



**HOCHSCHULE  
MITTWEIDA**  
University of Applied Sciences

# Rechtsgrundlagen Cybercrime Gesetzliche Grundlagen

Prof. Dr. Dirk Labudde



Bundeskriminalamt

# Cybercrime

Das Wort ‚Cyber‘ und in Folge der Begriff ‚Cyberspace‘ bezieht sich auf eine virtuelle Welt. Das Kunstwort bezieht sich auf ‚Cyber‘ (Kybernetic) und ‚Space‘ (Raum). Man befindet sich also in einer virtuellen Welt, in der es andere Regeln als in der realen Welt gibt.

traditionellen Bereich des ‚Cybercrime‘ nicht zuordbar:

- Cyberstalking
- Cybermobbing
- Urheberrechtsverletzungen,



**Eine genaue rechtliche Differenzierung wird immer schwieriger.**

# Das Problem einer eindeutigen Definition

- Wissenschaftssprache ist eine stark standardisierte und formalisierte Sprache.
- Beherrscht von **Definitionen und Theorien**, die das gemeinsame Verständnis einer Fragestellung oder der **Beschäftigung mit einem Thema** erleichtern und leiten sollen.

# Cybercrime

„Unter ‚Cybercrime‘ oder ‚IuK-Kriminalität‘ versteht man Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden.

Das sind:

- alle Straftaten, bei denen Elemente der EDV in den Tatbestandsmerkmalen enthalten sind (Computerkriminalität) oder bei denen die IuK zur Planung, Vorbereitung oder Ausführung einer Tat eingesetzt wird/wurde,
- Straftaten im Zusammenhang mit Datennetzen wie z. B. dem Internet und
- Fälle der Bedrohung von Informationstechnik. Dies schließt alle widerrechtlichen Handlungen gegen die Integrität, Verfügbarkeit und Authentizität von elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeicherten oder übermittelten Daten (Hacking, Computersabotage, Datenveränderung, Missbrauch von Telekommunikationsmitteln etc.) ein.“

([www.bka.de](http://www.bka.de), unter der Rubrik „Themen A-Z → → Internetkriminalität“)

# Cybercrime

Einfluss auf die Definition und das Verständnis hat der jeweils länderspezifische Rechts- und Kulturkreis.

Auf dieser Basis definiert jedes Land autonom, welche Vorfälle Cybercrime-Delikte sind oder nicht. Was in einem Land als kriminell betrachtet wird, kann in einem anderen Land als nicht relevant gesehen werden.

- Cyber Konvention
- Nationale Paragraphen

# Cybercrime

Jede wissenschaftliche Fachdisziplin hat eine eigene Fachsprache und eigene Definitionen.

Im Fall des Begriffs ‚Cybercrime‘ spannt sich der Bogen der Definitionen von Technik-, Rechts- und Wirtschaftswissenschaft bis hin zur Kriminologie, Psychologie und Soziologie.

Diese Disziplinen haben sich übergreifend nicht auf einen Einheitlichen Begriff verständigt, sodass unter dem Begriff ‚Cybercrime‘ maximal von einer Phänomenologie und nicht von einer Definition gesprochen werden kann.

# Kriminologie

In der Kriminologie ist Cybercrime noch eine recht junge Disziplin!

Fokus: Digitalisierung der Lebenswelt – besonders durch die neuen Medien

Cyberkriminologie

# Cyberkriminologie

Neue Formen von sozialer Abweichung, von Straftaten, von Opferwerdungen aber auch von sozialer und staatlicher Kontrolle entstehen und erfordern einen radikal neuen Ansatz der Kriminologie: Die Cyberkriminologie erforscht:

- Ursachen
- Zusammenhänge
- Präventionsmöglichkeiten von Straftaten

die im virtuellen Raum geschehen und Auswirkungen auf die physische Realität haben.



# Zusammenfassung

Es gibt keine einheitliche Beschreibung, bzw. Definition von Cybercrime.

Aktuell drei Arten der Differenzierung:

Variante 1: Cybercrime im engeren Sinn (Core Cybercrime bzw. Cyberdependent Crime):  
alle Delikte, die es in keiner Variante offline gibt

Variante 2: Cybercrime im weiteren Sinn (Non-cyberspecific Cybercrime bzw. Cyberenabled Crime):  
Delikte, die unter diese Kategorie fallen, können auch offline existieren

Variante 3: Verschleierung der Identität:  
Dies betrifft Täter, die sich einen Online-Avatar zulegen  
und die Anonymität dazu verwenden, kriminell zu handeln, bzw. Täter, die  
sich gestohlener Identitäten oder Fake-Identities bedienen.

