



Gesetzgebung zur Computerkriminalität – Länderprofil Deutschland

Dieses Länderprofil wurde im Rahmen des Projekts zur Computerkriminalität des Europarats erstellt, um Informationen über die Gesetzgebung in Bezug auf Computerkriminalität auszutauschen und den gegenwärtigen Stand der Umsetzung des Übereinkommens über Computerkriminalität in nationales Recht zu bewerten. Das Länderprofil stellt nicht in jedem Fall die offizielle Position des jeweiligen Lande oder des Europarats dar.

Anregungen und Kommentare werden gerne entgegen genommen von:

Alexander Seger
Leiter des Referats für Wirtschaftskriminalität
Abteilung für technische Zusammenarbeit
Generaldirektorat für Menschenrechte und rechtliche
Angelegenheiten
Europarat, Straßburg, Frankreich

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Version 22 07 10

Land:	Deutschland
Unterzeichnung des Übereinkommens:	Ja: 23. November 2001
Ratifikation/Beitritt:	Ja: 09. März 2009
Bestimmungen des Übereinkommens	
<i>Kapitel I – Begriffsbestimmungen</i>	
Artikel 1 – „Computersystem“, „Computerdaten“, „Diensteanbieter“, „Verkehrsdaten“:	

<p>Im Sinne dieses Übereinkommens bedeutet:</p> <p>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;</p> <p>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;</p> <p>c „Diensteanbieter“</p> <p>i jede öffentliche oder private Stelle, die es Nutzern ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren;</p> <p>ii jede andere Stelle, die für einen solchen Kommunikationsdienst oder für seine Nutzer Computerdaten verarbeitet oder speichert;</p> <p>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.</p>	<p>Während das deutsche Recht in Bezug auf „Computersysteme“ in § 303b des Strafgesetzbuchs („StGB“) lediglich von „Datenverarbeitungsanlagen“ spricht (siehe unter Artikel 5), behandelt § 202a Abs. 2 StGB den Begriff „Daten“, ohne ihn jedoch gesetzlich zu definieren (Stand Oktober 2009):</p> <p>§ 202a StGB</p> <p>Ausspähen von Daten</p> <p>(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.</p> <p>Der Begriff „Diensteanbieter“ wird teilweise von § 3 Nr. 6 des Telekommunikationsgesetzes („TKG“, Stand Februar 2010) und teilweise von § 2 Nr. 1 des Telemediengesetzes („TMG“, Stand Mai 2010) abgedeckt:</p> <p>§ 3 TKG</p> <p>Begriffsbestimmungen</p> <p>Im Sinne dieses Gesetzes ist oder sind</p> <p>1. [...]</p> <p>6. "Diensteanbieter" jeder, der ganz oder teilweise geschäftsmäßig</p> <p>a) Telekommunikationsdienste erbringt oder</p> <p>b) an der Erbringung solcher Dienste mitwirkt;</p> <p>§ 2 TMG</p> <p>Begriffsbestimmungen</p> <p>Im Sinne dieses Gesetzes</p> <p>1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde</p>
--	---

	<p>Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert,</p> <p>2. [...]</p> <p>„Verkehrsdaten“ sind in § 3 Nr. 30 TKG definiert:</p> <p>§ 3 TKG</p> <p>Begriffsbestimmungen</p> <p>Im Sinne dieses Gesetzes ist oder sind</p> <p>1. [...]</p> <p>30. "Verkehrsdaten" Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden;</p>
<p>Kapitel II – Innerstaatlich zu treffende Maßnahmen Abschnitt 1 – Materielles Strafrecht</p>	
<p>Artikel 2 – Rechtswidriger Zugang</p> <p>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.</p>	<p>Strafgesetzbuch, 2009 ("StGB"):</p> <p>§ 202a StGB</p> <p>Ausspähen von Daten</p> <p>(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.</p>
<p>Artikel 3 – Rechtswidriges Abfangen</p> <p>Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um das mit technischen Hilfsmitteln bewirkte unbefugte</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 202b StGB</p>

<p>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.</p>	<p>Abfangen von Daten</p> <p>Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.</p>
<p>Artikel 4 – Eingriff in Daten</p> <p>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.</p> <p>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.</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 303a StGB</p> <p>Datenveränderung</p> <p>(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.</p>
<p>Artikel 5 – Eingriff in ein System</p> <p>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.</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 303b StGB</p> <p>Computersabotage</p> <p>(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er</p> <ol style="list-style-type: none"> 1. eine Tat nach § 303a Abs. 1 begeht, 2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder 3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

	<p>wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.</p> <p>(3) Der Versuch ist strafbar.</p> <p>(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter</p> <ol style="list-style-type: none"> 1. einen Vermögensverlust großen Ausmaßes herbeiführt, 2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat, 3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt. <p>(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.</p>
<p>Artikel 6 – Missbrauch von Vorrichtungen</p> <p>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:</p> <ol style="list-style-type: none"> a das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen <ol style="list-style-type: none"> i einer Vorrichtung einschließlich eines Computerprogramms, die in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine nach den Artikeln 2 bis 5 umschriebene Straftat zu begehen; ii eines Computerpassworts, eines Zugangscodes oder 	<p>Strafgesetzbuch, 2009:</p> <p>§ 202c StGB</p> <p>Vorbereiten des Ausspähens und Abfangens von Daten</p> <p>(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er</p> <ol style="list-style-type: none"> 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder 2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. <p>(2) § 149 Abs. 2 und 3 gilt entsprechend.</p>

<p>ähnlicher Daten, die den Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon ermöglichen,</p> <p>mit dem Vorsatz, sie zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden, und</p> <p>b den Besitz eines unter Buchstabe a Ziffer i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden. Eine Vertragspartei kann als gesetzliche Voraussetzung vorsehen, dass die strafrechtliche Verantwortlichkeit erst mit Besitz einer bestimmten Anzahl dieser Mittel eintritt.</p> <p>2 Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.</p> <p>3 Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 nicht anzuwenden, sofern der Vorbehalt nicht das Verkaufen, Verbreiten oder anderweitige Verfügbarmachen der in Absatz 1 Buchstabe a Ziffer ii bezeichneten Mittel betrifft.</p>	<p>§ 149 StGB</p> <p>Vorbereitung der Fälschung von Geld und Wertzeichen</p> <p>(1) Wer eine Fälschung von Geld oder Wertzeichen vorbereitet, indem er</p> <ol style="list-style-type: none"> 1. Platten, Formen, Drucksätze, Druckstöcke, Negative, Matrizen, Computerprogramme oder ähnliche Vorrichtungen, die ihrer Art nach zur Begehung der Tat geeignet sind, 2. Papier, das einer solchen Papierart gleicht oder zum Verwechseln ähnlich ist, die zur Herstellung von Geld oder amtlichen Wertzeichen bestimmt und gegen Nachahmung besonders gesichert ist, oder 3. Hologramme oder andere Bestandteile, die der Sicherung gegen Fälschung dienen, <p>herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überläßt, wird, wenn er eine Geldfälschung vorbereitet, mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe, sonst mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Nach Absatz 1 wird nicht bestraft, wer freiwillig</p> <ol style="list-style-type: none"> 1. die Ausführung der vorbereiteten Tat aufgibt und eine von ihm verursachte Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abwendet oder die Vollendung der Tat verhindert und 2. die Fälschungsmittel, soweit sie noch vorhanden und zur Fälschung brauchbar sind, vernichtet, unbrauchbar macht, ihr Vorhandensein einer Behörde anzeigt oder sie dort abliefert. <p>(3) Wird ohne Zutun des Täters die Gefahr, daß andere die Tat weiter vorbereiten oder sie ausführen, abgewendet oder die Vollendung der Tat verhindert, so genügt an Stelle der Voraussetzungen des Absatzes 2 Nr. 1 das freiwillige und ernsthafte Bemühen des Täters, dieses Ziel zu erreichen.</p>
<p>Artikel 7 – Computerbezogene Fälschung</p> <p>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:</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 269 Fälschung beweisheblicher Daten</p> <p>(1) Wer zur Täuschung im Rechtsverkehr beweishebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen</p>

<p>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.</p>	<p>würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>(3) § 267 Abs. 3 und 4 gilt entsprechend.</p> <p>§ 267 StGB</p> <p>Urkundenfälschung</p> <p>(1) Wer zur Täuschung im Rechtsverkehr eine unechte Urkunde herstellt, eine echte Urkunde verfälscht oder eine unechte oder verfälschte Urkunde gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter</p> <ol style="list-style-type: none"> 1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Betrug oder Urkundenfälschung verbunden hat, 2. einen Vermögensverlust großen Ausmaßes herbeiführt, 3. durch eine große Zahl von unechten oder verfälschten Urkunden die Sicherheit des Rechtsverkehrs erheblich gefährdet oder 4. seine Befugnisse oder seine Stellung als Amtsträger mißbraucht. <p>(4) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer die Urkundenfälschung als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.</p>
<p>Artikel 8 – Computerbezogener Betrug</p> <p>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</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 263a StGB</p> <p>Computerbetrug</p> <p>(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu</p>

<p>a Eingeben, Verändern, Löschen oder Unterdrücken von Computerdaten;</p> <p>b Eingreifen in den Betrieb eines Computersystems,</p> <p>in der betrügerischen oder unredlichen Absicht, sich oder einem anderen unbefugt einen wirtschaftlichen Vorteil zu verschaffen.</p>	<p>verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis 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 beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) § 263 Abs. 2 bis 7 gilt entsprechend.</p> <p>(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.</p> <p>§ 263 StGB</p> <p>Betrug</p> <p>(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter</p> <ol style="list-style-type: none"> 1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Urkundenfälschung oder Betrug verbunden hat, 2. einen Vermögensverlust großen Ausmaßes herbeiführt oder in der Absicht handelt, durch die fortgesetzte Begehung von Betrug eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen, 3. eine andere Person in wirtschaftliche Not bringt, 4. seine Befugnisse oder seine Stellung als Amtsträger mißbraucht oder 5. einen Versicherungsfall vortäuscht, nachdem er oder ein anderer zu diesem Zweck eine Sache von bedeutendem Wert in Brand gesetzt oder durch eine Brandlegung ganz oder
---	---

	<p>teilweise zerstört oder ein Schiff zum Sinken oder Stranden gebracht hat.</p> <p>(4) § 243 Abs. 2 sowie die §§ 247 und 248a gelten entsprechend.</p> <p>(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer den Betrug als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.</p> <p>(6) Das Gericht kann Führungsaufsicht anordnen (§ 68 Abs. 1).</p> <p>(7) Die §§ 43a und 73d sind anzuwenden, wenn der Täter als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat. § 73d ist auch dann anzuwenden, wenn der Täter gewerbsmäßig handelt.</p>
<p>Artikel 9 – Straftaten mit Bezug zu Kinderpornographie</p> <p>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:</p> <p>a das Herstellen von Kinderpornographie zum Zweck ihrer Verbreitung über ein Computersystem;</p> <p>b das Anbieten oder Verfügbarmachen von Kinderpornographie über ein Computersystem;</p> <p>c das Verbreiten oder Übermitteln von Kinderpornographie über ein Computersystem;</p> <p>d das Beschaffen von Kinderpornographie über ein Computersystem für sich selbst oder einen anderen;</p> <p>e den Besitz von Kinderpornographie in einem Computersystem oder auf einem Computerdatenträger.</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 184b StGB</p> <p>Verbreitung, Erwerb und Besitz kinderpornographischer Schriften</p> <p>(1) Wer pornographische Schriften (§ 11 Abs. 3), die sexuelle Handlungen von, an oder vor Kindern (§ 176 Abs. 1) zum Gegenstand haben (kinderpornographische Schriften),</p> <ol style="list-style-type: none"> 1. verbreitet, 2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder 3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummer 1 oder Nummer 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, <p>wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft.</p> <p>(2) Ebenso wird bestraft, wer es unternimmt, einem anderen den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben.</p> <p>(3) In den Fällen des Absatzes 1 oder des Absatzes 2 ist auf Freiheitsstrafe von sechs Monaten bis zu zehn Jahren zu erkennen, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, und die kinderpornographischen Schriften ein tatsächliches oder wirklichkeitsnahes</p>

<p>2 Im Sinne des Absatzes 1 umfasst der Ausdruck „Kinderpornographie“ pornographisches Material mit der visuellen Darstellung</p> <p>a einer minderjährigen Person bei eindeutig sexuellen Handlungen;</p> <p>b einer Person mit dem Erscheinungsbild einer minderjährigen Person bei eindeutig sexuellen Handlungen;</p> <p>c einer Person mit dem Erscheinungsbild einer minderjährigen Person bei eindeutig sexuellen Handlungen;</p>	<p>Geschehen wiedergeben.</p> <p>(4) Wer es unternimmt, sich den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer die in Satz 1 bezeichneten Schriften besitzt.</p> <p>(5) Die Absätze 2 und 4 gelten nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.</p> <p>(6) In den Fällen des Absatzes 3 ist § 73d anzuwenden. Gegenstände, auf die sich eine Straftat nach Absatz 2 oder Absatz 4 bezieht, werden eingezogen. § 74a ist anzuwenden.</p> <p>§ 184c StGB</p>
<p>3 Im Sinne des Absatzes 2 umfasst der Ausdruck „minderjährige Person“ alle Personen, die das 18. Lebensjahr noch nicht vollendet haben. Eine Vertragspartei kann jedoch eine niedrigere Altersgrenze vorsehen, wobei 16 Jahre nicht unterschritten werden dürfen.</p>	<p>Verbreitung, Erwerb und Besitz jugendpornographischer Schriften</p> <p>(1) Wer pornographische Schriften (§ 11 Abs. 3), die sexuelle Handlungen von, an oder vor Personen von vierzehn bis achtzehn Jahren zum Gegenstand haben (jugendpornographische Schriften),</p>
<p>4 Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 1 Buchstaben d und e sowie Absatz 2 Buchstaben b und c ganz oder teilweise nicht anzuwenden.</p>	<p>1. verbreitet,</p> <p>2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder</p> <p>3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummer 1 oder Nummer 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen,</p> <p>wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Ebenso wird bestraft, wer es unternimmt, einem anderen den Besitz von jugendpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben.</p> <p>(3) In den Fällen des Absatzes 1 oder des Absatzes 2 ist auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu erkennen, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, und die jugendpornographischen Schriften ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben.</p> <p>(4) Wer es unternimmt, sich den Besitz von jugendpornographischen Schriften zu</p>

