in Freiburg und promovierte 1992 zum Dr. jur. durch die Rechtswissenschaftliche Fakultät der Universität Freiburg, 1999 wurde ihm die *venia legendi* durch die Rechtswissenschaftliche Fakultät der Universität Freiburg für Strafrecht, Strafprozessrecht, Rechtsvergleichung und Rechtslehre erteilt. Von 1988-1990 und 1994-1999 war er wissenschaftlicher Angestellter und Assistent bei Prof. Dr. Dr. h. c. mult. Klaus Tiedemann in Freiburg, 1999-2000 folgte die Professur für Strafrecht und Rechtsphilosophie sowie Rechtsinformatik an der Universität München, 2000-2012 war Vogel Professor für Strafrecht und Strafprozessrecht an der Universität Tübingen, 2012 bis zu seinem Tod im Sommer 2013 an der Ludwig-Maximilians-Universität München. 2001 wurde er zum Richter im zweiten Hauptamt am Oberlandesgericht Stuttgart berufen, seit 2012 war er im zweiten Hauptamt am Oberlandesgericht München tätig. Außerdem war er seit 2003 Mitherausgeber der JuristenZeitung (JZ). Von 2005-2009 war er Dekan der Juristischen Fakultät der Universität Tübingen. Vogel engagierte sich daneben als Mitglied und Sekretär der Deutschen Landesgruppe der Association internationale de Droit Pénal und war Mitglied der Gesellschaft für Rechtsvergleichung e.V.



Dr. Christoph Burchard, LL.M (NYU), Jahrgang 1976, nahm 1996 sein Studium der Rechtswissenschaften an der Universität Passau auf und legte 2001 das Erste Juristische Staatsexamen ab. Von 2002 bis 2003 absolvierte er ein LL.M-Studium an der New York University School of Law mit den Schwerpunkten Völkerrecht sowie amerikanisches Straf- und Strafprozessrecht. Gleichzeitig durchlief er den juristischen Vorbereitungsdienst am Landgericht Freiburg, wo er 2006 die Zweite Juristische Staatsprüfung ablegte. Im August 2007 wurde er an der Universität Passau mit einer grundlagendogmatischen Arbeit zu Vorsatz und Tatbestandsirrtum promoviert. Im April 2012 folgte der Wechsel an die LMU München als Akad. Rat a. Z. am Lehrstuhl von Prof. Dr. Joachim Vogel, RiOLG. Im Rahmen des Verbundprojekts Open C<sup>3</sup>S lehrt Herr Burchard in verschiedenen juristischen Modulen, darunter im Computerstraf- und Computerstrafprozessrecht.

### III. Modullehrziele

In diesem Modul lernen Sie nun die strafprozessrechtlichen Grundzüge der deutschen Rechtsordnung kennen. Das Modul „Computerstrafprozessrecht“ ergänzt dabei das Modul „Computerstrafrecht“, in dem man die materiellstrafrechtlichen Grundlagen der Verfolgung von Kriminalität mit IT-Bezug erlernt.

Was wird Ihnen vermittelt?

Mit diesem Modul sollen folgende Lehrziele erreicht werden:

- Sie entwickeln ein Verständnis für die Relevanz der Grundrechte und des Prinzips der Verhältnismäßigkeit für das Strafprozessrecht.
- Sie verstehen den Ablauf eines Strafverfahrens und dabei die jeweilige Bedeutung des Ermittlungs- und des Hauptverfahrens.
- Sie können mit computerstrafrechtlich relevanten Ermittlungsbefugnissen umgehen und erkennen die Grenzen rechtsstaatlichen Handelns.
- Sie wissen, wie „IT-Beweismittel“ im Prozess, insbesondere im gerichtlichen Hauptverfahren, verwendet und verwertet werden sowie „IT“ im Strafprozess zum Einsatz kommt bzw. kommen kann.