# Europol

Zum Thema Cybercrime definiert Europol folgendes:

- Die Intensität von Cybercrime hängt von kulturellen, juristischen, wirtschaftlichen und regionalen Einflussfaktoren ab;
- traditionelle Methoden der Verbrechensbekämpfung greifen hier nicht mehr. Elektronische ‚Beweise‘ verteilen sich oft über mehrere Orte der Welt, was ein Auffinden der Täter erschwert;
- in einer Welt von **Cloud Computing** muss sich die Legislative künftig überlegen, welche Beweise zur Verurteilung von Tätern in Frage kommen, damit eine effiziente Strafverfolgung möglich wird;
- es bedarf einer Harmonisierung der nationalen Rechte, um eine Strafverfolgung im internationalen Umfeld zu erleichtern und
- die Cybercrime-Prävention muss in allen Ländern im Vordergrund stehen

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Gesetzesgrundlagen


Mit dem Inkrafttreten der Cybercrime Konvention in Deutschland am 01.07.2009 wurde das deutsche Strafrecht an die aktuellen Entwicklungen im Bereich der Internet- und Computerstraftaten angepasst.

Allerdings werden in dieser Konvention **keine Straftatbestände** festgelegt, sondern **Kategorien** gebildet, denen jeder Mitgliedstaat seine strafbewehrten Handlungen zuordnen kann oder in Ermangelung entsprechender Tatbestände verpflichtet ist, neue Gesetze zu erlassen.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Deutschland ratifiziert Cybercrime-Abkommen

09.03.2009 14:44 Uhr

 vorlesen

Die Bundesregierung verstärkt die internationale Zusammenarbeit im Kampf gegen die Internetkriminalität. Deutschland hat nach [Angaben des Europarates](#) als 24. der 47 Europaratsländer die [Cybercrime Convention](#) der Staatenorganisation ratifiziert.

Kinderpornografie, Verstöße gegen das Urheberrecht und Angriffe auf die Sicherheit von Computersystemen stehen im Mittelpunkt des Textes. Die Justizverfahren betroffener Länder sollen koordiniert und beschleunigt werden. Der deutsche Vertreter beim Europarat, Eberhard Kölsch, hinterlegte heute in Straßburg die offizielle Urkunde.

Straftäter im Internet können nach Einschätzung des Bundeskriminalamts noch nicht wirksam genug bekämpft werden. In Deutschland steigt die Zahl der ermittelten Fälle von Kinderpornografie ständig und erreichte 2007 bereits 11.357 Fälle. (dpa) / (dpa) / ([anw](#))

# CONVENTION ON CYBERCRIME PROTOCOL ON XENOPHOBIA AND RACISM



Explanatory Reports  
and Guidance Notes

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

WWW.COE.INT HUMAN RIGHTS DEMOCRACY RULE OF LAW EXPLORE English Connect

COUNCIL OF EUROPE COUNCIL OF EUROPE Cybercrime

Home Budapest Convention T-CY Committee Capacity Building C-PROC Office Octopus Resources Newsletters

You are here: Cybercrime > T-CY Committee > T-CY News

T-CY News

Paris Call on Cyberspace: "Budapest Convention a key tool"

PARIS, FRANCE | 12 NOVEMBER 2018

Tools on Cybercrime & Electronic Evidence Empowering You!

Search tool

Octopus Community Join us or sign in!

Events  
T-CY 19th Plenary / 2nd Protocol Drafting Plenary (10-11-12-2018)

# Cybercrime Convention

Mehr als 50 Staaten, 90 NGOs und Hochschulen sowie 130 Unternehmen und Gruppen haben dem Pariser Aufruf zu Vertrauen und Sicherheit im Cyberspace zugestimmt. Der Aufruf wurde am 12. November vom französischen Präsidenten Macron ins Leben gerufen.

Ihre Unterstützer verpflichten sich, unter anderem **zusammenzuarbeiten, um die Verhinderung und Widerstandsfähigkeit gegen böswillige Online-Aktivitäten** zu stärken, Eingriffe in Wahlen zu verhindern, die Zugänglichkeit und Integrität des Internets zu schützen, Söldneraktivitäten im Internet und nichtstaatliche Aktivitäten einzudämmen Akteure und zur Stärkung einschlägiger internationaler Standards.

Staaten und Organisationen, die der Forderung zustimmen, erkennen an, dass die Bedrohung durch Cyber-Kriminalität mehr Anstrengungen erfordert, um die Sicherheit der von uns verwendeten Produkte zu verbessern, unsere Abwehrkräfte gegen Kriminelle zu stärken und die Zusammenarbeit zwischen allen Beteiligten innerhalb und über die Landesgrenzen hinweg zu fördern *Die Budapester Konvention* gegen Cyberkriminalität ist in dieser Hinsicht ein wichtiges Instrument. “

# Grundlagen für die Verfolgung von Cybercrime-Delikten

WWW.COE.INT HUMAN RIGHTS DEMOCRACY RULE OF LAW EXPLORE English Connect

COUNCIL OF EUROPE Treaty Office

Home About Full list Signatures and Ratifications Searches Partial Agreements Translations Templates Notifications Contact

You are here: Conventions



## Chart of signatures and ratifications of Treaty 185

Convention on Cybercrime

Status as of 18/12/2020

<b>Title</b>	Convention on Cybercrime
<b>Reference</b>	ETS No.185
<b>Opening of the treaty</b>	Budapest, 23/11/2001 - Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States
<b>Entry into Force</b>	01/07/2004 - 5 Ratifications including at least 3 member States of the Council of Europe