	<p>verschaffen, die ein tatsächliches Geschehen wiedergeben, oder wer solche Schriften besitzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. Satz 1 ist nicht anzuwenden auf Handlungen von Personen in Bezug auf solche jugendpornographischen Schriften, die sie im Alter von unter achtzehn Jahren mit Einwilligung der dargestellten Personen hergestellt haben.</p> <p>(5) § 184b Abs. 5 und 6 gilt entsprechend.</p> <p>§ 184d StGB</p> <p>Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste</p> <p>Nach den §§ 184 bis 184c wird auch bestraft, wer eine pornographische Darbietung durch Rundfunk, Medien- oder Teledienste verbreitet. In den Fällen des § 184 Abs. 1 ist Satz 1 bei einer Verbreitung durch Medien- oder Teledienste nicht anzuwenden, wenn durch technische oder sonstige Vorkehrungen sichergestellt ist, dass die pornographische Darbietung Personen unter achtzehn Jahren nicht zugänglich ist.</p>
<p>Artikel 10 – Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte</p> <p>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 Übereinkunft zum Schutz von Werken der Literatur und Kunst vom 24. Juli 1971, dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Urheberrechtsvertrag festgelegt sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte, wenn diese Handlungen vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben.</p> <p>2 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um Verletzungen verwandter Schutzrechte, wie sie im Recht dieser Vertragspartei aufgrund ihrer</p>	<p>Gesetz über Urheberrecht und verwandte Schutzrechte, Stand Dezember 2008 ("UrhG"):</p> <p>§ 106 UrhG</p> <p>Unerlaubte Verwertung urheberrechtlich geschützter Werke</p> <p>(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>§ 107 UrhG</p> <p>Unzulässiges Anbringen der Urheberbezeichnung</p> <p>(1) Wer</p> <p>1. auf dem Original eines Werkes der bildenden Künste die Urheberbezeichnung (§ 10 Abs. 1) ohne Einwilligung des Urhebers anbringt oder ein derart bezeichnetes Original verbreitet,</p>

<p>Verpflichtungen nach dem Internationalen Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen (Abkommen von Rom), dem Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums und dem WIPO-Vertrag über Darbietungen und Tonträger festgelegt sind, mit Ausnahme der nach diesen Übereinkünften verliehenen Urheberpersönlichkeitsrechte, wenn diese Handlungen vorsätzlich, in gewerbsmäßigem Umfang und mittels eines Computersystems begangen werden, nach ihrem innerstaatlichen Recht als Straftaten zu umschreiben.</p> <p>3 Eine Vertragspartei kann sich das Recht vorbehalten, eine strafrechtliche Verantwortlichkeit nach den Absätzen 1 und 2 unter einer begrenzten Zahl von Umständen nicht vorzusehen, sofern andere wirksame Abhilfen zur Verfügung stehen und dieser Vorbehalt die internationalen Verpflichtungen dieser Vertragspartei aus den in den Absätzen 1 und 2 genannten völkerrechtlichen Übereinkünften nicht beeinträchtigt.</p>	<p>2. auf einem Vervielfältigungsstück, einer Bearbeitung oder Umgestaltung eines Werkes der bildenden Künste die Urheberbezeichnung (§ 10 Abs. 1) auf eine Art anbringt, die dem Vervielfältigungsstück, der Bearbeitung oder Umgestaltung den Anschein eines Originals gibt, oder ein derart bezeichnetes Vervielfältigungsstück, eine solche Bearbeitung oder Umgestaltung verbreitet,</p> <p>wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.</p> <p>(2) Der Versuch ist strafbar.</p> <p>§ 108 UrhG</p> <p>Unerlaubte Eingriffe in verwandte Schutzrechte</p> <p>(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten</p> <ol style="list-style-type: none"> 1. eine wissenschaftliche Ausgabe (§ 70) oder eine Bearbeitung oder Umgestaltung einer solchen Ausgabe vervielfältigt, verbreitet oder öffentlich wiedergibt, 2. ein nachgelassenes Werk oder eine Bearbeitung oder Umgestaltung eines solchen Werkes entgegen § 71 verwertet, 3. ein Lichtbild (§ 72) oder eine Bearbeitung oder Umgestaltung eines Lichtbildes vervielfältigt, verbreitet oder öffentlich wiedergibt, 4. die Darbietung eines ausübenden Künstlers entgegen den § 77 Abs. 1 oder Abs. 2 Satz 1, § 78 Abs. 1 verwertet, 5. einen Tonträger entgegen § 85 verwertet, 6. eine Funksendung entgegen § 87 verwertet, 7. einen Bildträger oder Bild- und Tonträger entgegen §§ 94 oder 95 in Verbindung mit § 94 verwertet, 8. eine Datenbank entgegen § 87b Abs. 1 verwertet, <p>wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p>
---	---

§ 108a UrhG

Gewerbsmäßige unerlaubte Verwertung

(1) Handelt der Täter in den Fällen der §§ 106 bis 108 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(2) Der Versuch ist strafbar.

§ 108b UrhG

Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen

(1) Wer

1. in der Absicht, sich oder einem Dritten den Zugang zu einem nach diesem Gesetz geschützten Werk oder einem anderen nach diesem Gesetz geschützten Schutzgegenstand oder deren Nutzung zu ermöglichen, eine wirksame technische Maßnahme ohne Zustimmung des Rechtsinhabers umgeht oder

2. wissentlich unbefugt

a) eine von Rechtsinhabern stammende Information für die Rechtewahrnehmung entfernt oder verändert, wenn irgendeine der betreffenden Informationen an einem Vervielfältigungsstück eines Werkes oder eines sonstigen Schutzgegenstandes angebracht ist oder im Zusammenhang mit der öffentlichen Wiedergabe eines solchen Werkes oder Schutzgegenstandes erscheint, oder

b) ein Werk oder einen sonstigen Schutzgegenstand, bei dem eine Information für die Rechtewahrnehmung unbefugt entfernt oder geändert wurde, verbreitet, zur Verbreitung einführt, sendet, öffentlich wiedergibt oder öffentlich zugänglich macht

und dadurch wenigstens leichtfertig die Verletzung von Urheberrechten oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert oder verschleiert,

wird, wenn die Tat nicht ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer entgegen § 95a Abs. 3 eine Vorrichtung, ein Erzeugnis oder

	<p>einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet.</p> <p>(3) Handelt der Täter in den Fällen des Absatzes 1 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.</p>
<p>Artikel 11 – Versuch und Beihilfe oder Anstiftung</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die vorsätzliche Beihilfe oder Anstiftung zur Begehung einer nach den Artikeln 2 bis 10 umschriebenen Straftat mit dem Vorsatz, dass eine solche Straftat begangen werde, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.</p> <p>2 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Versuch der Begehung einer nach den Artikeln 3 bis 5 sowie 7, 8 und 9 Absatz 1 Buchstaben a und c umschriebenen Straftat, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.</p> <p>3 Jede Vertragspartei kann sich das Recht vorbehalten, Absatz 2 ganz oder teilweise nicht anzuwenden.</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 22 StGB</p> <p>Begriffsbestimmung</p> <p>Eine Straftat versucht, wer nach seiner Vorstellung von der Tat zur Verwirklichung des Tatbestandes unmittelbar ansetzt.</p> <p>§ 23 StGB</p> <p>Strafbarkeit des Versuchs</p> <p>(1) Der Versuch eines Verbrechens ist stets strafbar, der Versuch eines Vergehens nur dann, wenn das Gesetz es ausdrücklich bestimmt.</p> <p>(2) Der Versuch kann milder bestraft werden als die vollendete Tat (§ 49 Abs. 1).</p> <p>(3) Hat der Täter aus grobem Unverstand verkannt, daß der Versuch nach der Art des Gegenstandes, an dem, oder des Mittels, mit dem die Tat begangen werden sollte, überhaupt nicht zur Vollendung führen konnte, so kann das Gericht von Strafe absehen oder die Strafe nach seinem Ermessen mildern (§ 49 Abs. 2).</p> <p>§ 24 StGB</p> <p>Rücktritt</p> <p>(1) Wegen Versuchs wird nicht bestraft, wer freiwillig die weitere Ausführung der Tat aufgibt oder deren Vollendung verhindert. Wird die Tat ohne Zutun des Zurücktretenden nicht vollendet, so wird er straflos, wenn er sich freiwillig und ernsthaft bemüht, die Vollendung zu verhindern.</p> <p>(2) Sind an der Tat mehrere beteiligt, so wird wegen Versuchs nicht bestraft, wer freiwillig die Vollendung verhindert. Jedoch genügt zu seiner Straflosigkeit sein freiwilliges und ernsthaftes Bemühen, die Vollendung der Tat zu verhindern, wenn sie ohne sein Zutun</p>

	<p>nicht vollendet oder unabhängig von seinem früheren Tatbeitrag begangen wird.</p> <p>§ 26 StGB</p> <p>Anstiftung</p> <p>Als Anstifter wird gleich einem Täter bestraft, wer vorsätzlich einen anderen zu dessen vorsätzlich begangener rechtswidriger Tat bestimmt hat.</p> <p>§ 27 StGB</p> <p>Beihilfe</p> <p>(1) Als Gehilfe wird bestraft, wer vorsätzlich einem anderen zu dessen vorsätzlich begangener rechtswidriger Tat Hilfe geleistet hat.</p> <p>(2) Die Strafe für den Gehilfen richtet sich nach der Strafdrohung für den Täter. Sie ist nach § 49 Abs. 1 zu mildern.</p>
<p>Artikel 12 – Verantwortlichkeit juristischer Personen</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass juristische Personen für eine nach diesem Übereinkommen umschriebene Straftat verantwortlich gemacht werden können, die zu ihren Gunsten von einer natürlichen Person begangen wird, die entweder allein oder als Teil eines Organs der juristischen Person handelt und die eine Führungsposition innerhalb der juristischen Person innehat aufgrund</p> <ul style="list-style-type: none"> a einer Vertretungsmacht für die juristische Person; b einer Befugnis, Entscheidungen im Namen der juristischen Person zu treffen; c einer Kontrollbefugnis innerhalb der juristischen Person. <p>2 Neben den in Absatz 1 bereits vorgesehenen Fällen trifft jede</p>	<p>Gesetz über Ordnungswidrigkeiten, Stand Juli 2009 ("OWiG"):</p> <p>§ 30 OWiG</p> <p>Geldbuße gegen juristische Personen und Personenvereinigungen</p> <p>(1) Hat jemand</p> <ul style="list-style-type: none"> 1. als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs, 2. als Vorstand eines nicht rechtsfähigen Vereins oder als Mitglied eines solchen Vorstandes, 3. als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft, 4. als Generalbevollmächtigter oder in leitender Stellung als Prokurist oder Handlungsbevollmächtigter einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung oder 5. als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung verantwortlich handelt, wozu auch die Überwachung der Geschäftsführung oder die

<p>Vertragspartei die erforderlichen Maßnahmen, um sicherzustellen, dass eine juristische Person verantwortlich gemacht werden kann, wenn mangelnde Überwachung oder Kontrolle durch eine in Absatz 1 genannte natürliche Person die Begehung einer nach diesem Übereinkommen umschriebenen Straftat zugunsten der juristischen Person durch eine ihr unterstellte natürliche Person ermöglicht hat.</p> <p>3 Vorbehaltlich der Rechtsgrundsätze der Vertragspartei kann die Verantwortlichkeit einer juristischen Person straf-, zivil- oder verwaltungsrechtlicher Art sein.</p> <p>4 Diese Verantwortlichkeit berührt nicht die strafrechtliche Verantwortlichkeit der natürlichen Personen, welche die Straftat begangen haben.</p>	<p>sonstige Ausübung von Kontrollbefugnissen in leitender Stellung gehört, eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.</p> <p>(2) Die Geldbuße beträgt</p> <ol style="list-style-type: none"> 1. im Falle einer vorsätzlichen Straftat bis zu einer Million Euro, 2. im Falle einer fahrlässigen Straftat bis zu fünfhunderttausend Euro. <p>Im Falle einer Ordnungswidrigkeit bestimmt sich das Höchstmaß der Geldbuße nach dem für die Ordnungswidrigkeit angedrohten Höchstmaß der Geldbuße. Satz 2 gilt auch im Falle einer Tat, die gleichzeitig Straftat und Ordnungswidrigkeit ist, wenn das für die Ordnungswidrigkeit angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.</p> <p>(3) § 17 Abs. 4 und § 18 gelten entsprechend.</p> <p>(4) Wird wegen der Straftat oder Ordnungswidrigkeit ein Straf- oder Bußgeldverfahren nicht eingeleitet oder wird es eingestellt oder wird von Strafe abgesehen, so kann die Geldbuße selbständig festgesetzt werden. Durch Gesetz kann bestimmt werden, daß die Geldbuße auch in weiteren Fällen selbständig festgesetzt werden kann. Die selbständige Festsetzung einer Geldbuße gegen die juristische Person oder Personenvereinigung ist jedoch ausgeschlossen, wenn die Straftat oder Ordnungswidrigkeit aus rechtlichen Gründen nicht verfolgt werden kann; § 33 Abs. 1 Satz 2 bleibt unberührt.</p> <p>(5) Die Festsetzung einer Geldbuße gegen die juristische Person oder Personenvereinigung schließt es aus, gegen sie wegen derselben Tat den Verfall nach den §§ 73 oder 73a des Strafgesetzbuches oder nach § 29a anzuordnen.</p> <p>§ 130 OWiG</p> <p>Verletzung der Aufsichtspflicht in Betrieben und Unternehmen</p> <p>(1) Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterläßt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn</p>
---	--