Mit diesen Kenntnissen und Fähigkeiten sollen Sie die rechtlichen Rahmenbedingungen für computerforensische Analysen beurteilen können. Sie verstehen die Relevanz und Brisanz strafprozessualer Ermittlungsbefugnisse.

Was können Sie nach erfolgreichem Abschluss des Moduls?

### Hinweise

Die Studienbriefe zu diesem Modul befinden sich auf dem Stand 1.5.2014. Später erschienene Literatur und Rechtsprechung konnten nur in Ausnahmefällen berücksichtigt werden.

Stand des Skripts

Geringe Teile dieser Studienbriefe entsprechen – z. T. auch ohne ausdrücklichen Hinweis – der von mir gemeinsam mit Herrn Professor Felix C. Freiling verfassten Studie „Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft“. Der Studienbrief 1 basiert in Teilen auf Vorlesungsunterlagen von Herrn Professor Joachim Vogel. Diese Studienbriefe beruhen überdies auf den Erfahrungen im Studiengang „Digitale Forensik“, deren Skripte hier weiterentwickelt und angepasst wurden.

Quellenhinweis

Eine juristische Betrachtung der Cyberkriminalität erfordert stets einen Blick in das Gesetz. Es ist daher unverzichtbar, sich die in den Studienbriefen zitierten Normen sogleich auch im Wortlaut zu vergegenwärtigen. Die wichtigsten bundesgesetzlichen Regelungen finden Sie im Anhang sowie unter <http://www.gesetze-im-internet.de/>, die wichtigsten strafrechtlichen Normen der Europäischen Union unter <http://db.eurocrim.org/>.

Gesetzestexte und Lehrbücher

Auch wenn die in diesen Studienbriefen vermittelten Inhalte völlig ausreichend für die Prüfungsvorbereitung sind, sei bereits an dieser Stelle auf die vier auf dem Markt erhältlichen Lehrbücher zum Computer- bzw. Internetstrafprozessrecht verwiesen:

- Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009.
- Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Auflage, 2012.
- Malek, Strafsachen im Internet, 2. Auflage, 2014.
- Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Auflage, 2010.



Die für den jeweiligen Studienbrief maßgeblichen Abschnitte aus diesen Lehrbüchern sind jeweils zu Beginn des Studienbriefs angegeben; ferner finden Sie dort weitere Literaturangaben zur Vertiefung, sollten Sie noch tiefer in die Materie einsteigen wollen. Für den Studienbrief 1 sind dies:

**Lehrbücher zum Strafprozessrecht (Auswahl):** Beulke; Kindhäuser; Roxin/Schünemann; Volk.

**Kommentare (Auswahl):** Meyer-Goßner, KK-StPO, Löwe-Rosenberg.

## Studienbrief 1 Cyberkriminalität und die Grundlagen des Strafprozessrechts

### 1.1 Lernergebnisse

Dieser Studienbrief enthält einen kursorischen Überblick über den Ablauf des Strafverfahrens, die daran beteiligten Akteure und die das Strafprozessrecht dominierenden Prinzipien. Auf diese hier vermittelte Grundstruktur bauen die nachfolgenden Studienbriefe auf; auch Studierende, die bereits mit dem Strafprozessrecht und seinen Grundzügen vertraut sind, sollten diesen Studienbrief als Chance zur Wiederholung nützen. Das Skript eignet sich jedoch insbesondere für Studierende ohne Vorkenntnisse, um sich einen Eindruck vom Strafprozessrecht im Allgemeinen zu machen. Ohne Wissen der Grundlagen ist nämlich ein Studium des Computerstrafprozessrechts im Besonderen nicht möglich.

### 1.2 Advance Organizer

Krimi-, Polizei- und Gerichtssendungen verzerren die Realität des deutschen Strafverfahrens teils gravierend. Versuchen Sie daher, sich dem Strafprozessrecht im Allgemeinen und dem Computerstrafprozessrecht im Besonderen mit einem „frischen“ Blick zu nähern, d. h. lassen Sie sich nicht von medial geprägten oder sonstigen Vorverständnissen leiten.