State who signed  State who ratified  State who neither signed nor ratified  State who suspended  State who denounced

	Signature	Ratification	Entry into Force	Notes	R.	D.	A.	T.	C.	Q.
Members of Council of Europe										
Albania	23/11/2001	20/06/2002	01/07/2004				A			
Andorra	23/04/2013	16/11/2016	01/03/2017		R	D	A			



# Grundlagen für die Verfolgung von Cybercrime-Delikten

*Übersetzung*

0.311.43

## **Übereinkommen über die Cyberkriminalität<sup>1</sup>**

Abgeschlossen in Budapest am 23. November 2001  
Von der Bundesversammlung genehmigt am 18. März 2011<sup>2</sup>  
Schweizerische Ratifikationsurkunde hinterlegt am 21. September 2011  
In Kraft getreten für die Schweiz am 1. Januar 2012  
(Stand am 8. August 2017)

<https://www.coe.int/en/web/conventions/full-list>

*Präambel*

*Die Mitgliedstaaten des Europarats  
und  
die anderen Staaten, die dieses Übereinkommen unterzeichnen,*

in der Erwägung, dass es das Ziel des Europarats ist, eine engere Verbindung zwischen seinen Mitgliedern herbeizuführen;

in Anerkennung der Bedeutung einer verstärkten Zusammenarbeit mit den anderen Staaten, die Vertragsparteien dieses Übereinkommens sind;

überzeugt von der Notwendigkeit, vorrangig eine gemeinsame Strafrechtspolitik zu verfolgen, die den Schutz der Gesellschaft vor Computerkriminalität, unter anderem durch die Annahme geeigneter Rechtsvorschriften und die Förderung der internationalen Zusammenarbeit, zum Ziel hat;

eingedenk der tiefgreifenden Veränderungen, die durch die Digitalisierung, die Konvergenz und die kontinuierliche Globalisierung von Rechnernetzen hervorgerufen werden;

besorgt über die Gefahr, dass Rechnernetze und elektronische Informationen auch zur Begehung von Straftaten benutzt und Beweismaterial für Straftaten über solche Netze gespeichert und übermittelt werden können;

in der Erkenntnis, dass die Staaten und die Privatwirtschaft bei der Bekämpfung der Computerkriminalität zusammenarbeiten und berechnete Interessen am Einsatz und an der Entwicklung von Informationstechnologien geschützt werden müssen;

in der Überzeugung, dass zur wirksamen Bekämpfung der Computerkriminalität eine verstärkte, zügige und gut funktionierende internationale Zusammenarbeit in Strafsachen nötig ist;

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel 1 – Begriffsbestimmungen

### Artikel 1 – Begriffsbestimmungen

Im Sinne dieses Übereinkommens bedeutet

- a „Computersystem“ eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen;
- b „Computerdaten“ jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschließlich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann;
- c „Diensteanbieter“
  - i jede öffentliche oder private Stelle, die es Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren;
  - ii jede andere Stelle, die für einen solchen Kommunikationsdienst oder für seine Nutzer Computerdaten verarbeitet oder speichert;
- d „Verkehrsdaten“ alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

### Abschnitt 1 – Materielles Strafrecht

#### *Titel 1 – Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen*

##### **Artikel 2 – Rechtswidriger Zugang**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

##### **Artikel 3 – Rechtswidriges Abfangen**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Computersystem, aus einem Computersystem oder innerhalb eines Computersystems einschließlich elektromagnetischer Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat in unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

### Abschnitt 1 – Materielles Strafrecht

#### Artikel 4 – Eingriff in Daten

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

2 Eine Vertragspartei kann sich das Recht vorbehalten, als Voraussetzung vorzusehen, dass das in Absatz 1 beschriebene Verhalten zu einem schweren Schaden geführt haben muss.

#### Artikel 5 – Eingriff in ein System

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die unbefugte schwere Behinderung des Betriebs eines Computersystems durch Eingeben, Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

### Abschnitt 1 – Materielles Strafrecht

#### Artikel 6 – Missbrauch von Vorrichtungen

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

- a das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

### Abschnitt 1 – Materielles Strafrecht

#### *Titel 2 – Computerbezogene Straftaten*

##### **Artikel 7 – Computerbezogene Fälschung**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben: das zu unechten Daten führende Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten in der Absicht, dass diese Daten für rechtliche Zwecke so angesehen oder einer Handlung zugrunde gelegt werden, als wären sie echt, gleichviel, ob die Daten unmittelbar lesbar und verständlich sind. Eine Vertragspartei kann als Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst in Verbindung mit einer betrügerischen oder ähnlichen unredlichen Absicht eintritt.