	<p>eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.</p> <p>(2) Betrieb oder Unternehmen im Sinne des Absatzes 1 ist auch das öffentliche Unternehmen.</p> <p>(3) Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. Ist die Pflichtverletzung mit Geldbuße bedroht, so bestimmt sich das Höchstmaß der Geldbuße wegen der Aufsichtspflichtverletzung nach dem für die Pflichtverletzung angedrohten Höchstmaß der Geldbuße. Satz 2 gilt auch im Falle einer Pflichtverletzung, die gleichzeitig mit Strafe und Geldbuße bedroht ist, wenn das für die Pflichtverletzung angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.</p>
<p>Artikel 13 – Sanktionen und Maßnahmen</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass die nach den Artikeln 2 bis 11 umschriebenen Straftaten mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen, einschließlich Freiheitsentziehung, bedroht werden.</p> <p>2 Jede Vertragspartei stellt sicher, dass juristische Personen, die nach Artikel 12 verantwortlich gemacht werden, wirksamen, verhältnismäßigen und abschreckenden strafrechtlichen oder nichtstrafrechtlichen Sanktionen oder Maßnahmen, einschließlich Geldsanktionen, unterliegen.</p>	<p>Artikel 13 Abs. 1 wird berücksichtigt durch die oben genannten Normen (§§ 202a, 202b, 202c, 263a, 269, 303a, 303a StGB sowie §§ 106, 107, 108, 108a, 108b UrhG).</p> <p>Artikel 13 Abs. 2 wird berücksichtigt durch § 30 OWiG (siehe oben Artikel 12).</p>
<p>Abschnitt 2 – Verfahrensrecht</p>	
<p>Artikel 14 – Geltungsbereich verfahrensrechtlicher Bestimmungen</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um die Befugnisse und Verfahren zu schaffen,</p>	<p>Siehe unten Artikel 16 bis 21.</p>

<p>die in diesem Abschnitt für die Zwecke spezifischer strafrechtlicher Ermittlungen oder Verfahren vorgesehen sind.</p> <p>2 Sofern in Artikel 21 nichts anderes vorgesehen ist, wendet jede Vertragspartei die in Absatz 1 bezeichneten Befugnisse und Verfahren an in Bezug auf</p> <ul style="list-style-type: none"> a die nach den Artikeln 2 bis 11 umschriebenen Straftaten; b andere mittels eines Computersystems begangene Straftaten; c die Erhebung von in elektronischer Form vorhandenem Beweismaterial für eine Straftat. <p>3 a Jede Vertragspartei kann sich das Recht vorbehalten, die in Artikel 20 bezeichneten Maßnahmen nur auf Straftaten oder Kategorien von Straftaten anzuwenden, die in dem Vorbehalt bezeichnet sind; die Reihe dieser Straftaten oder Kategorien von Straftaten darf nicht enger gefasst sein als die Reihe der Straftaten, auf die sie die in Artikel 21 bezeichneten Maßnahmen anwendet. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt zu beschränken, damit die in Artikel 20 bezeichnete Maßnahme im weitesten Umfang angewendet werden kann.</p> <p>b Kann eine Vertragspartei aufgrund von Beschränkungen in ihren Rechtsvorschriften, die im Zeitpunkt der Annahme dieses Übereinkommens in Kraft sind, die in den Artikeln 20 und 21 bezeichneten Maßnahmen nicht auf Kommunikationen anwenden, die innerhalb eines Computersystems eines Diensteanbieters übermittelt werden, das</p> <ul style="list-style-type: none"> i für eine geschlossene Nutzergruppe betrieben wird 	
--	--

<p>und</p> <p>ii sich keiner öffentlichen Kommunikationsnetze bedient und nicht mit einem anderen öffentlichen oder privaten Computersystem verbunden ist,</p> <p>so kann diese Vertragspartei sich das Recht vorbehalten, diese Maßnahmen auf solche Kommunikationen nicht anzuwenden. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt zu beschränken, damit die in den Artikeln 20 und 21 bezeichneten Maßnahmen im weitesten Umfang angewendet werden können.</p>	
<p>Artikel 15 – Bedingungen und Garantien</p> <p>1 Jede Vertragspartei stellt sicher, dass für die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats von 1950 zum Schutz der Menschenrechte und Grundfreiheiten, dem Internationalen Pakt der Vereinten Nationen von 1966 über bürgerliche und politische Rechte und anderen anwendbaren völkerrechtlichen Übereinkünften auf dem Gebiet der Menschenrechte ergeben und zu denen der Grundsatz der Verhältnismäßigkeit gehören muss.</p> <p>2 Diese Bedingungen und Garantien umfassen, soweit dies in Anbetracht der Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem eine gerichtliche oder sonstige unabhängige Kontrolle, eine Begründung der Anwendung</p>	<p>Siehe unten Artikel 16 bis 21.</p>

<p>sowie die Begrenzung des Umfangs und der Dauer der Befugnis oder des Verfahrens.</p> <p>3 Soweit es mit dem öffentlichen Interesse, insbesondere mit einer geordneten Rechtspflege, vereinbar ist, berücksichtigt jede Vertragspartei die Auswirkungen der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter.</p>	
<p>Artikel 16 – Umgehende Sicherung gespeicherter Computerdaten</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.</p> <p>2 Führt eine Vertragspartei Absatz 1 so durch, dass eine Person im Wege einer Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, sicherzustellen, so trifft diese Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen, um diese Person zu verpflichten, die Unversehrtheit dieser Computerdaten so lange wie notwendig, längstens aber neunzig Tage, zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschließend verlängert werden kann.</p> <p>3 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Verwahrer oder eine andere Person,</p>	<p>Strafprozessordnung, Stand Juli 2009 (“StPO”):</p> <p>Im Hinblick auf Computerdaten wird Artikel 16 durch die §§ 94, 95 und 98 StPO berücksichtigt.</p> <p>§ 94 StPO</p> <p>(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.</p> <p>(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.</p> <p>(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.</p> <p>§ 95 StPO</p> <p>(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.</p> <p>(2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.</p> <p>§ 98 StPO</p> <p>(1) Beschlagnahmen dürfen nur durch das Gericht, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. Die Beschlagnahme nach § 97 Abs. 5 Satz 2 in den Räumen einer Redaktion, eines Verlages, einer Druckerei oder einer</p>

<p>welche die Computerdaten zu sichern hat, zu verpflichten, die Durchführung dieser Verfahren für den nach ihrem innerstaatlichen Recht vorgesehenen Zeitraum vertraulich zu behandeln.</p> <p>4 Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.</p>	<p>Rundfunkanstalt darf nur durch das Gericht angeordnet werden.</p> <p>(2) Der Beamte, der einen Gegenstand ohne gerichtliche Anordnung beschlagnahmt hat, soll binnen drei Tagen die gerichtliche Bestätigung beantragen, wenn bei der Beschlagnahme weder der davon Betroffene noch ein erwachsener Angehöriger anwesend war oder wenn der Betroffene und im Falle seiner Abwesenheit ein erwachsener Angehöriger des Betroffenen gegen die Beschlagnahme ausdrücklichen Widerspruch erhoben hat. Der Betroffene kann jederzeit die gerichtliche Entscheidung beantragen. Die Zuständigkeit des Gerichts bestimmt sich nach § 162. Der Betroffene kann den Antrag auch bei dem Amtsgericht einreichen, in dessen Bezirk die Beschlagnahme stattgefunden hat; dieses leitet den Antrag dem zuständigen Gericht zu. Der Betroffene ist über seine Rechte zu belehren.</p> <p>(3) Ist nach erhobener öffentlicher Klage die Beschlagnahme durch die Staatsanwaltschaft oder eine ihrer Ermittlungspersonen erfolgt, so ist binnen drei Tagen dem Gericht von der Beschlagnahme Anzeige zu machen; die beschlagnahmten Gegenstände sind ihm zur Verfügung zu stellen.</p> <p>(4) Wird eine Beschlagnahme in einem Dienstgebäude oder einer nicht allgemein zugänglichen Einrichtung oder Anlage der Bundeswehr erforderlich, so wird die vorgesetzte Dienststelle der Bundeswehr um ihre Durchführung ersucht. Die ersuchende Stelle ist zur Mitwirkung berechtigt. Des Ersuchens bedarf es nicht, wenn die Beschlagnahme in Räumen vorzunehmen ist, die ausschließlich von anderen Personen als Soldaten bewohnt werden.</p> <p>Im Hinblick auf Verkehrsdaten wird Artikel 16 durch § 100g StPO umgesetzt.</p> <p>§ 100g StPO</p> <p>(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer</p> <ol style="list-style-type: none"> 1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder 2. eine Straftat mittels Telekommunikation begangen hat, <p>so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des</p>
--	---

Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.

(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(3) Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.

(4) Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:

1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;

2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstrafat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;

4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren.

§ 100a StPO

(1) [...]

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

	<p>§ 100b StPO</p> <p>(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.</p> <p>(2) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:</p> <ol style="list-style-type: none"> 1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, 2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, 3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes. <p>(3) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Abs. 2 gilt entsprechend.</p> <p>(4) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.</p> <p>(5) [...]</p>
<p>Artikel 17 – Umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten</p> <p>1 Jede Vertragspartei trifft in Bezug auf Verkehrsdaten, die nach Artikel 16 zu sichern sind, die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen</p>	<p>Umgesetzt durch § 100g StPO (siehe oben Artikel 16).</p>

<p>a dass die umgehende Sicherung von Verkehrsdaten unabhängig davon möglich ist, ob ein oder mehrere Diensteanbieter an der Übermittlung dieser Kommunikation beteiligt waren, und</p> <p>b dass Verkehrsdaten in einem solchen Umfang umgehend an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, dass die Vertragspartei die Diensteanbieter und den Weg feststellen kann, auf dem die Kommunikation übermittelt wurde.</p> <p>2 Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.</p>	
<p>Artikel 18 – Anordnung der Herausgabe</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen,</p> <p>a dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und</p> <p>b dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat.</p> <p>2 Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.</p>	<p>Artikel 18 Abs. 1 lit. a wird durch § 95 der Strafprozessordnung („StPO“, Stand Juli 2009) berücksichtigt:</p> <p>§ 95 StPO</p> <p>(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.</p> <p>(2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.</p> <p>Artikel 18 Abs. 1 lit. b wird durch die §§ 112 und 113 des Telekommunikationsgesetzes („TKG“, Stand Februar 2010) umgesetzt:</p> <p>§ 112 TKG Automatisiertes Auskunftsverfahren</p> <p>(1) Wer Telekommunikationsdienste für die Öffentlichkeit erbringt, hat die nach § 111 Abs. 1 Satz 1, 3 und 4 und Abs. 2 erhobenen Daten unverzüglich in Kundendateien zu speichern, in die auch Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere Anbieter von Telekommunikationsdiensten vergeben werden, sowie bei portierten Rufnummern die</p>

<p>3 Im Sinne dieses Artikels bedeutet der Ausdruck „Bestandsdaten“ alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:</p> <p>a die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dauer des Dienstes;</p> <p>b die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;</p> <p>c andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.</p>	<p>aktuelle Portierungskennung aufzunehmen sind. Für die Berichtigung und Löschung der in den Kundendateien gespeicherten Daten gilt § 111 Abs. 1 Satz 4 und Abs. 4 entsprechend. In Fällen portierter Rufnummern sind die Rufnummer und die zugehörige Portierungskennung erst nach Ablauf des Jahres zu löschen, das dem Zeitpunkt folgt, zu dem die Rufnummer wieder an den Netzbetreiber zurückgegeben wurde, dem sie ursprünglich zugeteilt worden war. Der Verpflichtete hat zu gewährleisten, dass</p> <ol style="list-style-type: none"> 1. die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann, 2. der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichkeitsfunktion erfolgen kann. <p>Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können. Die Bundesnetzagentur darf Daten aus den Kundendateien nur abrufen, soweit die Kenntnis der Daten erforderlich ist</p> <ol style="list-style-type: none"> 1. für die Verfolgung von Ordnungswidrigkeiten nach diesem Gesetz oder nach dem Gesetz gegen den unlauteren Wettbewerb, 2. für die Erledigung von Auskunftersuchen der in Absatz 2 genannten Stellen. <p>Die ersuchende Stelle prüft unverzüglich, inwieweit sie die als Antwort übermittelten Daten benötigt, nicht benötigte Daten löscht sie unverzüglich; dies gilt auch für die Bundesnetzagentur für den Abruf von Daten nach Satz 6 Nr. 1.</p> <p>(2) Auskünfte aus den Kundendateien nach Absatz 1 werden</p> <ol style="list-style-type: none"> 1. den Gerichten und Strafverfolgungsbehörden, 2. den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr, 3. dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes, 4. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst, 5. den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Rufnummer 124 124, 6. der Bundesanstalt für Finanzdienstleistungsaufsicht sowie 7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen
---	--

	<p>Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden.</p> <p>(3) Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen sowie dem Bundesministerium der Verteidigung eine Rechtsverordnung mit Zustimmung des Bundesrates zu erlassen, in der geregelt werden</p> <ol style="list-style-type: none"> 1. die wesentlichen Anforderungen an die technischen Verfahren <ol style="list-style-type: none"> a) zur Übermittlung der Ersuchen an die Bundesnetzagentur, b) zum Abruf der Daten durch die Bundesnetzagentur von den Verpflichteten einschließlich der für die Abfrage zu verwendenden Datenarten und c) zur Übermittlung der Ergebnisse des Abrufs von der Bundesnetzagentur an die ersuchenden Stellen, 2. die zu beachtenden Sicherheitsanforderungen, 3. für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichkeitsfunktion <ol style="list-style-type: none"> a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person, b) die Zeichen, die in der Abfrage verwendet werden dürfen, c) Anforderungen an den Einsatz sprachwissenschaftlicher Verfahren, die gewährleisten, dass unterschiedliche Schreibweisen eines Personen-, Straßen- oder Ortsnamens sowie Abweichungen, die sich aus der Vertauschung, Auslassung oder Hinzufügung von Namensbestandteilen ergeben, in die Suche und das Suchergebnis einbezogen werden, d) die zulässige Menge der an die Bundesnetzagentur zu übermittelnden Antwortdatensätze sowie 4. wer abweichend von Absatz 1 Satz 1 aus Gründen der Verhältnismäßigkeit keine Kundendateien für das automatisierte Auskunftsverfahren vorhalten muss; in diesen Fällen gilt § 111 Abs. 1 Satz 5 entsprechend. <p>Im Übrigen können in der Verordnung auch Einschränkungen der Abfragemöglichkeit für die in Absatz 2 Nr. 5 bis 7 genannten Stellen auf den für diese Stellen erforderlichen Umfang geregelt werden. Die technischen Einzelheiten des automatisierten Abrufverfahrens gibt die Bundesnetzagentur in einer unter Beteiligung der betroffenen Verbände und der berechtigten Stellen zu erarbeitenden Technischen Richtlinie vor, die bei Bedarf an den Stand der Technik anzupassen und von der Bundesnetzagentur in ihrem</p>
--	---

Amtsblatt bekannt zu machen ist. Der Verpflichtete nach Absatz 1 und die berechtigten Stellen haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

(4) Auf Ersuchen der in Absatz 2 genannten Stellen hat die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen die in Absatz 2 genannten Stellen. Die Bundesnetzagentur protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach einem Jahr zu löschen.