### 1.3 Aufgaben und Zwecke des Strafprozessrechts, Einordnung in das System der Strafrechtspflege

Das Strafprozessrecht dient der Durchsetzung des Strafrechts, indem es ein Verfahren zur Verfügung stellt, mit dem der Staat auf eine ihm bekannt gewordene mutmaßliche Verletzung eines Strafgesetzes reagieren kann, die dann in einer Sanktionierung münden kann. Gleichzeitig dient das Strafprozessrecht auch der Wahrung der Freiheitsrechte der Bürger: Diese darf der Staat nur nach diesem geordneten Verfahren bestrafen. Als Mittel zur Durchsetzung der schärfsten Eingriffe des Staates in Rechtspositionen seiner Bürger – und auch indirekt als Methode zur Beeinflussung oder Verängstigung der Bürger – wird es zutreffenderweise auch als „Seismograph der Staatsverfassung“ bezeichnet.<sup>1</sup>

Die Aufgaben des Strafprozessrechts können folgendermaßen beschrieben werden<sup>2</sup>:

- **Ermittlung der Wahrheit:** Zu Unrecht darf niemand bestraft werden. Im Strafverfahren soll die Feststellung des Sachverhaltes erfolgen, wie er sich tatsächlich abgespielt hat. Auf dieser Grundlage muss dann eine materiell-rechtlich richtige Entscheidung getroffen werden.

---

<sup>1</sup> So Roxin/Schünemann, § 2 Rdnr. 1.

<sup>2</sup> So Engländer, Strafprozessrecht, § 1 Rdnr. 1.

## Studienbrief 2 Ermittlungsmaßnahmen I: Allgemeiner Teil

Zur Vertiefung sei für diesen Studienbrief insbesondere auf folgende Literatur verwiesen:

Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren; Marbereth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl., Rdnr. 390 ff.; Valerius, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internets sowie die Lehrbücher und Kommentare zur StPO (Studienbrief 1).

### 2.1 Lernergebnisse

Wesentliche Voraussetzung für die Verurteilung eines Straftäters ist es, den Täter zu ermitteln und ihm die Tat nachzuweisen. Die hierfür notwendigen Weichenstellungen werden in aller Regel im Ermittlungsverfahren gestellt, dessen Grundzüge Sie bereits kennengelernt haben. Für Ermittlungen in Computerstrafsachen stehen den Strafverfolgungsbehörden eine Vielzahl an Ermittlungsmaßnahmen zur Verfügung. Deren Systematik und gemeinsame Grundfragen werden in diesem Studienbrief beleuchtet.

### 2.2 Advance Organizer

Denken Sie – auch wenn Sie anderes andernorts gelernt haben sollten – die Ermittlung von sachdienlichen Informationen (Beweismitteln) vom Betroffenen einer Ermittlungsmaßnahme her. Nehmen Sie diese Perspektive ein, haben Sie einen rechtsstaatlichen Orientierungspunkt, anhand dessen Sie ergründen können, ob und wenn ja welche Ermittlungsmaßnahme mit welchen Voraussetzungen und Beschränkungen zulässig ist. Denn nur wenn die Ermittlungsmaßnahme rechtmäßig war, können Sie in der Regel (von wenigen Ausnahmen abgesehen) sicher sein, dass die gewonnene Information bzw. das erhobene Beweismittel auch „gerichtsfest“ ist, d. h. gegen einen Beschuldigten verwendet und verwertet werden darf.