##### **Artikel 8 – Computerbezogener Betrug**

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlung, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben: die Beschädigung des Vermögens eines anderen durch

- a Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten;

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

### Abschnitt 1 – Materielles Strafrecht

#### *Titel 3 – Inhaltsbezogene Straftaten*

#### **Artikel 9 – Straftaten mit Bezug zu Kinderpornographie**

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um folgende Handlungen, wenn vorsätzlich und unbefugt begangen, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben:

- a das Herstellen von Kinderpornographie zum Zweck ihrer Verbreitung über ein Computersystem;
- b das Anbieten oder Verfügbarmachen von Kinderpornographie über ein Computersystem;
- c das Verbreiten oder Übermitteln von Kinderpornographie über ein Computersystem;
- d das Beschaffen von Kinderpornographie über ein Computersystem für sich selbst oder einen anderen;
- e den Besitz von Kinderpornographie in einem Computersystem oder auf einem Computerdatenträger.

2 Im Sinne des Absatzes 1 umfasst der Ausdruck „Kinderpornographie“ pornographisches Material mit der visuellen Darstellung

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

### Abschnitt 1 – Materielles Strafrecht

#### *Titel 4 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte*

#### **Artikel 10 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte**

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Urheberrechtsverletzungen, wie sie im Recht dieser Vertragspartei aufgrund ihrer Verpflichtungen nach der Pariser Fassung der Berner



# Grundlagen für die Verfolgung von Cybercrime-Delikten

Kapitel II – Innerstaatlich zu treffende Maßnahmen

Abschnitt 1 – Materielles Strafrecht

*Titel 5 – Weitere Formen der Verantwortlichkeit und Sanktionen*

- Versuch und Beihilfe oder Anstiftung
- Verantwortlichkeit juristischer Personen
- Sanktionen und Maßnahmen

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel II – Innerstaatlich zu treffende Maßnahmen

Abschnitt 2 – Verfahrensrecht

*Titel 1 – Allgemeine Bestimmungen*

Titel 2 – Umgehende Sicherung gespeicherter Computerdaten

Titel 3 – Anordnung der Herausgabe

Titel 4 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten

Titel 5 – Erhebung von Computerdaten in Echtzeit

## Abschnitt 3 – Gerichtsbarkeit

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Abschnitt 3 – Gerichtsbarkeit

### Artikel 22 – Gerichtsbarkeit

- 1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre Gerichtsbarkeit über die nach den Artikeln 2 bis 11 umschriebenen Straftaten zu begründen, wenn die Straftat wie folgt begangen wird:
  - a in ihrem Hoheitsgebiet;
  - b an Bord eines Schiffes, das die Flagge dieser Vertragspartei führt;
  - c an Bord eines Luftfahrzeugs, das nach dem Recht dieser Vertragspartei eingetragen ist, oder
  - d von einem ihrer Staatsangehörigen, wenn die Straftat nach dem am Tatort geltenden Recht strafbar ist oder die Straftat außerhalb des Hoheitsbereichs irgendeines Staates begangen wird.
- 2 Jede Vertragspartei kann sich das Recht vorbehalten, die in Absatz 1 Buchstaben b bis d oder in Teilen davon enthaltenen Vorschriften in Bezug auf die Gerichtsbarkeit nicht oder nur in bestimmten Fällen oder unter bestimmten Bedingungen anzuwenden.
- 3 Jede Vertragspartei trifft die erforderlichen Maßnahmen, um ihre Gerichtsbarkeit über die in Artikel 24 Absatz 1 bezeichneten Straftaten in den Fällen zu begründen, in denen sich eine verdächtige Person in ihrem Hoheitsgebiet befindet und sie sie, nachdem ein Auslieferungersuchen gestellt worden ist, nur deshalb nicht an eine andere Vertragspartei ausliefert, weil sie ihre Staatsangehörige ist.
- 4 Dieses Übereinkommen schließt die Ausübung einer Strafgerichtsbarkeit durch eine Vertragspartei nach ihrem innerstaatlichen Recht nicht aus.
- 5 Wird die Gerichtsbarkeit für eine mutmaßliche Straftat, die nach diesem Übereinkommen umschrieben ist, von mehr als einer Vertragspartei geltend gemacht, so konsultieren die beteiligten Vertragsparteien einander, soweit angebracht, um die für die Strafverfolgung geeignetste Gerichtsbarkeit zu bestimmen.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel III – Internationale Zusammenarbeit

### Abschnitt 1 – Allgemeine Grundsätze

#### *Titel 1 – Allgemeine Grundsätze der internationalen Zusammenarbeit*

### **Artikel 23 – Allgemeine Grundsätze der internationalen Zusammenarbeit**

Die Vertragsparteien arbeiten untereinander im Einklang mit diesem Kapitel im größtmöglichen Umfang zusammen, indem sie einschlägige völkerrechtliche Übereinkünfte über die internationale Zusammenarbeit in Strafsachen sowie Übereinkünfte, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurden, und innerstaatliche Rechtsvorschriften für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat anwenden.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

## Kapitel IV – Schlussbestimmungen

Artikel 36 – Unterzeichnung und Inkrafttreten

Artikel 37 – Beitritt zum Übereinkommen

Artikel 38 – Räumlicher Geltungsbereich

Artikel 39 – Wirkungen des Übereinkommens



...