(5) Der Verpflichtete nach Absatz 1 hat alle technischen Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für die Erteilung der Auskünfte nach dieser Vorschrift erforderlich sind. Dazu gehören auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte, die Einrichtung eines geeigneten Telekommunikationsanschlusses und die Teilnahme an dem geschlossenen Benutzersystem sowie die laufende Bereitstellung dieser Vorkehrungen nach Maßgaben der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3. Eine Entschädigung für im automatisierten Verfahren erteilte Auskünfte wird den Verpflichteten nicht gewährt.

§ 113 TKG

Manuelles Auskunftsverfahren

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes

	<p>oder des Militärischen Abschirmdienstes erforderlich ist. Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN oder PUK, hat der nach Satz 1 Verpflichtete auf Grund eines Auskunftersuchens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung, der Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, § 8 Abs. 1 des Bundesverfassungsschutzgesetzes, der entsprechenden Bestimmungen der Landesverfassungsschutzgesetze, § 2 Abs. 1 des BND-Gesetzes oder § 4 Abs. 1 des MAD-Gesetzes zu erteilen; an andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren.</p> <p>(2) Der Verpflichtete nach Absatz 1 hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen.</p>
<p>Artikel 19 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen,</p> <p style="padding-left: 40px;">a ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und</p> <p style="padding-left: 40px;">b einen Computerdatenträger, auf dem Computerdaten gespeichert sein können</p> <p style="padding-left: 40px;">in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.</p> <p>2 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in</p>	<p>Artikel 19 Abs. 1 und Abs. 3 werden durch die §§ 94, 95, 102, 103, 105, 161 und 163 der Strafprozessordnung („StPO“, Stand Juli 2009) berücksichtigt:</p> <p>§ 94 StPO</p> <p>(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.</p> <p>(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.</p> <p>(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.</p> <p>§ 95 StPO</p> <p>(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.</p> <p>(2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.</p>

<p>ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.</p> <p>3 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, Computerdaten, auf die nach Absatz 1 oder 2 Zugriff genommen wurde, zu beschlagnahmen oder in ähnlicher Weise sicherzustellen. Diese Maßnahmen umfassen die Befugnis,</p> <p>a ein Computersystem oder einen Teil davon oder einen Computerdatenträger zu beschlagnahmen oder in ähnlicher Weise sicherzustellen;</p> <p>b eine Kopie dieser Computerdaten anzufertigen und zurückzubehalten;</p> <p>c die Unversehrtheit der einschlägigen gespeicherten Computerdaten zu erhalten;</p> <p>d diese Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen.</p> <p>4 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen, dass jede Person, die Kenntnisse über die Funktionsweise des Computersystems oder über Maßnahmen zum Schutz der darin enthaltenen Daten hat, in vernünftigem Maß die notwendigen Auskünfte zu erteilen hat, um die Durchführung der in den Absätzen 1 und 2 genannten Maßnahmen zu ermöglichen.</p> <p>5 Die Befugnisse und Verfahren nach diesem Artikel unterliegen den</p>	<p>§ 102 StPO</p> <p>Bei dem, welcher als Täter oder Teilnehmer einer Straftat oder der Begünstigung, Strafvereitelung oder Hehlerei verdächtig ist, kann eine Durchsuchung der Wohnung und anderer Räume sowie seiner Person und der ihm gehörenden Sachen sowohl zum Zweck seiner Ergreifung als auch dann vorgenommen werden, wenn zu vermuten ist, daß die Durchsuchung zur Auffindung von Beweismitteln führen werde.</p> <p>§ 103 StPO</p> <p>(1) Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet. Zum Zwecke der Ergreifung eines Beschuldigten, der dringend verdächtig ist, eine Straftat nach § 89a des Strafgesetzbuchs oder nach § 129a, auch in Verbindung mit § 129b Abs. 1, des Strafgesetzbuches oder eine der in dieser Vorschrift bezeichneten Straftaten begangen zu haben, ist eine Durchsuchung von Wohnungen und anderen Räumen auch zulässig, wenn diese sich in einem Gebäude befinden, von dem auf Grund von Tatsachen anzunehmen ist, daß sich der Beschuldigte in ihm aufhält.</p> <p>(2) Die Beschränkungen des Absatzes 1 Satz 1 gelten nicht für Räume, in denen der Beschuldigte ergriffen worden ist oder die er während der Verfolgung betreten hat.</p> <p>§ 105 StPO</p> <p>(1) Durchsuchungen dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. Durchsuchungen nach § 103 Abs. 1 Satz 2 ordnet der Richter an; die Staatsanwaltschaft ist hierzu befugt, wenn Gefahr im Verzug ist.</p> <p>(2) Wenn eine Durchsuchung der Wohnung, der Geschäftsräume oder des befriedeten Besitztums ohne Beisein des Richters oder des Staatsanwalts stattfindet, so sind, wenn möglich, ein Gemeindebeamter oder zwei Mitglieder der Gemeinde, in deren Bezirk die Durchsuchung erfolgt, zuzuziehen. Die als Gemeindemitglieder zugezogenen Personen dürfen nicht Polizeibeamte oder Ermittlungspersonen der Staatsanwaltschaft sein.</p> <p>(3) Wird eine Durchsuchung in einem Dienstgebäude oder einer nicht allgemein zugänglichen Einrichtung oder Anlage der Bundeswehr erforderlich, so wird die</p>
--	--

Artikeln 14 und 15.

vorgesetzte Dienststelle der Bundeswehr um ihre Durchführung ersucht. Die ersuchende Stelle ist zur Mitwirkung berechtigt. Des Ersuchens bedarf es nicht, wenn die Durchsuchung von Räumen vorzunehmen ist, die ausschließlich von anderen Personen als Soldaten bewohnt werden.

§ 161 StPO

(1) Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und in diesem Falle befugt, von allen Behörden Auskunft zu verlangen.

(2) Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweis Zwecken im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen. § 100d Abs. 5 Nr. 3 bleibt unberührt.

(3) In oder aus einer Wohnung erlangte personenbezogene Daten aus einem Einsatz technischer Mittel zur Eigensicherung im Zuge nicht offener Ermittlungen auf polizeirechtlicher Grundlage dürfen unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu Beweis Zwecken nur verwendet werden (Artikel 13 Abs. 5 des Grundgesetzes), wenn das Amtsgericht (§ 162 Abs. 1), in dessen Bezirk die anordnende Stelle ihren Sitz hat, die Rechtmäßigkeit der Maßnahme festgestellt hat; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen.

§ 163 StPO

(1) Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. Zu diesem Zweck sind sie befugt, alle Behörden um Auskunft zu ersuchen, bei Gefahr im Verzug auch, die Auskunft zu verlangen, sowie Ermittlungen jeder Art vorzunehmen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln.

(2) Die Behörden und Beamten des Polizeidienstes übersenden ihre Verhandlungen ohne Verzug der Staatsanwaltschaft. Erscheint die schleunige Vornahme richterlicher Untersuchungshandlungen erforderlich, so kann die Übersendung unmittelbar an das

	<p>Amtsgericht erfolgen.</p> <p>(3) Bei der Vernehmung eines Zeugen durch Beamte des Polizeidienstes sind § 52 Absatz 3, § 55 Absatz 2, § 57 Satz 1 und die §§ 58, 58a, 68 bis 69 entsprechend anzuwenden. Über eine Gestattung nach § 68 Absatz 3 Satz 1 und über die Beiordnung eines Zeugenbeistands entscheidet die Staatsanwaltschaft; im Übrigen trifft die erforderlichen Entscheidungen die die Vernehmung leitende Person. Bei Entscheidungen durch Beamte des Polizeidienstes nach § 68b Absatz 1 Satz 3 gilt § 161a Absatz 3 Satz 2 bis 4 entsprechend. Für die Belehrung des Sachverständigen durch Beamte des Polizeidienstes gelten § 52 Absatz 3 und § 55 Absatz 2 entsprechend. In den Fällen des § 81c Absatz 3 Satz 1 und 2 gilt § 52 Absatz 3 auch bei Untersuchungen durch Beamte des Polizeidienstes sinngemäß.</p> <p>Artikel 19 Abs. 2 wird umgesetzt durch § 110 Abs. 3 der Strafprozessordnung („StPO“, Stand Juli 2009):</p> <p>§ 110 StPO</p> <p>(1) Die Durchsicht der Papiere des von der Durchsuchung Betroffenen steht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zu.</p> <p>(2) Im Übrigen sind Beamte zur Durchsicht der aufgefundenen Papiere nur dann befugt, wenn der Inhaber die Durchsicht genehmigt. Andernfalls haben sie die Papiere, deren Durchsicht sie für geboten erachten, in einem Umschlag, der in Gegenwart des Inhabers mit dem Amtssiegel zu verschließen ist, an die Staatsanwaltschaft abzuliefern.</p> <p>(3) Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.</p>
<p>Artikel 20 – Erhebung von Verkehrsdaten in Echtzeit</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen,</p>	<p>Strafprozessordnung, 2009:</p> <p>§ 100g StPO</p> <p>(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer</p>

<p>a Verkehrsdaten, die mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übermittelten Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und</p>	<p>1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder</p> <p>2. eine Straftat mittels Telekommunikation begangen hat,</p>
<p>b einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten,</p> <p>i solche Verkehrsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder</p> <p>ii bei der Erhebung oder Aufzeichnung solcher Verkehrsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.</p>	<p>so dürfen auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1, § 113a des Telekommunikationsgesetzes) erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Im Falle des Satzes 1 Nr. 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Die Erhebung von Standortdaten in Echtzeit ist nur im Falle des Satzes 1 Nr. 1 zulässig.</p> <p>(2) § 100a Abs. 3 und § 100b Abs. 1 bis 4 Satz 1 gelten entsprechend. Abweichend von § 100b Abs. 2 Satz 2 Nr. 2 genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.</p>
<p>2 Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht treffen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass Verkehrsdaten, die mit bestimmten in ihrem Hoheitsgebiet übermittelten Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.</p>	<p>(3) Erfolgt die Erhebung von Verkehrsdaten nicht beim Telekommunikationsdiensteanbieter, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.</p> <p>(4) Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:</p> <p>1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;</p> <p>2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;</p>
<p>3 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Diensteanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.</p>	<p>3. die jeweils zugrunde liegende Anlassstrafat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;</p> <p>4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;</p> <p>5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren.</p>
<p>4 Die Befugnisse und Verfahren nach diesem Artikel unterliegen den</p>	

Artikeln 14 und 15.

§ 100a StPO

(1) [...]

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

§ 100b StPO

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes.

(3) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Abs. 2 gilt entsprechend.

(4) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.

	(5) [...]
<p>Artikel 21 – Erhebung von Inhaltsdaten in Echtzeit</p> <p>1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden in Bezug auf eine Reihe schwerer Straftaten, die durch ihr innerstaatliches Recht zu bestimmen sind, zu ermächtigen,</p> <p>a inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen und</p> <p>b einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten,</p> <p>i solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder</p> <p>ii bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.</p> <p>2 Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht treffen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.</p>	<p>Strafprozessordnung, 2009:</p> <p>§ 100a StPO</p> <p>(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn</p> <ol style="list-style-type: none"> 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. <p>(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:</p> <ol style="list-style-type: none"> 1. aus dem Strafgesetzbuch: <ol style="list-style-type: none"> a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80 bis 82, 84 bis 86, 87 bis 89a, 94 bis 100a, b) Abgeordnetenbestechung nach § 108e, c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h, d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130, e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4, f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Abs. 2 Nr. 2 und des § 179 Abs. 5 Nr. 2, g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Abs. 1 bis 3, § 184c Abs. 3, h) Mord und Totschlag nach den §§ 211 und 212,

<p>3 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Diensteanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.</p>	<p>i) Straftaten gegen die persönliche Freiheit nach den §§ 232 bis 233a, 234, 234a, 239a und 239b,</p> <p>j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,</p> <p>k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,</p> <p>l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,</p>
<p>4 Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.</p>	<p>m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4,</p> <p>n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,</p> <p>o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,</p> <p>p) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,</p> <p>q) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,</p> <p>r) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,</p> <p>s) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,</p> <p>t) Bestechlichkeit und Bestechung nach den §§ 332 und 334,</p> <p>2. aus der Abgabenordnung:</p> <p>a) Steuerhinterziehung unter den in § 370 Abs. 3 Satz 2 Nr. 5 genannten Voraussetzungen,</p> <p>b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,</p> <p>c) Steuerhehlerei im Falle des § 374 Abs. 2,</p>

3. aus dem Arzneimittelgesetz:

Straftaten nach § 95 Abs. 1 Nr. 2a unter den in § 95 Abs. 3 Satz 2 Nr. 2 Buchstabe b genannten Voraussetzungen,

4. aus dem Asylverfahrensgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Abs. 2,

b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,

6. aus dem Außenwirtschaftsgesetz: Straftaten nach § 34 Abs. 1 bis 6,

7. aus dem Betäubungsmittelgesetz:

a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

8. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,

9. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,

b) Straftaten nach § 22a Abs. 1 bis 3,

10. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

11. aus dem Waffengesetz:

a) Straftaten nach § 51 Abs. 1 bis 3,

b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

§ 100b StPO

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,

2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes.

