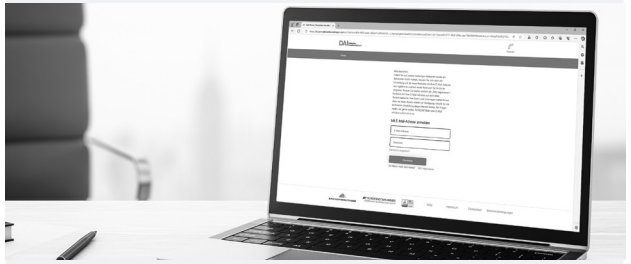
Online-Vortrag LIVE: Aktuelle Entwicklungen im Internetstrafrecht

Live-Übertragung:	5. März 2026, 13.30 – 19.00 Uhr (inkl. 30 Min. Pause)
Zeitstunden:	5,0 – mit Bescheinigung nach §15 Abs. 2 FAO
Kostenbeitrag:	**ab 265,– €** (USt.-befreit) für Mitglieder der kooperierenden Rechtsanwaltskammern **305,– €** (USt.-befreit) regulär
Nr.:	22257297

Anmeldung über die DAI-Webseite
www.anwaltsinstitut.de
mit vielen neuen Services:



- Zugriff auf alle digitalen Unterlagen zur Fortbildung: Von Arbeitsunterlage bis zur Teilnahmebescheinigung
- Komfortable Umbuchungsmöglichkeiten
- Direkter Zugriff auf alle digitalen Lernangebote
- Speichern interessanter Fortbildungen auf Ihrer persönlichen Merkliste

Die DAI Online-Vorträge LIVE

Bei einem Online-Vortrag LIVE verfolgen Sie die Veranstaltung/Fortbildung zum angegebenen Termin über das eLearning Center. Ein moderierter textbasierter Chat ermöglicht Ihnen die Interaktion mit den Referierenden und anderen Teilnehmenden. Sie benötigen nur einen aktuellen Browser, eine stabile Internetverbindung und Lautsprecher. Die Arbeitsunterlage steht elektronisch zur Verfügung.

Teilnahmebescheinigung nach §15 Abs. 2 FAO

Das DAI stellt die Voraussetzungen zum Nachweis der durchgängigen Teilnahme sowie die Möglichkeit der Interaktion während der Dauer der Fortbildung bereit. Die Online-Vorträge LIVE werden damit wie Präsenzveranstaltungen anerkannt und können für die gesamten 15 Zeitstunden genutzt werden.

Kontakt

Deutsches Anwaltsinstitut e. V.
Gerard-Mortier-Platz 3, 44793 Bochum
Tel. 0234 970640
support@anwaltsinstitut.de
Vereinsregister des Amtsgerichts Bochum: VR-Nr. 961

FAOcomplete – Ihr eLearning-Paket im DAI

Dieses eLearning-Angebot ist Bestandteil von FAOcomplete: Mit diesem eLearning-Paket können Sie sich aus unserem vielfältigen Angebot Ihre komplette FAO-Fortbildung in einem Fachinstitut komfortabel, flexibel und zu einem attraktiven Festpreis zusammenstellen. **Genauere Informationen finden Sie unter www.anwaltsinstitut.de/faocomplete**

DAI-Newsletter – Jetzt anmelden

Einfach QR-Code scannen oder unter www.anwaltsinstitut.de/dainewsletter/

DAI Deutsches Anwaltsinstitut e.V.

Fachinstitute für Informationstechnologierecht/ Strafrecht

Online-Vortrag LIVE

Aktuelle Entwicklungen im Internetstrafrecht

5. März 2026
13.30 – 19.00 Uhr
Online

Martin Reiter
Staatsanwalt

FAO complete Fachinstitut Informationstechnologierecht

FAO complete Fachinstitut Strafrecht

www.anwaltsinstitut.de

Gemeinnützige Einrichtung der Bundesrechtsanwaltskammer, Bundesnotarkammer, Rechtsanwaltskammern und Notarkammern.

Referent

Martin Reiter, Staatsanwalt

Inhalt

Der Vortrag beschäftigt sich mit den rechtlichen Grundlagen der Verfolgung von Kriminalität im Internet und deren praktischer Umsetzung. Hierbei wird insbesondere Wert darauf gelegt, die in der Praxis regelmäßig auftretenden Fallsituationen anschaulich zu vermitteln.

Der Vortrag richtet sich an alle, die gelegentlich oder regelmäßig mit Sachverhalten mit Internetbezug beschäftigt sind. Besondere technische oder juristische Vorkenntnisse werden nicht vorausgesetzt. Nach einer gehaltvollen Einleitung, in der die aktuellen Phänomene der Cybercrime vorgestellt werden, gliedert sich der Vortrag in drei Teile:

I. Die Zuständigkeit der deutschen Justiz und sonstige allgemeine Bestimmungen

In einer kurzen Einführung werden die wesentlichen Bestimmungen zur Zuständigkeit im Allgemeinen und bei Internetstraftaten im Besonderen sowie die Verantwortlichkeit der am Internet Beteiligten dargestellt. Anhand von praktischen Beispielen wird erläutert, warum das Internet die Verfolgung vieler Straftaten erheblich erschwert und warum es hierbei im Juristischen so oft zu Fehlern kommt.