Artikel 47 – Kündigung

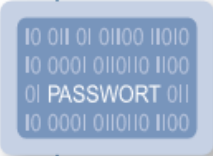
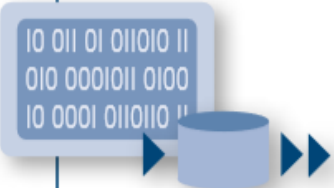
Artikel 48 – Notifikation

# Nationale Umsetzung

# Grundlagen für die Verfolgung von Cybercrime-Delikten

Straftatbestände	Inhalt (Kurzbeschreibung)
<p data-bbox="675 406 896 554"><b>§202a StGB</b> <b>Ausspähen von Daten</b></p> 	<p data-bbox="1039 406 1714 714">Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung.</p>
<p data-bbox="675 801 952 948"><b>§ 202b StGB</b> <b>Abfangen von Daten</b></p> 	<p data-bbox="1039 801 1714 1156">Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln.</p>

# Grundlagen für die Verfolgung von Cybercrime-Delikten

<p><b>§ 202c StGB</b> <b>Vorbereiten des Ausspähens und Abfangens von Daten</b></p> 	<p>Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist.</p>
<p><b>§ 202d StGB</b> <b>Datenhehlerei</b></p> 	<p>Das sich oder einem anderen Verschaffen, Überlassen, Verbreiten oder Zugänglichmachen von nicht allgemein zugänglichen und durch einen anderen aus einer rechtswidrigen Tat erlangten Daten mit der Absicht, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.</p>



# Grundlagen für die Verfolgung von Cybercrime-Delikten



## §263a StGB Computer- betrug



Das Schädigen des Vermögens eines Anderen durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf.

Des Weiteren das Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Feilhalten, Verwahren oder Überlassung eines Computerprogramms, deren Zweck die Begehung einer solchen Tat ist.

# Grundlagen für die Verfolgung von Cybercrime-Delikten

<p>Das Speichern oder Verändern beweisheblicher Daten zur Täuschung im Rechtsverkehr, so dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten.</p>	<p><b>§269 StGB</b> <b>Fälschung</b> <b>beweisheblicher</b> <b>Daten</b></p> 
<p>Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.</p>	<p><b>§303a StGB</b> <b>Datenveränderung</b></p> 

# Grundlagen für die Verfolgung von Cybercrime-Delikten

Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch

1. Begehung einer Datenveränderung (§ 303a),
2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen Nachteil zuzufügen, oder
3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.

**§303b StGB  
Computer-  
sabotage**



# Gründe ursächlich für die Nichterstattung von Anzeigen:

- Fehlende Sensibilisierung/Awareness bei den Verantwortlichen auf Leitungsebene.
- Keine Anzeigen aus Sorge vor Imageschäden durch befürchtete Presseveröffentlichungen.
- Befürchtete negative Auswirkungen unter Konkurrenz- oder Wettbewerbsaspekten.
- Die Strafverfolgung dauert aus Sicht der Unternehmen zu lange bzw. es wird Erfolglosigkeit der polizeilichen Ermittlungen befürchtet.
- Insbesondere kleinere Firmen haben Sorge, dass die Polizei Firmenrechner sicherstellt und diese erst nach einem längeren Zeitraum wieder aushändigt.
- Teilweise verfügen Unternehmen über unzureichend lizenzierte Software, sodass die Angst vor einem Strafverfahren gegen die Firma überwiegt. Gleiches gilt bei einem bekannten oder angenommenen Vorhandensein illegaler Dateien auf den Computern oder Profilen einzelner Beschäftigter der Firma.

- Es handelt sich oftmals um Innentäter, sodass eine firmeninterne Regulierung bevorzugt wird.
- Die Angriffe werden abgewehrt bzw. bleiben erfolglos.
- Zunächst keine Schäden erkennbar oder messbar.



## Polizeiliche Zuständigkeiten

Bei den Landespolizeien werden Cybercrime-Delikte in der Regel durch örtliche Fachdienststellen bearbeitet oder – z. B. bei schwerwiegenden und überregionalen Fällen – auch durch das jeweilige Landeskriminalamt (LKA).

Das Bundeskriminalamt (BKA) unterstützt die Polizeien der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. In bestimmten Fällen kann auch das BKA selbst die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen und Ermittlungsverfahren führen.

Im BKA sowie in den LKÄ wurden speziell für Unternehmen sowie öffentliche und nichtöffentliche Institutionen die sogenannten „**Zentralen Ansprechstellen Cybercrime**“ (ZAC) eingerichtet. Diese dienen als „Single Point of Contact“ (SPoC), um als kompetenter Ansprechpartner Informationen zu IT-Sicherheitsvorfällen direkt von Ihnen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen.

# Das Netzwerkdurchsetzungsgesetz



## Regeln gegen Hass im Netz – das Netzwerkdurchsetzungsgesetz

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) ist seit dem 1. Oktober 2017 in Kraft.