	<p>(3) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Abs. 2 gilt entsprechend.</p> <p>(4) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.</p> <p>(5) Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet. 1)</p> <p>(6) In den Berichten nach Absatz 5 sind anzugeben:</p> <ol style="list-style-type: none"> 1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Abs. 1 angeordnet worden sind; 2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1, unterschieden nach <ol style="list-style-type: none"> a) Erst- und Verlängerungsanordnungen sowie b) Festnetz-, Mobilfunk- und Internettelekommunikation; 3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2.
<p>Abschnitt 3 – Gerichtsbarkeit</p>	
<p>Artikel 22 – Gerichtsbarkeit</p> <p>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:</p>	<p>Strafgesetzbuch, 2009:</p> <p>§ 3 StGB</p> <p>Geltung für Inlandstaten</p> <p>Das deutsche Strafrecht gilt für Taten, die im Inland begangen werden.</p>

<p>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.</p> <p>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.</p> <p>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 Auslieferungsersuchen gestellt worden ist, nur deshalb nicht an eine andere Vertragspartei ausliefert, weil sie ihre Staatsangehörige ist.</p> <p>4 Dieses Übereinkommen schließt die Ausübung einer Strafgerichtsbarkeit durch eine Vertragspartei nach ihrem innerstaatlichen Recht nicht aus.</p> <p>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.</p>	<p>§ 4 StGB Geltung für Taten auf deutschen Schiffen und Luftfahrzeugen</p> <p>Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für Taten, die auf einem Schiff oder in einem Luftfahrzeug begangen werden, das berechtigt ist, die Bundesflagge oder das Staatszugehörigkeitszeichen der Bundesrepublik Deutschland zu führen.</p> <p>§ 5 StGB Auslandstaten gegen inländische Rechtsgüter</p> <p>Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für folgende Taten, die im Ausland begangen werden:</p> <ol style="list-style-type: none"> 1. Vorbereitung eines Angriffskrieges (§ 80); 2. Hochverrat (§§ 81 bis 83); 3. Gefährdung des demokratischen Rechtsstaates <ol style="list-style-type: none"> a) in den Fällen der §§ 89, 90a Abs. 1 und des § 90b, wenn der Täter Deutscher ist und seine Lebensgrundlage im räumlichen Geltungsbereich dieses Gesetzes hat, und b) in den Fällen der §§ 90 und 90a Abs. 2; 4. Landesverrat und Gefährdung der äußeren Sicherheit (§§ 94 bis 100a); 5. Straftaten gegen die Landesverteidigung <ol style="list-style-type: none"> a) in den Fällen der §§ 109 und 109e bis 109g und b) in den Fällen der §§ 109a, 109d und 109h, wenn der Täter Deutscher ist und seine Lebensgrundlage im räumlichen Geltungsbereich dieses Gesetzes hat; 6. Verschleppung und politische Verdächtigung (§§ 234a, 241a), wenn die Tat sich gegen einen Deutschen richtet, der im Inland seinen Wohnsitz oder gewöhnlichen Aufenthalt hat; 6a. Entziehung eines Kindes in den Fällen des § 235 Abs. 2 Nr. 2, wenn die Tat sich gegen eine Person richtet, die im Inland ihren Wohnsitz oder gewöhnlichen Aufenthalt hat; 7. Verletzung von Betriebs- oder Geschäftsgeheimnissen eines im räumlichen
---	---

	<p>Geltungsbereich dieses Gesetzes liegenden Betriebs, eines Unternehmens, das dort seinen Sitz hat, oder eines Unternehmens mit Sitz im Ausland, das von einem Unternehmen mit Sitz im räumlichen Geltungsbereich dieses Gesetzes abhängig ist und mit diesem einen Konzern bildet;</p> <p>8. Straftaten gegen die sexuelle Selbstbestimmung</p> <p>a) in den Fällen des § 174 Abs. 1 und 3, wenn der Täter und der, gegen den die Tat begangen wird, zur Zeit der Tat Deutsche sind und ihre Lebensgrundlage im Inland haben, und</p> <p>b) in den Fällen der §§ 176 bis 176b und 182, wenn der Täter Deutscher ist;</p> <p>9. Abbruch der Schwangerschaft (§ 218), wenn der Täter zur Zeit der Tat Deutscher ist und seine Lebensgrundlage im räumlichen Geltungsbereich dieses Gesetzes hat;</p> <p>10. falsche uneidliche Aussage, Meineid und falsche Versicherung an Eides Statt (§§ 153 bis 156) in einem Verfahren, das im räumlichen Geltungsbereich dieses Gesetzes bei einem Gericht oder einer anderen deutschen Stelle anhängig ist, die zur Abnahme von Eiden oder eidesstattlichen Versicherungen zuständig ist;</p> <p>11. Straftaten gegen die Umwelt in den Fällen der §§ 324, 326, 330 und 330a, die im Bereich der deutschen ausschließlichen Wirtschaftszone begangen werden, soweit völkerrechtliche Übereinkommen zum Schutze des Meeres ihre Verfolgung als Straftaten gestatten;</p> <p>11a. Straftaten nach § 328 Abs. 2 Nr. 3 und 4, Abs. 4 und 5, auch in Verbindung mit § 330, wenn der Täter zur Zeit der Tat Deutscher ist;</p> <p>12. Taten, die ein deutscher Amtsträger oder für den öffentlichen Dienst besonders Verpflichteter während eines dienstlichen Aufenthalts oder in Beziehung auf den Dienst begeht;</p> <p>13. Taten, die ein Ausländer als Amtsträger oder für den öffentlichen Dienst besonders Verpflichteter begeht;</p> <p>14. Taten, die jemand gegen einen Amtsträger, einen für den öffentlichen Dienst besonders Verpflichteten oder einen Soldaten der Bundeswehr während der Ausübung ihres Dienstes oder in Beziehung auf ihren Dienst begeht;</p> <p>14a. Abgeordnetenbestechung (§ 108e), wenn der Täter zur Zeit der Tat Deutscher ist oder die Tat gegenüber einem Deutschen begangen wird;</p> <p>15. Organ- und Gewebehandel (§ 18 des Transplantationsgesetzes), wenn der Täter zur</p>
--	---

Zeit der Tat Deutscher ist.

§ 6 StGB

Auslandstaten gegen international geschützte Rechtsgüter

Das deutsche Strafrecht gilt weiter, unabhängig vom Recht des Tatorts, für folgende Taten, die im Ausland begangen werden:

1. (weggefallen)
2. Kernenergie-, Sprengstoff- und Strahlungsverbrechen in den Fällen der §§ 307 und 308 Abs. 1 bis 4, des § 309 Abs. 2 und des § 310;
3. Angriffe auf den Luft- und Seeverkehr (§ 316c);
4. Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft sowie Förderung des Menschenhandels (§§ 232 bis 233a);
5. unbefugter Vertrieb von Betäubungsmitteln;
6. Verbreitung pornographischer Schriften in den Fällen der §§ 184a, 184b Abs. 1 bis 3 und § 184c Abs. 1 bis 3, jeweils auch in Verbindung mit § 184d Satz 1;
7. Geld- und Wertpapierfälschung (§§ 146, 151 und 152), Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks (§ 152b Abs. 1 bis 4) sowie deren Vorbereitung (§§ 149, 151, 152 und 152b Abs. 5);
8. Subventionsbetrug (§ 264);
9. Taten, die auf Grund eines für die Bundesrepublik Deutschland verbindlichen zwischenstaatlichen Abkommens auch dann zu verfolgen sind, wenn sie im Ausland begangen werden.

§ 7 StGB

Geltung für Auslandstaten in anderen Fällen

(1) Das deutsche Strafrecht gilt für Taten, die im Ausland gegen einen Deutschen begangen werden, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt.

	<p>(2) Für andere Taten, die im Ausland begangen werden, gilt das deutsche Strafrecht, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Straf Gewalt unterliegt und wenn der Täter</p> <p>1. zur Zeit der Tat Deutscher war oder es nach der Tat geworden ist oder</p> <p>2. zur Zeit der Tat Ausländer war, im Inland betroffen und, obwohl das Auslieferungsgesetz seine Auslieferung nach der Art der Tat zuließe, nicht ausgeliefert wird, weil ein Auslieferungersuchen innerhalb angemessener Frist nicht gestellt oder abgelehnt wird oder die Auslieferung nicht ausführbar ist.</p> <p>§ 8 StGB</p> <p>Zeit der Tat</p> <p>Eine Tat ist zu der Zeit begangen, zu welcher der Täter oder der Teilnehmer gehandelt hat oder im Falle des Unterlassens hätte handeln müssen. Wann der Erfolg eintritt, ist nicht maßgebend.</p> <p>§ 9 StGB</p> <p>Ort der Tat</p> <p>(1) Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte.</p> <p>(2) Die Teilnahme ist sowohl an dem Ort begangen, an dem die Tat begangen ist, als auch an jedem Ort, an dem der Teilnehmer gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem nach seiner Vorstellung die Tat begangen werden sollte. Hat der Teilnehmer an einer Auslandstat im Inland gehandelt, so gilt für die Teilnahme das deutsche Strafrecht, auch wenn die Tat nach dem Recht des Tatorts nicht mit Strafe bedroht ist.</p>
<p>Kapitel III – Internationale Zusammenarbeit Abschnitt 1 – Allgemeine Grundsätze</p>	
<p>Artikel 24 – Auslieferung</p> <p>1 a Dieser Artikel findet auf die Auslieferung zwischen den Vertragsparteien wegen der nach den Artikeln 2 bis 11</p>	<p>Artikel 24 wird berücksichtigt durch die §§ 2 und 3 des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009), soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind:</p>

<p>umschriebenen Straftaten Anwendung, sofern sie nach den Rechtsvorschriften der beiden beteiligten Vertragsparteien mit einer Freiheitsstrafe im Höchstmaß von mindestens einem Jahr oder mit einer schwereren Strafe bedroht sind.</p> <p>b Gilt nach einer Übereinkunft auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften oder nach einem Auslieferungsvertrag einschließlich des Europäischen Auslieferungsübereinkommens (SEV Nr. 24), der zwischen zwei oder mehr Vertragsparteien anwendbar ist, eine andere Mindeststrafe, so findet die nach dieser Übereinkunft oder nach diesem Vertrag vorgesehene Mindeststrafe Anwendung.</p>	<p>§ 2 IRG Grundsatz</p> <p>(1) Ein Ausländer, der in einem ausländischen Staat wegen einer Tat, die dort mit Strafe bedroht ist, verfolgt wird oder verurteilt worden ist, kann diesem Staat auf Ersuchen einer zuständigen Stelle zur Verfolgung oder zur Vollstreckung einer wegen der Tat verhängten Strafe oder sonstigen Sanktion ausgeliefert werden.</p> <p>(2) Ein Ausländer, der in einem ausländischen Staat wegen einer Tat, die dort mit Strafe bedroht ist, verurteilt worden ist, kann einem anderen ausländischen Staat, der die Vollstreckung übernommen hat, auf Ersuchen einer zuständigen Stelle dieses Staates zur Vollstreckung einer wegen der Tat verhängten Strafe oder sonstigen Sanktion ausgeliefert werden.</p> <p>(3) Ausländer im Sinne dieses Gesetzes sind Personen, die nicht Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes sind.</p>
<p>2 Die in Absatz 1 beschriebenen Straftaten gelten als in jeden zwischen den Vertragsparteien bestehenden Auslieferungsvertrag einbezogene der Auslieferung unterliegende Straftaten. Die Vertragsparteien verpflichten sich, diese Straftaten als der Auslieferung unterliegende Straftaten in jeden zwischen ihnen zu schließenden Auslieferungsvertrag aufzunehmen.</p>	<p>§ 3 IRG Auslieferung zur Verfolgung oder zur Vollstreckung</p> <p>(1) Die Auslieferung ist nur zulässig, wenn die Tat auch nach deutschem Recht eine rechtswidrige Tat ist, die den Tatbestand eines Strafgesetzes verwirklicht, oder wenn sie bei sinngemäßer Umstellung des Sachverhalts auch nach deutschem Recht eine solche Tat wäre.</p> <p>(2) Die Auslieferung zur Verfolgung ist nur zulässig, wenn die Tat nach deutschem Recht im Höchstmaß mit Freiheitsstrafe von mindestens einem Jahr bedroht ist oder wenn sie bei sinngemäßer Umstellung des Sachverhalts nach deutschem Recht mit einer solchen Strafe bedroht wäre.</p> <p>(3) Die Auslieferung zur Vollstreckung ist nur zulässig, wenn wegen der Tat die Auslieferung zur Verfolgung zulässig wäre und wenn eine freiheitsentziehende Sanktion zu vollstrecken ist. Sie ist ferner nur zulässig, wenn zu erwarten ist, daß die noch zu vollstreckende freiheitsentziehende Sanktion oder die Summe der noch zu vollstreckenden freiheitsentziehenden Sanktionen mindestens vier Monate beträgt.</p>
<p>3 Erhält eine Vertragspartei, welche die Auslieferung vom Bestehen eines Vertrags abhängig macht, ein Auslieferungersuchen von einer anderen Vertragspartei, mit der sie keinen Auslieferungsvertrag hat, so kann sie dieses Übereinkommen als Rechtsgrundlage für die Auslieferung in Bezug auf die in Absatz 1 bezeichneten Straftaten ansehen.</p>	
<p>4 Vertragsparteien, welche die Auslieferung nicht vom Bestehen eines Vertrags abhängig machen, erkennen unter sich die in Absatz 1 bezeichneten Straftaten als der Auslieferung unterliegende Straftaten an.</p>	
<p>5 Die Auslieferung unterliegt den im Recht der ersuchten</p>	