### 2.3 Systematik der Ermittlungsmaßnahmen

Bislang konnte sich keine einheitliche Systematisierung der Ermittlungsmaßnahmen durchsetzen. Folgende unterschiedliche Charakterisierungen lassen sich aber heranziehen, auch um die Intensität, den Beweiswert und die verfassungsrechtlichen Implikationen der einzelnen Ermittlungsmaßnahmen besser vergleichen zu können:

Keine einheitliche Systematik

Erstens lassen sich Ermittlungsmaßnahmen danach unterscheiden, ob sie eine aktive Mitwirkung oder eine passive Duldung verlangen.<sup>1</sup> Beispiele für eine aktive Mitwirkung sind etwa die Befragung von Zeugen oder die Pflicht zur Herausgabe von beweiserheblichen Gegenständen (§ 95 StPO); für passive Duldung die Duldung einer Blutentnahme, einer Durchsuchung und einer Beschlagnahme. Relevant wird diese

Aktive Mitwirkung oder passive Duldung?

---

<sup>1</sup> So Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, Rdnr. 7.

## Studienbrief 3 Ermittlungsmaßnahmen I: Allgemeiner Teil

Zur Vertiefung sei für diesen Studienbrief insbesondere auf folgende Literatur verwiesen:

Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren; Marbereth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl., Rdnr. 390 ff.; Valerius, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internets sowie die Lehrbücher und Kommentare zur StPO (Studienbrief 1).

### 3.1 Lernergebnisse

Für Ermittlungen in Computerstrafsachen stehen den Strafverfolgungsbehörden eine Vielzahl von Ermittlungsmethoden zur Verfügung. Deren Systematik und deren gemeinsame Grundfragen werden in diesem Studienbrief ebenso beleuchtet wie typischerweise „offene“, d. h. vom Beschuldigten erkennbare Ermittlungsmaßnahmen (Befragung, Durchsuchung und Beschlagnahme, Fahndung). Ergänzt wird dies durch eine Darstellung der Mitwirkungspflichten des Beschuldigten und (unverdächtiger) Dritter.

### 3.2 Advance Organizer

Wesentliche Voraussetzung für die Verurteilung eines Straftäters ist es, den Täter zu ermitteln und ihm die Tat nachzuweisen. Die hierfür notwendigen Weichenstellungen werden in aller Regel im Ermittlungsverfahren gestellt, dessen Grundzüge Sie bereits kennengelernt haben. Nun gilt es, Ihre Kenntnisse bezüglich „offener“ Ermittlungsmethoden zu vertiefen, bevor Sie im nächsten Studienbrief mehr über „verdeckte“ Ermittlungsmethoden lernen werden.

### 3.3 Befragung; Zeugen- und Beschuldigtenvernehmung

Das wohl klassischste Erkenntnismittel auch im Ermittlungsverfahren ist die Befragung von Personen: Sei es die informelle, informatorische Befragung, sei es die förmliche Vernehmung eines Zeugen oder eines Beschuldigten. Zwar sind die Fähigkeiten (und zum Teil auch der Wille) zu einer wahren und vollständigen Wiedergabe des tatsächlichen Geschehens begrenzt, insbesondere auch in Konstellationen, bei denen es auf technischen Sachverstand ankommt. Dennoch liefern die Informationen von Opfern, von Zeugen und zuweilen auch die Geständnisse und sonstigen Einlassungen von Beschuldigten zumeist wesentliche Ansätze für weitere, vertiefte Ermittlungen.

Bedeutung

Ein Zeuge kann (nur) über sinnlich wahrgenommene Tatsachen aussagen<sup>1</sup> oder sich (im Ermittlungsverfahren) schriftlich hierzu äußern. Auf welchem Wege diese Wahrnehmung erfolgte (optisch, akustisch, olfaktorisch und haptisch), ist irrelevant.

Gegenstand des Zeugenbeweises

---

<sup>1</sup> Meyer-Goßner Vor § 48 Rdnr. 1 ff.

## Studienbrief 4 Ermittlungsmaßnahmen III: Verdeckte Ermittlungsmethoden

Zur Vertiefung sei für diesen Studienbrief insbesondere auf folgende Literatur verwiesen:

Lehrbücher: Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren; Marbreth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl., Rdnr. 390 ff.

Die Lehrbücher und Kommentare zur StPO (Studienbrief 1) sowie ferner folgende Literatur: Brodowski, JR 2009, 402; Becker/Meinicke, StV 2011, S. 50.