Das Gesetz zielt darauf, **Hasskriminalität, strafbare Falschnachrichten und andere strafbare Inhalte auf den Plattformen sozialer Netzwerke wirksamer zu bekämpfen**. Dazu zählen z.B. Beleidigung, üble Nachrede, Verleumdung, öffentliche Aufforderung zu Straftaten, Volksverhetzung, Gewaltdarstellung und Bedrohung. Um die sozialen Netzwerke zu einer zügigeren und umfassenderen Bearbeitung von Beschwerden insbesondere von Nutzerinnen und Nutzer über Hasskriminalität und andere strafbare Inhalte anzuhalten, wurden mit dem NetzDG gesetzliche Compliance-Regeln für soziale Netzwerke eingeführt.

Dies beinhaltet eine gesetzliche Berichtspflicht für Anbieterinnen und Anbieter sozialer Netzwerke über den Umgang mit Hasskriminalität und anderen strafbaren Inhalten, Vorgaben zum Vorhalten eines wirksamen Beschwerdemanagements sowie zur Benennung eines inländischen Zustellungsbevollmächtigten. Verstöße gegen diese Pflichten können mit Bußgeldern gegen das Unternehmen und die Aufsichtspflichtigen geahndet werden. Außerdem wird Opfern von Persönlichkeitsrechtsverletzungen im Netz ermöglicht, aufgrund gerichtlicher Anordnung die Bestandsdaten der Verletzterinnen und Verletzter von den Diensteanbietenden zu erhalten.

[https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG\\_node.html](https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_node.html)

[https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE\\_Aenderung\\_NetzDG.pdf?\\_\\_blob=publicationFile&v=2](https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Aenderung_NetzDG.pdf?__blob=publicationFile&v=2)



# **Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)**

# Netzwerkdurchsetzungsgesetz - NetzDG

NetzDG

Ausfertigungsdatum: 01.09.2017

Vollzitat:

"Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352)"

## **Fußnote**

(+++ Textnachweis ab: 1.10.2017 +++)

Das G wurde als Art. 1 des G v. 1.9.2017 I 3352 vom Bundestag beschlossen. Es ist gem. Art. 3 dieses G am 1.10.2017 in Kraft getreten.

# Netzwerkdurchsetzungsgesetz - NetzDG

## § 1 Anwendungsbereich

(1) Dieses Gesetz gilt für Telemediendiensteanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die dazu bestimmt sind, dass Nutzer beliebige Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen (soziale Netzwerke). Plattformen mit journalistisch-redaktionell gestalteten Angeboten, die vom Diensteanbieter selbst verantwortet werden, gelten nicht als soziale Netzwerke im Sinne dieses Gesetzes. Das Gleiche gilt für Plattformen, die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind.

(2) Der Anbieter eines sozialen Netzwerks ist von den Pflichten nach den §§ 2 und 3 befreit, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat.

(3) Rechtswidrige Inhalte sind Inhalte im Sinne des Absatzes 1, die den Tatbestand der §§ 86, 86a, 89a, 91, 100a, 111, 126, 129 bis 129b, 130, 131, 140, 166, 184b in Verbindung mit 184d, 185 bis 187, 201a, 241 oder 269 des Strafgesetzbuchs erfüllen und nicht gerechtfertigt sind.

# Netzwerkdurchsetzungsgesetz - NetzDG

## § 2 Berichtspflicht

(1) Anbieter sozialer Netzwerke, die im Kalenderjahr mehr als 100 Beschwerden über rechtswidrige Inhalte erhalten, sind verpflichtet, einen deutschsprachigen Bericht über den Umgang mit Beschwerden über rechtswidrige Inhalte auf ihren Plattformen mit den Angaben nach Absatz 2 halbjährlich zu erstellen und im Bundesanzeiger sowie auf der eigenen Homepage spätestens einen Monat nach Ende eines Halbjahres zu veröffentlichen. Der auf der eigenen Homepage veröffentlichte Bericht muss leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein.

(2) Der Bericht hat mindestens auf folgende Aspekte einzugehen:

1. Allgemeine Ausführungen, welche Anstrengungen der Anbieter des sozialen Netzwerks unternimmt, um strafbare Handlungen auf den Plattformen zu unterbinden,
2. Darstellung der Mechanismen zur Übermittlung von Beschwerden über rechtswidrige Inhalte und der Entscheidungskriterien für Löschung und Sperrung von rechtswidrigen Inhalten,
3. Anzahl der im Berichtszeitraum eingegangenen Beschwerden über rechtswidrige Inhalte, aufgeschlüsselt nach Beschwerden von Beschwerdestellen und Beschwerden von Nutzern und nach dem Beschwerdegrund,
4. Organisation, personelle Ausstattung, fachliche und sprachliche Kompetenz der für die Bearbeitung von Beschwerden zuständigen Arbeitseinheiten und Schulung und Betreuung der für die Bearbeitung von Beschwerden zuständigen Personen,
5. Mitgliedschaft in Branchenverbänden mit Hinweis darauf, ob in diesen Branchenverbänden eine Beschwerdestelle existiert,
6. Anzahl der Beschwerden, bei denen eine externe Stelle konsultiert wurde, um die Entscheidung vorzubereiten,