<p>Vertragspartei oder in den geltenden Auslieferungsverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Auslieferung ablehnen kann.</p> <p>6 Wird die Auslieferung wegen einer in Absatz 1 bezeichneten Straftat allein aufgrund der Staatsangehörigkeit der verfolgten Person oder deswegen abgelehnt, weil die ersuchte Vertragspartei der Auffassung ist, sie habe die Gerichtsbarkeit über die Straftat, so unterbreitet die ersuchte Vertragspartei auf Ersuchen der ersuchenden Vertragspartei den Fall ihren zuständigen Behörden zum Zweck der Strafverfolgung und teilt der ersuchenden Vertragspartei zu gegebener Zeit das endgültige Ergebnis mit. Diese Behörden treffen ihre Entscheidung und betreiben ihre Ermittlungen und ihr Verfahren in derselben Weise wie bei jeder anderen vergleichbaren Straftat nach dem Recht dieser Vertragspartei.</p> <p>7 a Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift jeder Behörde mit, die, falls kein Vertrag besteht, für die Stellung oder Entgegennahme eines Ersuchens um Auslieferung oder vorläufige Verhaftung zuständig ist.</p> <p>b Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.</p>	
<p>Artikel 25 – Allgemeine Grundsätze der Rechtshilfe</p> <p>1 Die Vertragsparteien leisten einander im größtmöglichen Umfang Rechtshilfe 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</p>	<p>Die Grundsätze des Artikel 25 werden von diversen Bestimmungen des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) ganz oder teilweise abgedeckt, u.a. durch die §§ 2 und 3 IRG (siehe oben Artikel 24) und die §§ 59 ff. IRG:</p> <p>§ 59 IRG Zulässigkeit der Rechtshilfe</p>

<p>eine Straftat.</p>	<p>(1) Auf Ersuchen einer zuständigen Stelle eines ausländischen Staates kann sonstige Rechtshilfe in einer strafrechtlichen Angelegenheit geleistet werden.</p>
<p>2 Jede Vertragspartei trifft ferner die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den in den Artikeln 27 bis 35 bezeichneten Verpflichtungen nachzukommen.</p>	<p>(2) Rechtshilfe im Sinne des Absatzes 1 ist jede Unterstützung, die für ein ausländisches Verfahren in einer strafrechtlichen Angelegenheit gewährt wird, unabhängig davon, ob das ausländische Verfahren von einem Gericht oder von einer Behörde betrieben wird und ob die Rechtshilfebehandlung von einem Gericht oder von einer Behörde vorzunehmen ist.</p>
<p>3 In dringenden Fällen kann jede Vertragspartei Rechtshilfeersuchen oder damit in Zusammenhang stehende Mitteilungen durch schnelle Kommunikationsmittel einschließlich Telefax oder elektronischer Post übersenden, soweit diese Mittel einen angemessenen Sicherheits- und Authentisierungsstandard bieten (erforderlichenfalls auch unter Einsatz einer Verschlüsselung) und eine förmliche Bestätigung folgt, wenn die ersuchte Vertragspartei dies verlangt. Die ersuchte Vertragspartei nimmt das Ersuchen entgegen und beantwortet es mit einem dieser schnellen Kommunikationsmittel.</p>	<p>(3) Die Rechtshilfe darf nur geleistet werden, wenn die Voraussetzungen vorliegen, unter denen deutsche Gerichte oder Behörden einander in entsprechenden Fällen Rechtshilfe leisten könnten.</p> <p>§ 60 IRG Leistung der Rechtshilfe Hält die für die Bewilligung der Rechtshilfe zuständige Behörde die Voraussetzungen für die Leistung der Rechtshilfe für gegeben, so ist die für die Leistung der Rechtshilfe zuständige Behörde hieran gebunden. § 61 bleibt unberührt.</p>
<p>4 Soweit in den Artikeln dieses Kapitels nicht ausdrücklich etwas anderes vorgesehen ist, unterliegt die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungen einschließlich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann. Die ersuchte Vertragspartei darf das Recht auf Verweigerung der Rechtshilfe in Bezug auf die in den Artikeln 2 bis 11 bezeichneten Straftaten nicht allein mit der Begründung ausüben, dass das Ersuchen eine Straftat betrifft, die von ihr als fiskalische Straftat angesehen wird.</p>	<p>§ 61 IRG Gerichtliche Entscheidung (1) Hält ein Gericht, das für die Leistung der Rechtshilfe zuständig ist, die Voraussetzungen für die Leistung der Rechtshilfe für nicht gegeben, so begründet es seine Auffassung und holt die Entscheidung des Oberlandesgerichts ein. Das Oberlandesgericht entscheidet ferner auf Antrag der Staatsanwaltschaft bei dem Oberlandesgericht oder im Fall des § 66 auf Antrag desjenigen, der geltend macht, er würde durch die Herausgabe in seinen Rechten verletzt werden, darüber, ob die Voraussetzungen für die Leistung der Rechtshilfe gegeben sind. Für das Verfahren vor dem Oberlandesgericht gelten die §§ 30, 31 Abs. 1, 3 und 4, §§ 32, 33 Abs. 1, 2 und 4, § 38 Abs. 4 Satz 2, § 40 Abs. 1 sowie die Vorschriften des 11. Abschnittes des I. Buches der Strafprozeßordnung mit Ausnahme der §§ 140 bis 143 entsprechend. Für das weitere Verfahren gilt § 42 entsprechend.</p>
<p>5 Darf die ersuchte Vertragspartei nach diesem Kapitel die Rechtshilfe von der Bedingung abhängig machen, dass die beiderseitige Strafbarkeit gegeben ist, so gilt, gleichviel, ob die Straftat nach ihrem Recht in dieselbe Kategorie von Straftaten fällt oder mit dem gleichen Begriff benannt ist wie nach dem Recht der ersuchenden Vertragspartei, diese Bedingung als erfüllt, wenn die Handlung, die der Straftat, derentwegen um Rechtshilfe ersucht wird, zugrunde</p>	<p>(2) Örtlich zuständig sind das Oberlandesgericht und die Staatsanwaltschaft bei dem Oberlandesgericht, in deren Bezirk die Rechtshilfe geleistet werden soll oder geleistet worden ist. Sind Rechtshilfebehandlungen in den Bezirken verschiedener Oberlandesgerichte vorzunehmen oder vorgenommen worden, so richtet sich die Zuständigkeit danach, welches Oberlandesgericht oder, solange noch kein Oberlandesgericht befaßt ist, welche Staatsanwaltschaft bei dem Oberlandesgericht zuerst mit der Sache befaßt wurde.</p>

liegt, nach ihrem Recht eine Straftat darstellt.

(3) Die Entscheidung des Oberlandesgerichts ist für die Gerichte und Behörden, die für die Leistung der Rechtshilfe zuständig sind, bindend.

(4) Die Rechtshilfe darf nicht bewilligt werden, wenn das Oberlandesgericht entschieden hat, daß die Voraussetzungen für die Leistung der Rechtshilfe nicht vorliegen.

§ 62 IRG

Vorübergehende Überstellung in das Ausland für ein ausländisches Verfahren

(1) Wer sich im Geltungsbereich dieses Gesetzes in Untersuchungs- oder Strafhaft befindet oder auf Grund der Anordnung einer freiheitsentziehenden Maßregel der Besserung und Sicherung untergebracht ist, kann an einen ausländischen Staat auf Ersuchen einer zuständigen Stelle dieses Staates für ein dort anhängiges Verfahren als Zeuge zur Vernehmung, zur Gegenüberstellung oder zur Einnahme eines Augenscheins vorübergehend überstellt werden, wenn

1. er sich nach Belehrung zu Protokoll eines Richters damit einverstanden erklärt hat,
2. nicht zu erwarten ist, daß infolge der Überstellung die Freiheitsentziehung verlängert oder der Zweck des Strafverfahrens beeinträchtigt werden wird,
3. gewährleistet ist, daß der Betroffene während der Zeit seiner Überstellung nicht bestraft, einer sonstigen Sanktion unterworfen oder durch Maßnahmen, die nicht auch in seiner Abwesenheit getroffen werden können, verfolgt werden wird und daß er im Fall seiner Freilassung den ersuchenden Staat verlassen darf, und
4. gewährleistet ist, daß der Betroffene unverzüglich nach der Beweiserhebung zurücküberstellt werden wird, es sei denn, daß darauf verzichtet worden ist.

Das Einverständnis (Satz 1 Nr. 1) kann nicht widerrufen werden.

(2) Die Staatsanwaltschaft bei dem Oberlandesgericht bereitet die Überstellung vor und führt sie durch. Örtlich zuständig ist die Staatsanwaltschaft bei dem Oberlandesgericht, in dessen Bezirk die Freiheitsentziehung vollzogen wird.

(3) Die in dem ersuchenden Staat erlittene Freiheitsentziehung wird auf die im Geltungsbereich dieses Gesetzes zu vollziehende Freiheitsentziehung angerechnet. § 37 Abs. 4 gilt entsprechend.

§ 63 IRG

Vorübergehende Überstellung aus dem Ausland für ein ausländisches Verfahren

(1) Wer sich in einem ausländischen Staat in Untersuchungs- oder Strafhaft befindet oder auf Grund der Anordnung einer freiheitsentziehenden Maßregel untergebracht ist, kann für

ein dort anhängiges Verfahren auf Ersuchen einer zuständigen Stelle dieses Staates zu einer Beweiserhebung vorübergehend in den Geltungsbereich dieses Gesetzes übernommen und nach der Beweiserhebung zurücküberstellt werden. Zur Sicherung seiner Rücküberstellung wird der Betroffene in Haft gehalten.

(2) Die Haft wird durch schriftlichen Haftbefehl angeordnet. In dem Haftbefehl sind anzuführen

1. der Betroffene,
2. das Ersuchen um Beweiserhebung in Anwesenheit des Betroffenen sowie
3. der Haftgrund.

(3) Die Haftentscheidung trifft der Richter, der die Rechtshilfehandlung vornehmen soll, oder der Richter bei dem Amtsgericht, in dessen Bezirk die Behörde ihren Sitz hat, welche die Rechtshilfehandlung vornehmen soll. Die Entscheidung ist unanfechtbar.

(4) Die §§ 27, 45 Abs. 4 und § 62 Abs. 2 Satz 1 gelten entsprechend.

§ 64 IRG

Durchbeförderung von Zeugen

(1) Ein Ausländer, der sich in einem ausländischen Staat in Untersuchungs- oder Strafhaft befindet oder auf Grund der Anordnung einer freiheitsentziehenden Maßregel untergebracht ist, kann auf Ersuchen einer zuständigen Stelle als Zeuge zur Vernehmung, zur Gegenüberstellung oder zur Einnahme eines Augenscheins durch den Geltungsbereich dieses Gesetzes in einen dritten Staat befördert und nach der Beweiserhebung zurückbefördert werden.

(2) Zur Sicherung der Durchbeförderung wird der Betroffene in Haft gehalten. Die §§ 27, 30 Abs. 1, §§ 42, 44, 45 Abs. 3 und 4, §§ 47, 63 Abs. 2 gelten entsprechend.

§ 65 IRG

Durchbeförderung zur Vollstreckung

Für die Durchbeförderung eines Ausländers zur Vollstreckung einer Strafe oder sonstigen Sanktion aus dem Staat, in dem er verurteilt worden ist, durch den Geltungsbereich dieses Gesetzes in einen ausländischen Staat, der die Vollstreckung übernommen hat, gelten § 43 Abs. 2 bis 4, §§ 44, 45 und 47 entsprechend mit der Maßgabe, daß das Ersuchen auch von einer zuständigen Stelle des Urteilsstaates gestellt werden kann.

§ 68 IRG

	<p>Rücklieferung</p> <p>(1) Ein Verfolgter, der für ein im Geltungsbereich dieses Gesetzes gegen ihn geführtes Strafverfahren auf Ersuchen unter der Bedingung späterer Rücklieferung vorübergehend ausgeliefert worden ist, wird zum vereinbarten Zeitpunkt an den ersuchten Staat zurückgeliefert, sofern dieser nicht darauf verzichtet. Zuständig für die Anordnung und Durchführung der Rücklieferung ist die Staatsanwaltschaft, die an dem in Satz 1 bezeichneten Strafverfahren beteiligt ist.</p> <p>(2) Gegen den Verfolgten kann durch schriftlichen Haftbefehl die Haft angeordnet werden, wenn die Rücklieferung sonst nicht gewährleistet wäre. In dem Haftbefehl sind anzuführen</p> <ol style="list-style-type: none"> 1. der Verfolgte, 2. der Staat, an den die Rücklieferung erfolgen soll, sowie 3. die Gründe, welche die Haftanordnung rechtfertigen. <p>(3) Die Haftentscheidung trifft das Gericht, das in dem in Absatz 1 Satz 1 bezeichneten Strafverfahren für die Anordnung von freiheitsentziehenden Maßnahmen jeweils zuständig ist. Die Entscheidung ist unanfechtbar.</p> <p>(4) Die §§ 18, 19, 24, 25, 27 und 45 Abs. 4 gelten entsprechend.</p> <p>§ 69 IRG</p> <p>Vorübergehende Überstellung aus dem Ausland für ein deutsches Verfahren</p> <p>(1) Eine in einem ausländischen Staat in Untersuchungs- oder Strafhaft befindliche oder auf Grund der Anordnung einer freiheitsentziehenden Maßregel untergebrachte Person, die einem deutschen Gericht oder einer deutschen Behörde auf Ersuchen als Zeuge zur Vernehmung, zur Gegenüberstellung oder zur Einnahme eines Augenscheins vorübergehend überstellt worden ist, wird während ihres Aufenthalts im Geltungsbereich dieses Gesetzes zur Sicherung ihrer Rücküberstellung in Haft gehalten.</p> <p>(2) Die Haftentscheidung trifft das Gericht, das mit der Sache befaßt ist, im vorbereitenden Verfahren der Richter bei dem Amtsgericht, in dessen Bezirk die das Verfahren führende Staatsanwaltschaft ihren Sitz hat. Die Entscheidung ist unanfechtbar.</p> <p>(3) Die §§ 27, 45 Abs. 4, § 62 Abs. 2 Satz 1, § 63 Abs. 2 gelten entsprechend.</p>
<p>Artikel 26 – Unaufgeforderte Übermittlung von Informationen</p> <p>1 Eine Vertragspartei kann einer anderen Vertragspartei, soweit ihr innerstaatliches Recht es erlaubt und ohne vorheriges Ersuchen,</p>	<p>Artikel 26 wird von den §§ 61a und 92 des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) abgedeckt, soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind:</p>