### 4.1 Lernergebnisse

Verdeckte, heimliche Ermittlungen in einem Strafverfahren bedeuten stets einen besonders einschneidenden Eingriff in die Grundrechte. Daher sind diesbezüglich etliche, spezielle Eingriffsgrundlagen erforderlich, die in diesem Studienbrief kursorisch vorgestellt werden. Besonderes Augenmerk wird dabei auf Konstellationen wie E-Mail-Kommunikation gelegt, bei denen sich die hergebrachten Eingriffsgrundlagen nicht ohne Weiteres auf die Herausforderungen der IT-Technologie übertragen lassen.

### 4.2 Advance Organizer

Im vergangenen Studienbrief haben Sie die verfassungsrechtlichen Implikationen und Grundfragen der Ermittlungsmaßnahmen im Strafverfahren kennengelernt. Dies gilt es nunmehr auf die heimlichen Ermittlungsmaßnahmen im Strafverfahren anzuwenden – und dabei neben der Telekommunikationsüberwachung insbesondere auch Fragen rund um die „Online-Durchsuchung informationstechnischer Systeme“ zu beleuchten.

### 4.3 Inhaltliche Überwachung der Kommunikation

Kontrollaufgabe 4.1

Was sind Bestands-, Inhalts- und Verkehrsdaten?

K

Die Überwachung der Telekommunikation ist nicht nur archetypisch für verdeckte Ermittlungen im Strafverfahren, sondern auch von zentraler Bedeutung für die Strafverfolgung von Computerstraftaten. Dabei sind grundsätzlich drei verschiedene Konstellationen zu unterscheiden:

Zentrale Bedeutung der Bestands-, Verkehrs- und Inhaltsdaten

- Eine Überwachung des Inhalts der Telekommunikation (Inhaltsdaten) – diese richtet sich vorrangig nach § 100a StPO unter Umständen aber auch nach anderen Eingriffsbefugnissen,
- eine Abfrage, wer zu einem bestimmten Zeitpunkt einen bestimmten Telekommunikationsanschluss verwendete (Bestandsdatenabfrage, sowie schließlich

## **Studienbrief 5 Beweisführung und Beweisverwertung – der Einsatz von Informationstechnik im Strafprozess**

Zur Vertiefung sei für diesen Studienbrief insbesondere auf folgende Literatur verwiesen:

Beweisführung im Strafverfahren: Vgl. die Lehrbücher und Kommentare zur StPO (Studienbrief 1) sowie Frieling/Ulrich/Jessnitzer, Der gerichtliche Sachverständige, 12. Aufl. 2007.

Beweiswert elektronischer Informationen: Bohatiuk CR 1989, 535: „Beweiswert gespeicherter Informationen“; Bäcker/Freiling/Schmitt, DuD 2010, 80; Grimm/Pähler DuD 2010, 86.

Verantwortlichkeit von Ermittlungsakteuren: Schroeder, GA 1993, 389; Amelung, JuS 1986, 329.

### **5.1 Lernergebnisse**

Die Verurteilung des Angeklagten in einer Hauptverhandlung verläuft nach einem förmlichen Verfahren, in dem der Tatnachweis mit bestimmten, verwertbaren Beweismitteln zu führen ist. In diesem Studienbrief werden diese Beweismittel, die in der Hauptverhandlung zur Verfügung stehen, näher beleuchtet (SB 4 4.3). Zudem werden die Risiken für Ermittlungsbeamte und Sachverständige aus strafrechtlicher, aber auch aus dienst- und zivilrechtlicher Sicht betrachtet (4.4).

