

**Online-Vortrag LIVE: Aktuelle Entwicklungen im Internetstrafrecht****Live-Übertragung:** 18. Dezember 2024,  
13.30 – 19.00 Uhr  
(inkl. 30 Min. Pause)**Zeitstunden:** 5,0 – mit Bescheinigung  
nach §15 Abs.2 FAO**Kostenbeitrag:** 275,- € (USt.-befreit)Ermäßigter Kostenbeitrag für Mitglieder der  
kooperierenden Rechtsanwaltskammern**Nr.:** 224170Anmeldung über die neue DAI-Webseite  
**www.anwaltsinstitut.de**  
mit vielen neuen Services:**Mit E-Mail-Adresse anmelden**

E-Mail-Adresse

Kennwort

Kennwort vergessen?

Anmelden

Sie haben noch kein Konto? Jetzt registrieren

- 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](http://www.anwaltsinstitut.de/faocomplete)**

**Fachinstitute für  
Informationstechnologierecht/  
Strafrecht**


Online-Vortrag LIVE

**Aktuelle Entwicklungen im  
Internetstrafrecht**
**18. Dezember 2024  
13.30 – 19.00 Uhr  
Online**
**Martin Reiter**  
Staatsanwalt
**www.anwaltsinstitut.de**Gemeinnützige Einrichtung der Bundesrechtsanwaltskammer,  
Bundesnotarkammer, Rechtsanwaltskammern und Notarkammern.

**Referent****Martin Reiter**, Staatsanwalt**Inhalt**

Fast täglich werden wir mit den kriminellen Schattenseiten des Internets konfrontiert. Sei es in der journalistischen Berichterstattung über die Gefahren des Cyber-Wars, als Zielobjekt von Spam-Attacken oder bei der beruflichen Befassung mit Tätern oder Opfern dieser Form der Kriminalität. Berührungspunkte gibt es ständig. Es ist aufgrund der aktuellen technischen Entwicklung kaum möglich, hier einen Überblick zu behalten. Zugleich sollte sich auch der im Informationstechnologierecht und/oder Strafrecht tätige Anwalt mit diesen Phänomenen auseinandersetzen, um das notwendige Rüstzeug für die anwaltliche Praxis zu erhalten.

Der Vortrag beschäftigt sich mit den rechtlichen Grundlagen der Verfolgung von Kriminalität im Internet und deren praktischer Umsetzung. Hierbei wird insbesondere Wert darauf gelegt, immer wieder auftauchende Begriffe lebensnah zu erläutern, die in der Praxis regelmäßig auftretenden Fallsituationen anschaulich zu vermitteln und die Arbeitsweise der Strafverfolgungsbehörden nachvollziehbar zu machen. Besondere technische Vorkenntnisse werden nicht vorausgesetzt.

Teilnehmer und Teilnehmerinnen erhalten eine instruktive Arbeitsunterlage mit allen wichtigen Hinweisen des Referenten.

**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. Auslandsbezug von Ermittlungen – E-Evidence

**C. Prozessuale Probleme im Zusammenhang mit Internetstraftaten****I. Einleitung**

1. Moderne Methoden zur Begründung des Anfangsverdachts
2. Erste Maßnahmen der Beweissicherung
3. 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

**III. Erkenntnisse von Ausländischen Ermittlungsbehörden (EncroChat, Anom etc.)****IV. Ermittlungen beim Anbieter von Telekommunikations- oder Telemediendiensten**

1. Einleitung
2. Arten der Bestandsdatenauskunft
3. Verkehrsdaten, Vorratsdaten, Funkzellendaten, Standortdaten gemäß § 100g StPO
4. Nutzungsdaten bei Telemediendiensten 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 gemäß § 100a Abs. 1 Satz 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

**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 (§ 202a StGB)
2. Abfangen von Daten (§ 202b StGB) – W-LAN und Wardriver
3. Strafbare Vorbereitung (§ 202c StGB)
4. Datenhehlerei (§ 202d StGB)
5. Datenveränderung (§ 303a StGB)
6. Computersabotage (§ 303b StGB)
7. Exkurs: Bemühungen des Gesetzgebers zur Schließung von Strafbarkeitslücken

**II. Computerbezogene Delikte**

1. Betreiben krimineller Handelsplattformen im Internet (§ 127 StGB)
2. Computerbetrug
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

**IV. Phishing**

1. Ablauf des Phishings
2. Rechtliche Bewertung des Phishings

**V. Schutzmaßnahme**