<p>Informationen übermitteln, die sie im Rahmen eigener Ermittlungen gewonnen hat, wenn sie der Auffassung ist, dass die Übermittlung dieser Informationen der anderen Vertragspartei bei der Einleitung oder Durchführung von Ermittlungen oder Verfahren wegen nach diesem Übereinkommen umschriebener Straftaten helfen oder dazu führen könnte, dass diese Vertragspartei ein Ersuchen um Zusammenarbeit nach diesem Kapitel stellt.</p> <p>2 Vor Übermittlung dieser Informationen kann die übermittelnde Vertragspartei um vertrauliche Behandlung oder um Verwendung nur unter bestimmten Bedingungen ersuchen. Kann die andere Vertragspartei diesem Ersuchen nicht entsprechen, so teilt sie dies der übermittelnden Vertragspartei mit; diese entscheidet dann, ob die Informationen dennoch übermittelt werden sollen. Nimmt die andere Vertragspartei die Informationen unter den vorgeschriebenen Bedingungen an, so ist sie an diese Bedingungen gebunden.</p>	<p>§ 61a IRG Datenübermittlung ohne Ersuchen</p> <p>(1) Gerichte und Staatsanwaltschaften dürfen ohne ein Ersuchen personenbezogene Daten aus strafprozessualen Ermittlungen an öffentliche Stellen anderer Staaten sowie zwischen- und überstaatliche Stellen übermitteln, soweit</p> <ol style="list-style-type: none"> 1. eine Übermittlung ohne Ersuchen an ein deutsches Gericht oder eine deutsche Staatsanwaltschaft zulässig wäre, 2. Tatsachen die Annahme rechtfertigen, dass die Übermittlung erforderlich ist, um <ol style="list-style-type: none"> a) ein Ersuchen des Empfängerstaates um Rechtshilfe in einem Verfahren zur Strafverfolgung oder zur Strafvollstreckung wegen einer im Geltungsbereich dieses Gesetzes im Höchstmaß mit Freiheitsstrafe von mehr als fünf Jahren bedrohten Straftat vorzubereiten und die Voraussetzungen zur Leistung von Rechtshilfe auf Ersuchen vorlägen, wenn ein solches gestellt würde, oder b) eine im Einzelfall bestehende Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, abzuwehren oder eine Straftat der in Buchstabe a genannten Art zu verhindern, und 3. die Stelle, an die die Daten übermittelt werden, für die zu treffende Maßnahme nach Nummer 2 zuständig ist. <p>Ist im Empfängerstaat ein angemessenes Datenschutzniveau gewährleistet, so ist Satz 1 Nr. 2 Buchstabe a mit der Maßgabe anzuwenden, dass an die Stelle einer Straftat, die im Geltungsbereich dieses Gesetzes im Höchstmaß mit Freiheitsstrafe von mehr als fünf Jahren bedroht ist, eine Straftat von erheblicher Bedeutung tritt.</p> <p>(2) Die Übermittlung ist mit der Bedingung zu verbinden, dass</p> <ol style="list-style-type: none"> a) nach dem deutschen Recht geltende Löschungs- oder Lösungsprüffristen einzuhalten sind, b) die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt worden sind, und c) die übermittelten Daten im Falle einer Unterrichtung nach Absatz 4 unverzüglich zu löschen oder zu berichtigen sind. <p>(3) Die Übermittlung unterbleibt, soweit für das Gericht oder die Staatsanwaltschaft offensichtlich ist, dass - auch unter Berücksichtigung des besonderen öffentlichen Interesses an der Datenübermittlung - im Einzelfall schutzwürdige Interessen des Betroffenen an dem Ausschluss der Übermittlung überwiegen; zu den schutzwürdigen</p>
--	--

	<p>Interessen des Betroffenen gehört auch das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat.</p> <p>(4) Stellt sich heraus, dass personenbezogene Daten, die nicht hätten übermittelt werden dürfen, oder unrichtige personenbezogene Daten übermittelt worden sind, ist der Empfänger unverzüglich zu unterrichten.</p> <p>§ 92 IRG Datenübermittlung ohne Ersuchen</p> <p>(1) Soweit eine völkerrechtliche Vereinbarung dies vorsieht, dürfen öffentliche Stellen ohne Ersuchen personenbezogene Daten, die den Verdacht einer Straftat begründen, an öffentliche Stellen eines anderen Mitgliedstaates der Europäischen Union sowie Organe und Einrichtungen der Europäischen Gemeinschaften übermitteln, soweit</p> <ol style="list-style-type: none"> 1. eine Übermittlung auch ohne Ersuchen an ein deutsches Gericht oder eine deutsche Staatsanwaltschaft zulässig wäre und 2. die Übermittlung geeignet ist, <ol style="list-style-type: none"> a) ein Strafverfahren in dem anderen Mitgliedstaat einzuleiten oder b) ein dort bereits eingeleitetes Strafverfahren zu fördern, und 3. die Stelle, an die die Daten übermittelt werden, für die zu treffenden Maßnahmen nach Nummer 2 zuständig ist. <p>(2) § 61a Abs. 2 bis 4 gilt entsprechend.</p>
<p>Artikel 27 – Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte</p> <p>1 Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so finden die Absätze 2 bis 9 Anwendung. Liegen ein solcher Vertrag, eine solche Übereinkunft oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung, wenn die betreffenden Vertragsparteien übereinkommen, an Stelle des Vertrags, der Übereinkunft oder der Rechtsvorschriften die Absätze 2 bis 9 ganz oder teilweise anzuwenden.</p>	<p>Artikel 27 wird von den §§ 59 ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) berücksichtigt (siehe oben Artikel 25), soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind.</p>

<p>2</p> <p>a Jede Vertragspartei bestimmt eine oder mehrere zentrale Behörden, welche die Aufgabe haben, Rechtshilfeersuchen abzusenden, zu beantworten, zu erledigen oder an die für die Erledigung zuständigen Behörden weiterzuleiten.</p> <p>b Die zentralen Behörden verkehren unmittelbar miteinander.</p> <p>c Jede Vertragspartei teilt dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde die Bezeichnung und Anschrift der nach diesem Absatz bestimmten Behörden mit.</p> <p>d Der Generalsekretär des Europarats erstellt und aktualisiert ein Verzeichnis der von den Vertragsparteien so bestimmten zentralen Behörden. Jede Vertragspartei stellt sicher, dass die in dem Verzeichnis enthaltenen Angaben stets richtig sind.</p> <p>3 Rechtshilfeersuchen nach diesem Artikel werden nach den von der ersuchenden Vertragspartei bezeichneten Verfahren erledigt, sofern dies mit dem Recht der ersuchten Vertragspartei nicht unvereinbar ist.</p> <p>4 Zusätzlich zu den Ablehnungsgründen nach Artikel 25 Absatz 4 kann die ersuchte Vertragspartei die Rechtshilfe verweigern, wenn</p> <p>a das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder</p> <p>b sie der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (<i>ordre public</i>) oder andere wesentliche Interessen zu</p>	
--	--

beeinträchtigen.

- 5 Die ersuchte Vertragspartei kann die Durchführung der in einem Ersuchen genannten Maßnahmen aufschieben, wenn die Gefahr besteht, dass sie die von ihren Behörden geführten strafrechtlichen Ermittlungen oder Verfahren beeinträchtigen.
- 6 Bevor die ersuchte Vertragspartei die Rechtshilfe verweigert oder aufschiebt, prüft sie, gegebenenfalls nach Konsultation der ersuchenden Vertragspartei, ob dem Ersuchen zum Teil oder vorbehaltlich der von ihr als erforderlich erachteten Bedingungen entsprochen werden kann.
- 7 Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei umgehend das Ergebnis der Erledigung eines Rechtshilfeersuchens mit. Jede Ablehnung und jeder Aufschub des Ersuchens ist zu begründen. Die ersuchte Vertragspartei teilt der ersuchenden Vertragspartei gegebenenfalls auch die Gründe mit, aus denen die Erledigung des Ersuchens unmöglich ist oder sich wahrscheinlich erheblich verzögern wird.
- 8 Die ersuchende Vertragspartei kann die ersuchte Vertragspartei bitten, das Vorliegen eines Ersuchens nach diesem Kapitel und dessen Inhalt vertraulich zu behandeln, soweit die Erledigung des Ersuchens nichts anderes gebietet. Kann die ersuchte Vertragspartei der erbetenen Vertraulichkeit nicht entsprechen, so teilt sie dies der ersuchenden Vertragspartei umgehend mit; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.
- 9
 - a In dringenden Fällen können Rechtshilfeersuchen und damit in Zusammenhang stehende Mitteilungen unmittelbar von den Justizbehörden der ersuchenden Vertragspartei an die Justizbehörden der ersuchten Vertragspartei übermittelt werden. In diesen Fällen ist gleichzeitig über die zentrale

<p>Behörde der ersuchenden Vertragspartei eine Kopie an die zentrale Behörde der ersuchten Vertragspartei zu senden.</p> <p>b Jedes Ersuchen oder jede Mitteilung nach diesem Absatz kann über die Internationale Kriminalpolizeiliche Organisation (Interpol) übermittelt werden.</p> <p>c Wird ein Ersuchen nach Buchstabe a übermittelt und ist die befassende Behörde für die Erledigung nicht zuständig, so leitet sie das Ersuchen an die zuständige Behörde ihres Landes weiter und setzt die ersuchende Vertragspartei unmittelbar davon in Kenntnis.</p> <p>d Ersuchen oder Mitteilungen nach diesem Absatz, die keine Zwangsmaßnahmen erfordern, können unmittelbar von den zuständigen Behörden der ersuchenden Vertragspartei den zuständigen Behörden der ersuchten Vertragspartei übermittelt werden.</p> <p>e Jede Vertragspartei kann dem Generalsekretär des Europarats bei der Unterzeichnung oder bei der Hinterlegung ihrer Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde mitteilen, dass Ersuchen nach diesem Absatz aus Gründen der Effizienz an ihre zentrale Behörde zu richten sind.</p>	
<p>Artikel 28 – Vertraulichkeit und Beschränkung der Verwendung</p> <p>1 Ist zwischen der ersuchenden und der ersuchten Vertragspartei ein Rechtshilfevertrag oder eine Übereinkunft, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurde, nicht in Kraft, so findet dieser Artikel Anwendung. Liegen ein solcher Vertrag, eine solche Übereinkunft oder solche Rechtsvorschriften vor, so findet dieser Artikel nur Anwendung,</p>	<p>Artikel 28 wird von den §§ 59 ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) berücksichtigt (siehe oben Artikel 25), soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind.</p>

<p>wenn die betreffenden Vertragsparteien übereinkommen, an Stelle des Vertrags, der Übereinkunft oder der Rechtsvorschriften die Absätze 2 bis 4 ganz oder teilweise anzuwenden.</p> <p>2 Die ersuchte Vertragspartei kann die Überlassung von Informationen oder Unterlagen in Erledigung eines Ersuchens von der Bedingung abhängig machen, dass sie:</p> <p style="padding-left: 20px;">a vertraulich behandelt werden, wenn das Rechtshilfeersuchen ohne diese Bedingung nicht erledigt werden könnte, oder</p> <p style="padding-left: 20px;">b nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden.</p> <p>3 Kann die ersuchende Vertragspartei einer Bedingung nach Absatz 2 nicht entsprechen, so setzt sie die andere Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob die Informationen dennoch zur Verfügung gestellt werden sollen. Nimmt die ersuchende Vertragspartei die Bedingung an, so ist sie daran gebunden.</p> <p>4 Jede Vertragspartei, die Informationen oder Unterlagen unter einer in Absatz 2 genannten Bedingung zur Verfügung stellt, kann von der anderen Vertragspartei verlangen, dass sie in Zusammenhang mit dieser Bedingung Angaben über die Verwendung der Informationen oder Unterlagen macht.</p>	
<p>Abschnitt 2 – Besondere Bestimmungen Artikel 29 – Umgehende Sicherung gespeicherter Computerdaten</p> <p>1 Eine Vertragspartei kann eine andere Vertragspartei um Anordnung oder anderweitige Bewirkung der umgehenden Sicherung von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der anderen Vertragspartei befindet, und derentwegen die ersuchende Vertragspartei beabsichtigt, ein Rechtshilfeersuchen um</p>	<p>Artikel 29 wird von den §§ 66 und 67 des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) abgedeckt, soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind:</p> <p>§ 66 IRG Herausgabe von Gegenständen (1) Auf Ersuchen einer zuständigen Stelle eines ausländischen Staates können Gegenstände herausgegeben werden,</p>