### **5.2 Advance Organizer**

In den Studienbriefen zu den Ermittlungsmaßnahmen haben Sie sich bereits mit der Vernehmung des Beschuldigten, von Zeugen und der Einbindung von Sachverständigen vertraut gemacht. Die im Ermittlungsverfahren erlangten Erkenntnisse gilt es nunmehr aber auch in der Hauptverhandlung umzusetzen, um einen Tatnachweis zu führen oder zu entkräften. Zudem haben Sie im Modul „Cyberkriminalität und Computerstrafrecht“ einige Tatbestände kennengelernt, die einem digitalen Forensiker tagtäglich begegnen: So ist geradezu Kern seiner Aufgabe, geschützte Daten auszuspähen (§ 202a Abs. 1 StGB). Warum sich ein digitaler Forensiker dennoch in den seltensten Fällen strafbar macht, erfahren Sie im zweiten Teil dieses Studienbriefs.

## 5.6 Übungen

### Übung 5.1

Im Rahmen einer ordnungsgemäß angeordneten und durchgeführten „Online-Durchsuchung“ finden die Terrorfahnder des BKAs auf dem PC des A zwar keine Anhaltspunkte dafür, dass A in terroristische Machenschaften verstrickt ist, dafür aber zehn Bilddateien mit kinderpornographischem Inhalt. Hierüber informieren sie die örtlich zuständige Staatsanwaltschaft. Diese lässt nach richterlichem Beschluss den Rechner des A beschlagnahmen und auswerten, wobei diese Bilddateien (erneut) aufgefunden werden. Können diese Erkenntnisse durch Befragung der ermittelnden Polizeibeamten in das Hauptverfahren eingeführt werden? Kann sich die Verurteilung des A wegen des Besitzes kinderpornographischer Schriften allein darauf stützen?

Ü

### Übung 5.2

Variante 1) Polizist P wertet das Verhalten des A irrtümlich als des internationalen Betäubungsmittelschmuggels höchst verdächtig und hält A zudem irrtümlich für höchst gefährlich, wobei er die erheblichen Bedenken seiner Kollegen Q, R, S und T geflissentlich ignoriert. Er ordnet wegen Gefahr im Verzug die Durchsuchung der Wohnung des A an, Zeugen zieht er nicht hinzu, weil er hierfür keinen zeitlichen Spielraum sieht. Bei der Durchsuchung der Wohnung des A werden nur entlastende Spuren entdeckt, allerdings auch eine „Raubkopie“ eines Computerspiels. Der Rechteinhaber und A stellen form- und fristgemäß Strafantrag.

Variante 2) Gegen A besteht Tatverdacht, dass er eine „Raubkopie“ eines Computerspiels angefertigt hat. Aufgrund eines richterlichen Durchsuchungsbeschlusses wird die Wohnung des A durch den Polizisten P durchsucht, auf die Hinzuziehung von Zeugen verzichtet P, weil die Gemeinde keinen Mitarbeiter zur Verfügung stellen möchte. A widerspricht der Durchsuchung und verzichtet nicht auf die Hinzuziehung von Zeugen; dies übergeht P unter Hinweis darauf, dass die Hinzuziehung von Zeugen nicht unbedingt notwendig sei. Bei der Durchsuchung der Wohnung des A wird die „Raubkopie“ eines Computerspiels entdeckt. Der Rechteinhaber und A stellen form- und fristgemäß Strafantrag.

*Frage 1: Ist die aufgefundene „Raubkopie“ sowie die sich hierauf stützende Zeu-  
genaussage des P im Strafverfahren gegen A verwertbar?*

*Frage 2: Hat sich P wegen Hausfriedensbruchs (§ 123 StGB) strafbar gemacht?*

Ü

## Verzeichnisse

### I. Kontrollaufgaben

Kontrollaufgabe 5.1.....	7
Kontrollaufgabe 5.2.....	10
Kontrollaufgabe 5.3.....	11
Kontrollaufgabe 5.4.....	14

### II. Literatur

Bäcker, Matthias/Freiling, Felix C./Schmitt, Sven, Selektion vor der Sicherung, Datenschutz und Datenrecht, S. 80 ff.