# Netzwerkdurchsetzungsgesetz - NetzDG

## § 2 Berichtspflicht

7. Anzahl der Beschwerden, die im Berichtszeitraum zur Löschung oder Sperrung des beanstandeten Inhalts führten, aufgeschlüsselt nach Beschwerden von Beschwerdestellen und von Nutzern, nach dem Beschwerdegrund, ob ein Fall des § 3 Absatz 2 Nummer 3 Buchstabe a vorlag, ob in diesem Fall eine Weiterleitung an den Nutzer erfolgte sowie ob eine Übertragung an eine anerkannte Einrichtung der Regulierten Selbstregulierung nach § 3 Absatz 2 Nummer 3 Buchstabe b erfolgte,

8. Zeit zwischen Beschwerdeeingang beim sozialen Netzwerk und Löschung oder Sperrung des rechtswidrigen

Inhalts, aufgeschlüsselt nach Beschwerden von Beschwerdestellen und von Nutzern, nach dem Beschwerdegrund sowie nach den Zeiträumen „innerhalb von 24 Stunden“/„innerhalb von 48 Stunden“/„innerhalb einer Woche“/„zu einem späteren Zeitpunkt“,

9. Maßnahmen zur Unterrichtung des Beschwerdeführers sowie des Nutzers, für den der beanstandete Inhalt

gespeichert wurde, über die Entscheidung über die Beschwerde.

# Netzwerkdurchsetzungsgesetz - NetzDG

## § 3 Umgang mit Beschwerden über rechtswidrige Inhalte

- (1) Der Anbieter eines sozialen Netzwerks muss ein wirksames und transparentes Verfahren nach Absatz 2 und 3 für den Umgang mit Beschwerden über rechtswidrige Inhalte vorhalten. Der Anbieter muss Nutzern ein leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Verfahren zur Übermittlung von Beschwerden über rechtswidrige Inhalte zur Verfügung stellen.
  
- (2) Das Verfahren muss gewährleisten, dass der Anbieter des sozialen Netzwerks
  1. unverzüglich von der Beschwerde Kenntnis nimmt und prüft, ob der in der Beschwerde gemeldete Inhalt rechtswidrig und zu entfernen oder der Zugang zu ihm zu sperren ist,
  2. einen offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt; dies gilt nicht, wenn das soziale Netzwerk mit der zuständigen Strafverfolgungsbehörde einen längeren Zeitraum für die Löschung oder Sperrung des offensichtlich rechtswidrigen Inhalts vereinbart hat,
  3. jeden rechtswidrigen Inhalt unverzüglich, in der Regel innerhalb von sieben Tagen nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt; die Frist von sieben Tagen kann überschritten werden, wenn
    - a) die Entscheidung über die Rechtswidrigkeit des Inhalts von der Unwahrheit einer Tatsachenbehauptung oder erkennbar von anderen tatsächlichen Umständen abhängt; das soziale Netzwerk kann in diesen Fällen dem Nutzer vor der Entscheidung Gelegenheit zur Stellungnahme zu der Beschwerde geben,
    - b) das soziale Netzwerk die Entscheidung über die Rechtswidrigkeit innerhalb von sieben Tagen nach Eingang der Beschwerde einer nach den Absätzen 6 bis 8 anerkannten Einrichtung der Regulierten Selbstregulierung überträgt und sich deren Entscheidung unterwirft,

# Rechtswidrige Inhalte sind Inhalte die den folgenden Tatbestand

- § 86: "Verwenden von Kennzeichen verfassungswidriger Organisationen"
- § 86a: "Verwenden von Kennzeichen verfassungswidriger Organisationen"
- § 89a: "Vorbereitung einer schweren staatsgefährdenden Gewalttat"
- § 91: "Angriff gegen den Bundespräsidenten"
- § 100a: "Vorbereitung eines Angriffskrieges"
- § 111: "Landesverrat"
- § 126: "Verletzung von Privatgeheimnissen"
- §§ 129 bis 129b: "Kriminelle Vereinigungen"

# Rechtswidrige Inhalte sind Inhalte die den folgenden Tatbestand

- § 130: "Volksverhetzung"
- § 131: "Gewaltdarstellung"
- § 140: "Belohnung und Billigung von Straftaten"
- § 166: "Beschimpfung von Bekenntnissen, Religionsgesellschaften und Weltanschauungsvereinigungen"
- § 184b in Verbindung mit § 184d: "Verbreitung, Erwerb und Besitz kinderpornographischer Schriften"
- §§ 185 bis 187: "Beleidigung"
- § 201a: "Verletzung des persönlichen Lebens- und Geheimbereichs durch Bildaufnahmen"
- § 241: "Störung des öffentlichen Friedens durch Androhung von Straftaten"
- § 269: "Unerlaubte Einfuhr von Kriegswaffen und anderen Kriegsmitteln"