II. Ermittlungsablauf

Vom Eingang der Anzeige bis zum Abschluss des Strafverfahrens werden typische Sach- und Prozessrechtsprobleme vorgestellt. Es geht etwa um die rechtliche Zulässigkeit von offenen und verdeckten polizeilichen Ermittlungen im Internet (OSINT), insbesondere im Darknet, der Erlangung von Bestands-, Verkehrs-, Nutzungs- und Inhaltsdaten sowie um Besonderheiten im Zusammenhang mit sonstigen Ermittlungsmaßnahmen wie beispiels¬weise bei der Durchsuchung, Sicherstellung und Auswertung von Computern und Mobil¬telefonen. Gerade hier war der nationale und der europäische Gesetzgeber in den letzten Jahren in einer Weise tätig, dass auch Spezialisten den Überblick verlieren können.

III. Straftatbestände im Internet

Im letzten Teil werden die typischen, im Internet auftretenden Straftatbestände besprochen. Hierbei geht es nicht nur um klassische Computerkriminalität im engeren Sinn, sondern insbesondere auch um Delikte, die die Justiz regelmäßig beschäftigen können, wie beispielsweise Betrug oder Fälschung beweiserheblicher Daten.

Arbeitsprogramm

A. Einleitung

B. Die Zuständigkeit

- Allgemeine Zuständigkeitsgrundsätze
  1. Tatorte im Einzelnen – Interlokalität
  2. Die Zuständigkeit auf Grund der Vereinbarungen der Generalstaatsanwälte
  3. Mehraktigkeit
  4. Einschub: Die Tatzeit – Noch mehr Mehraktigkeit
  5. Die Verantwortlichkeit der am Internet Beteiligten
  6. Sicherstellung von Servern – Auslandsbezug von Ermittlungen – E-Evidence

C. Prozessuale Probleme im Zusammenhang mit Internetstraftaten

I. Moderne Methoden zur Begründung des Anfangsverdachts
  1. Erste Maßnahmen der Beweissicherung
  2. Kritische Gedanken zum Grundrechtsschutz

II. Ermittlungen Unmittelbar im Internet – Osint
  1. Was sind Osint?
  2. Testkäufe, Auskunftsverlangen an Postdienstleister und sonstige Ermittlungen
  3. Spezielle Osint-Ermittlungstools
  4. Die Zulässigkeit von Osint-Ermittlungen – Die Hörfalle
  5. Was nicht geht – Gesichtserkennung
  6. Was doch manchmal geht – Überwindung des Tor-Netzwerks oder von Anoservern

III. Erkenntnisse von Ausländischen Ermittlungsbehörden (Encrochat, Anom Etc.)

IV. Ermittlungen beim Anbieter von Telekommunikationsdiensten oder digitalen Diensten
  1. Einleitung
  2. Arten der Bestandsdatenauskunft
  3. Verkehrsdaten, Vorratsdaten, Funkzellendaten, Standortdaten Gemäß § 100 G STPO
  4. Nutzungsdaten bei Digitalen Diensten gemäß § 100k STPO
  5. Inhaltsdaten gemäß § 100a STPO
  6. Grundrechtssichernde Verfahrensregelungen
  7. Überwachen von E-Mails
  8. Zuständigkeit und Übermittlungsform
  9. Verwertung von Daten im Prozess

V. Unmittelbare Maßnahmen gegen den Beschuldigten oder Dritte
  1. Die Online-Durchsuchung nach § 100b STPO
  2. Die Quellen-TKÜ § 100a I 2 Stpo
  3. Die Durchführung der Durchsuchung gemäß den §§ 102, 103 STPO
  4. Nach der Durchsuchung: Rechtsschutz, Auswertung, Einziehung und STREG
  5. „Retrograde“ Auskunftsverlangen der Strafverfolgungsbehörden an Postdienstleister
  6. IMSI-Catcher und W-LAN-Catcher
  7. Rückverfolgungsprogramme: Stille SMS – IP-Tracking

VI. Einschub: Akteneinsicht an Verteidiger

D. Straftatbestände mit Internetbezug

I. Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und Systemen
  1. Ausspähen von Daten (§ 202 A STGB)
  2. Abfangen von Daten (§ 202 B STGB) – W-LAN und Wardriver
  3. Strafbare Vorbereitung (§ 202 C STGB)
  4. Datenhehlerei (§ 202d STGB)
  5. Datenveränderung (§ 303 A STGB)
  6. Computersabotage (§ 303 B STGB)
  7. Exkurs: Bemühungen des Gesetzgebers zur Schließung von Strafbarkeitslücken

II. Computerbezogene Delikte
  1. Betreiben krimineller Handelsplattformen im Internet (§ 127 STGB)
  2. Computerbetrug (§ 263a STGB)
  3. Betrug (§ 263 Stgb)
  4. Fälschung Beweiserheblicher Daten (§ 269 STGB) und Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 STGB)

III. Sonstige Straftaten mit Internetbezug
  1. Erpressung (§ 253 STGB)
  2. Hehlerei (§ 259 STGB)

IV. Phishing
  1. Ablauf des Phishing
  2. Rechtliche Bewertung des Phishings

V. Online-Glücksspiel

VI. Schutzmaßnahmen