Baur, Max P./Fimmers, Rolf/Schneider, Peter M., Zur Beweiswürdigung von DNA-Analysen, Anmerkung zur Entscheidung des BGH vom 21.01.2009, Strafverteidiger 2010, S. 175 ff.

Beulke, Werner, Strafprozessrecht, 12. Aufl., Heidelberg 2012.

Bohاتیuk, Erwin, Beweiswert gespeicherter Information, Computer und Recht 1989, S. 535 ff.

Brodowski, Dominik, BVerfG, Beschl. v. 17. 2. 2009 – 2 BvR 1372/07 und 2 BvR 1745/07 – Automatischer Suchlauf bei Kreditinstituten zur Feststellung bestimmter Überweisungen („Mikado“). Juristische Rundschau 2010, S. 546 ff.

Fischer, Thomas, Strafgesetzbuch, Kommentar, 61. Aufl., München 2014.

Hannich, Rolf, Karlsruher Kommentar zur StPO, 7. Aufl., München 2013. (zitiert: Karlsruher Kommentar zur StPO).

Grimm, Rüdiger/Pähler, Daniel, E-Mail-Forensik, Datenschutz und Datenrecht-Schwerpunktheft "IT-Forensik", Nr. 2. S. 86 ff.

Krehl, Christoph, Die Erkundigungspflicht des Zeugen bei fehlender oder beeinträchtigter Erinnerung und mögliche Folgen ihrer Verletzung, Neue Zeitschrift für Strafrecht 1991, S. 416 ff.

Meyer-Goßner, Lutz/Schmitt Bertram, Strafprozessordnung, Kommentar, 57 Aufl., München 2014.

Thomas, Petri B., Auskunftsverlangen nach § 161 StPO gegenüber Privaten – eine verdeckte Rasterfahndung?, Strafverteidiger 2007, S. 266 ff.

Sponeck, Henning von, Beweiswert von Computerausdrucken, Computer und Recht 1991, S. 269 ff.

Wendler, Axel/Hoffmann, Helmut, Technik und Taktik der Befragung , Prüfung von Angaben, 2. Aufl., Stuttgart 2014.



## Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodulare im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von beruflicher und hochschulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits- und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

## Open Competence Center for Cyber Security

Open C<sup>3</sup>S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufs begleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

# Z402 Computerstrafprozessrecht

In diesem Modul lernen Sie nun die strafprozessrechtlichen Grundzüge der deutschen Rechtsordnung kennen. Das Modul „Computerstrafprozessrecht“ ergänzt dabei das Modul „Computerstrafrecht“, in dem man die materiellstrafrechtlichen Grundlagen der Verfolgung von Kriminalität mit IT-Bezug erlernt.

Das Modul befasst sich in mehreren Studienbriefen mit den Auswirkungen der Informationstechnologie auf das Strafprozessrecht. Unter Bezugnahme auf die im Modul Computerstrafrecht erworbenen materiellrechtlichen Grundkenntnisse werden im Modul grundlegende Kenntnisse im Bereich des Verfahrensrechts und des formellen Strafrechts vermittelt.

Auch in diesem Modul wird regelmäßig Bezug auf einschlägige Rechtsprechung genommen und Wert auf eine fallbezogene Wissensvermittlung gelegt. Angesichts der besonderen Bedeutung des Strafverfahrensrechts werden aber auch Grundzüge verfassungsrechtlicher Fragestellungen behandelt.

Die Studierenden erwerben Grundkenntnisse des Strafprozessrechts. Sie können die Grundzüge des Computerstrafprozessrechts in Bezug zur Informationstechnologie und zum Verfassungsrecht setzen. Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage, verfahrensrechtliche Maßnahmen auf ihre Zulässigkeit zu überprüfen und hierzu kritisch Stellung zu nehmen. Dabei erwerben Sie sowohl Fach- als auch eine grundlegende Methodenkompetenz.

## Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten können sie auf ein Studium angerechnet werden.

<https://zertifikatsprogramm.de>