**Sollten das alle sein?**





**StPO, TKÜ, TKM**

# Strafprozessordnung (StPO)

- Rechtsnorm in Deutschland, regelt das Strafverfahren vor deutschen Gerichten
  - Bestimmt Verfahrensabläufe, Rechte und Pflichten von Staatsanwaltschaft, Gericht, Verteidigung und Angeklagten
  - Enthält Regelungen zur Beweisaufnahme, zum Verfahrensablauf, zur Verhandlungsführung und zu Rechtsmitteln
  - Gewährleistet fairen und rechtsstaatlichen Ablauf von Strafverfahren
- § 100a Telekommunikationsüberwachung

# Telekommunikationsüberwachung (TKÜ)

- Gesetzlich verankert in § 100a Abs. 1 S. 2, 3 StPO und für das BKA zur Terrorismusbekämpfung nach §§ 5, 51 Abs.2 BKAG
- Maßnahme zur Überwachung von Telekommunikation, um strafrechtlich relevante Informationen zu sammeln
- Ermöglicht staatlichen Behörden wie Polizei oder Geheimdiensten die Überwachung von Telefonaten, E-Mails, SMS, Internetnutzung usw.
- Dient der Bekämpfung von schweren Straftaten wie Terrorismus, Organisierter Kriminalität, Drogenhandel usw.
- Erfordert richterliche Genehmigung und Einhaltung strenger rechtlicher Vorgaben zum Schutz der Privatsphäre und Grundrechte

# Telekommunikationsüberwachung (TKÜ)

## § 100a

### Telekommunikationsüberwachung

(1) <sup>1</sup>Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

<sup>2</sup>Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. <sup>3</sup>Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

# Telekommunikationsüberwachung (TKÜ)

- § 100a StPO regelt die "Verwendung technischer Mittel zur Überwachung von Telekommunikation" (TKÜ)
- umfasst Bestimmungen zur Durchführung von Maßnahmen zur Telekommunikationsüberwachung (TKÜ) im Rahmen von Ermittlungsverfahren bei schweren Straftaten oder zur Abwehr von Gefahren für hochwertige Rechtsgüter. Der Artikel legt fest, unter welchen Voraussetzungen und mit welchen Einschränkungen diese Maßnahmen durchgeführt werden dürfen und welche Behörden dazu befugt sind
- Anforderungen an die richterliche Anordnung sowie die Verwendung der gewonnenen Informationen festgelegt

# Die Paragraphen

- § 100a Telekommunikationsüberwachung
- § 100b Online-Durchsuchung
- § 100c Akustische Wohnraumüberwachung
- § 100d Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte
- § 100e Verfahren bei Maßnahmen nach den §§ 100a bis 100c
- § 100f Akustische Überwachung außerhalb von Wohnraum
- § 100g Erhebung von Verkehrsdaten
- § 100h Weitere Maßnahmen außerhalb von Wohnraum
- § 100i Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten
- § 100j Bestandsdatenauskunft
- § 100k Erhebung von Nutzungsdaten bei Telemediendiensten

# Technische Kontrolle und Maßnahmen (TKM)

- Umfassen verschiedene technische Maßnahmen zur Überwachung und Kontrolle von Telekommunikation
- Beinhalten die technische Umsetzung von Telekommunikationsüberwachung (TKÜ), die Erfassung von Verbindungsdaten (Vorratsdatenspeicherung) und die Entschlüsselung von verschlüsselten Kommunikationsinhalten
- Erfordern spezielle Technologien und Infrastrukturen zur Durchführung und Überwachung von Telekommunikationsaktivitäten
- Unterliegen strengen rechtlichen Regelungen und müssen mit Datenschutz- und Privatsphärebestimmungen im Einklang stehen

# Umsetzung von Überwachungsmaßnahmen, Erteilung von Auskünften

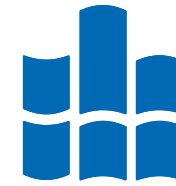
→ § 170 TKG

Auf Grund der gesetzlichen Vorschriften muss jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, bei Vorliegen einer entsprechenden schriftlichen Anordnung den berechtigten Stellen (z.B. Polizei- und Verfassungsschutzbehörden) die Überwachung und Aufzeichnung der Telekommunikation ermöglichen und Auskünfte über Verkehrsdaten erteilen.

Ob und in welchem Umfang die zur Mitwirkung verpflichteten Telekommunikationsunternehmen Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen oder die Erteilung von Auskünften treffen müssen, wird in § 170 des TKG und der TKÜV geregelt. Die Bundesnetzagentur ist zuständig für die Erarbeitung der technischen Vorgaben und die Kontrolle der entsprechenden technischen Einrichtungen und organisatorischen Maßnahmen.



# Vielen Dank



**HOCHSCHULE  
MITTWEIDA**  
University of Applied Sciences

Prof. Dr. rer. nat. Dirk Labudde

**Hochschule Mittweida** | University of Applied Sciences  
Technikumplatz 17 | 09648 Mittweida  
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

**T** +49 (0) 3727 58-1469

**F** +49 (0) 3727 58-21469

labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105  
Am Schwanenteich 6b | 09648 Mittweida

[hs-mittweida.de](https://www.hs-mittweida.de)