<p>Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu stellen.</p>	<p>1. die als Beweismittel für ein ausländisches Verfahren dienen können, 2. die der Betroffene oder ein Beteiligter für die dem Ersuchen zu Grunde liegende Tat oder aus ihr erlangt hat, 3. die der Betroffene oder ein Beteiligter durch die Veräußerung eines erlangten Gegenstandes oder als Ersatz für dessen Zerstörung, Beschädigung oder Entziehung oder aufgrund eines erlangten Rechtes erhalten oder als Nutzungen gezogen hat oder 4. die durch die dem Ersuchen zu Grunde liegende Tat hervorgebracht oder zu ihrer Begehung oder Vorbereitung gebraucht worden oder bestimmt gewesen sind.</p>
<p>2 Ein Ersuchen um Sicherung nach Absatz 1 hat Folgendes genau zu bezeichnen:</p> <p>a die Behörde, die um die Sicherung ersucht;</p> <p>b die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung;</p> <p>c die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat;</p> <p>d alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems;</p> <p>e die Notwendigkeit der Sicherung und</p> <p>f die Absicht der Vertragspartei, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der gespeicherten Computerdaten zu stellen.</p>	<p>(2) Die Herausgabe ist nur zulässig, wenn</p> <p>1. die dem Ersuchen zugrunde liegende Tat auch nach deutschem Recht eine rechtswidrige Tat ist, die den Tatbestand eines Strafgesetzes oder eines Gesetzes verwirklicht, das die Ahndung mit einer Geldbuße zuläßt, oder wenn sie bei sinngemäßer Umstellung des Sachverhalts auch nach deutschem Recht eine solche Tat wäre, 2. eine Beschlagnahmeanordnung einer zuständigen Stelle des ersuchenden Staates vorgelegt wird oder aus einer Erklärung einer solchen Stelle hervorgeht, daß die Voraussetzungen der Beschlagnahme vorlägen, wenn die Gegenstände sich im ersuchenden Staat befänden, und 3. gewährleistet ist, daß Rechte Dritter unberührt bleiben und unter Vorbehalt herausgegebene Gegenstände auf Verlangen unverzüglich zurückgegeben werden.</p> <p>(3) Die Herausgabe nach Absatz 1 Nr. 2 bis 4 ist nur zulässig, solange hinsichtlich der Gegenstände noch kein rechtskräftiges und vollstreckbares ausländisches Erkenntnis vorliegt.</p> <p>(4) Die Staatsanwaltschaft bei dem Landgericht bereitet die Entscheidung über die Herausgabe vor und führt die bewilligte Herausgabe durch. Örtlich zuständig ist die Staatsanwaltschaft bei dem Landgericht, in dessen Bezirk sich die Gegenstände befinden.</p>
<p>3 Nach Eingang des von einer anderen Vertragspartei gestellten Ersuchens trifft die ersuchte Vertragspartei alle geeigneten Maßnahmen zur umgehenden Sicherung der bezeichneten Daten in Übereinstimmung mit ihrem innerstaatlichen Recht. Für die Zwecke der Erledigung eines Ersuchens wird die beiderseitige Strafbarkeit als Voraussetzung für die Vornahme dieser Sicherung nicht verlangt.</p>	<p>§ 61 Abs. 2 Satz 2 gilt entsprechend.</p> <p>§ 67 IRG Beschlagnahme und Durchsuchung</p> <p>(1) Gegenstände, deren Herausgabe an einen ausländischen Staat in Betracht kommt, können, auch schon vor Eingang des Ersuchens um Herausgabe, beschlagnahmt oder sonst sichergestellt werden. Zu diesem Zweck kann auch eine Durchsuchung vorgenommen werden.</p>
<p>4 Eine Vertragspartei, welche die beiderseitige Strafbarkeit als Voraussetzung für die Erledigung eines Rechtshilfeersuchens um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche</p>	<p>(2) Gegenstände können unter den Voraussetzungen des § 66 Abs. 1 Nr. 1, Abs. 2 Nr. 1</p>

<p>Sicherstellung oder Weitergabe gespeicherter Daten verlangt, kann sich in Bezug auf andere als die nach den Artikeln 2 bis 11 umschriebenen Straftaten das Recht vorbehalten, Ersuchen um Sicherung nach diesem Artikel abzulehnen, wenn sie Grund zu der Annahme hat, dass im Zeitpunkt der Weitergabe die Voraussetzung der beiderseitigen Strafbarkeit nicht erfüllt werden kann.</p> <p>5 Darüber hinaus kann ein Ersuchen um Sicherung nur abgelehnt werden, wenn</p> <ul style="list-style-type: none"> a das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder b die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (<i>ordre public</i>) oder andere wesentliche Interessen zu beeinträchtigen. <p>6 Ist durch die Sicherung nach Ansicht der ersuchten Vertragspartei die künftige Verfügbarkeit der Daten nicht gewährleistet oder die Vertraulichkeit der Ermittlungen der ersuchenden Vertragspartei gefährdet oder in anderer Weise beeinträchtigt, so setzt sie die ersuchende Vertragspartei umgehend davon in Kenntnis; diese entscheidet dann, ob das Ersuchen dennoch erledigt werden soll.</p> <p>7 Jede Sicherung, die in Erledigung des in Absatz 1 bezeichneten Ersuchens vorgenommen wird, erfolgt für mindestens 60 Tage, damit die ersuchende Vertragspartei ein Ersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten stellen kann. Nach Eingang eines solchen Ersuchens werden die Daten weiterhin gesichert, bis über das Ersuchen entschieden worden ist.</p>	<p>auch dann beschlagnahmt oder sonst sichergestellt werden, wenn dies zur Erledigung eines nicht auf Herausgabe der Gegenstände gerichteten Ersuchens erforderlich ist. Absatz 1 Satz 2 gilt entsprechend.</p> <p>(3) Die Beschlagnahme und die Durchsuchung werden von dem Amtsgericht angeordnet, in dessen Bezirk die Handlungen vorzunehmen sind. § 61 Abs. 2 Satz 2 gilt entsprechend.</p> <p>(4) Bei Gefahr im Verzug sind die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) befugt, die Beschlagnahme und die Durchsuchung anzuordnen.</p>
---	--

<p>Artikel 30 – Umgehende Weitergabe gesicherter Verkehrsdaten</p> <p>1 Stellt die ersuchte Vertragspartei bei der Erledigung eines Ersuchens nach Artikel 29 um Sicherung von Verkehrsdaten bezüglich einer bestimmten Kommunikation fest, dass ein Diensteanbieter in einem anderen Staat an der Übermittlung dieser Kommunikation beteiligt war, so gibt die ersuchte Vertragspartei Verkehrsdaten in so ausreichender Menge an die ersuchende Vertragspartei umgehend weiter, dass dieser Diensteanbieter und der Weg, auf dem die Kommunikation übermittelt wurde, festgestellt werden können.</p> <p>2 Von der Weitergabe von Verkehrsdaten nach Absatz 1 darf nur abgesehen werden, wenn</p> <p>a das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird, oder</p> <p>b die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (<i>ordre public</i>) oder andere wesentliche Interessen zu beeinträchtigen.</p>	<p>Artikel 30 wird von den §§ 59 ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) berücksichtigt (siehe oben Artikel 25), soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind.</p>
<p>Artikel 31 – Rechtshilfe beim Zugriff auf gespeicherte Computerdaten</p> <p>1 Eine Vertragspartei kann eine andere Vertragspartei um Durchsuchung oder ähnlichen Zugriff, um Beschlagnahme oder ähnliche Sicherstellung und um Weitergabe von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet, einschließlich Daten, die nach Artikel 29 gesichert worden sind.</p>	<p>Artikel 31 wird von den §§ 66 und 67 des Gesetzes über die internationale Rechtshilfe in Strafsachen ("IRG", Stand Oktober 2009) berücksichtigt (siehe oben Artikel 29), soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind.</p>

<p>2 Die ersuchte Vertragspartei erledigt das Ersuchen, indem sie die in Artikel 23 bezeichneten völkerrechtlichen Übereinkünfte, sonstigen Übereinkünfte und Rechtsvorschriften anwendet und die anderen einschlägigen Bestimmungen dieses Kapitels einhält.</p> <p>3 Das Ersuchen ist umgehend zu erledigen, wenn</p> <p>a Gründe zu der Annahme bestehen, dass bei den einschlägigen Daten eine besondere Gefahr des Verlusts oder der Veränderung besteht oder</p> <p>b die in Absatz 2 bezeichneten Übereinkünfte und Rechtsvorschriften eine umgehende Zusammenarbeit vorsehen.</p>	
<p>Artikel 32 – Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind</p> <p>Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei</p> <p>a auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden, oder</p> <p>b auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.</p>	<p>Strafprozessordnung („StPO“, Stand Juli 2009):</p> <p>§ 94 StPO</p> <p>(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.</p> <p>(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.</p> <p>(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.</p>
<p>Artikel 33 – Rechtshilfe bei der -Erhebung von Verkehrsdaten in Echtzeit</p>	<p>Artikel 33 wird von den §§ 59 ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen („IRG“, Stand Oktober 2009) berücksichtigt (siehe oben Artikel 25), soweit</p>

<p>1 Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit in Zusammenhang mit bestimmten Kommunikationen in ihrem Hoheitsgebiet, die mittels eines Computersystems übermittelt werden. Vorbehaltlich des Absatzes 2 unterliegt die Rechtshilfe den nach innerstaatlichem Recht vorgesehenen Bedingungen und Verfahren.</p> <p>2 Jede Vertragspartei leistet zumindest in Bezug auf die Straftaten Rechtshilfe, bei denen die Erhebung von Verkehrsdaten in Echtzeit in einem gleichartigen inländischen Fall möglich wäre.</p>	<p>nicht im Einzelfall speziellere internationale Abkommen anwendbar sind.</p>
<p>Artikel 34 – Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit</p> <p>Die Vertragsparteien leisten einander Rechtshilfe bei der Erhebung oder Aufzeichnung von Inhaltsdaten bestimmter Kommunikationen, die mittels eines Computersystems übermittelt werden, in Echtzeit, soweit dies nach ihren anwendbaren Verträgen und innerstaatlichen Rechtsvorschriften zulässig ist.</p>	<p>Artikel 34 wird von den §§ 59 ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG“, Stand Oktober 2009) berücksichtigt (siehe oben Artikel 25), soweit nicht im Einzelfall speziellere internationale Abkommen anwendbar sind.</p>
<p>Artikel 35 – 24/7-Netzwerk</p> <p>1 Jede Vertragspartei bestimmt eine Kontaktstelle, die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um 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 unverzüglich für Unterstützung zu sorgen. Diese Unterstützung umfasst die Erleichterung oder, sofern dies nach innerstaatlichem Recht und innerstaatlicher Praxis zulässig ist, die unmittelbare Durchführung folgender Maßnahmen:</p>	<p>Die deutsche Kontaktstelle des 24/7-Netzwerks besteht beim Bundeskriminalamt (BKA“). Zugleich fungiert das Bundeskriminalamt in Wiesbaden als Kontaktstelle für die 24/7-Netzwerke der “G8 High-Tech Crime Subgroup” und der ICPO Interpol.</p>

<p>a fachliche Beratung; b Sicherung von Daten nach den Artikeln 29 und 30 und c Erheben von Beweismaterial, Erteilen von Rechtsauskünften und Ausfindigmachen verdächtiger Personen.</p> <p>2 a Die Kontaktstelle einer Vertragspartei muss über Möglichkeiten zur schnellen Kommunikation mit der Kontaktstelle einer anderen Vertragspartei verfügen.</p> <p>b Ist die von einer Vertragspartei bestimmte Kontaktstelle nicht Teil der für die internationale Rechtshilfe oder Auslieferung zuständigen Behörde oder Behörden dieser Vertragspartei, so stellt die Kontaktstelle sicher, dass sie sich mit dieser Behörde oder diesen Behörden schnell abstimmen kann.</p> <p>3 Jede Vertragspartei stellt sicher, dass geschultes und entsprechend ausgestattetes Personal zur Verfügung steht, um die Arbeit des Netzwerks zu erleichtern.</p>	
<p>Article 42 – Reservations</p> <p>Jeder Staat kann durch eine an den Generalsekretär des Europarats gerichtete schriftliche Notifikation bei der Unterzeichnung oder bei der Hinterlegung seiner Ratifikations-, Annahme-, Genehmigungs- oder Beitrittsurkunde erklären, dass er von einem oder mehreren der in Artikel 4 Absatz 2, Artikel 6 Absatz 3, Artikel 9 Absatz 4, Artikel 10 Absatz 3, Artikel 11 Absatz 3, Artikel 14 Absatz 3, Artikel 22 Absatz 2, Artikel 29 Absatz 4 und Artikel 41 Absatz 1 vorgesehenen Vorbehalten Gebrauch macht. Weitere Vorbehalte sind nicht zulässig.</p>	<p>Declaration contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl.</p> <p>In accordance with Article 40 of the Convention, the Federal Republic of Germany declares that it avails itself of the possibility of requiring that,</p> <p>(a) according to Article 2, second sentence, the additional element of commission by infringing security measures be included as an element of the offence of data espionage, which has been established under German law in section 202a of the Criminal Code pursuant to Article 2, first sentence, and</p> <p>(b) according to Article 7, second sentence, the additional element of an "intent to defraud, or similar dishonest intent" that takes the form of deception in legal transactions be included as an element of the offence of falsification of legally relevant data, which has been established under German law in section 269 of the Criminal Code pursuant to Article 7, first sentence.</p>

Reservation contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl.

The Federal Republic of Germany declares that it avails itself of Article 42 of the Convention to the extent that

- (a) Article 6, paragraph 1.a.i, as relates to "devices", and sub-paragraph b shall not be applied,
- (b) the attempt to commit the acts specified under Article 3 shall not be established as criminal offence under national law, and
- (c) requests for expedited preservation of stored data under Article 29 may be refused on the ground that dual criminality is not given, provided there is reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled, unless the offence in question is an offence established pursuant to Articles 2 to 11.

Declaration contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl.

In accordance with Article 24, paragraph 7, sub-paragraph a, of the Convention, the Federal Republic of Germany declares that the central authority responsible for making or receiving requests for extradition or provisional arrest is the Federal Foreign Office (address: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin).

Declaration contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009 - Or. Engl.

In accordance with Article 35, paragraph 1, of the Convention, the Federal Republic of Germany declares that the point of contact designated to fulfil the functions specified in this article is the National High Tech Crime Unit at the Federal Criminal Police Office (address: Thaerstr. 11, 65193 Wiesbaden, phone: 49-611-551-3101, fax: 49-611-554-5100, mail: so43auswertung@bka.bund.de (for non-emergency use only), nhtcu@bka.de (for emergency use only)).

Declaration contained in a letter from the Permanent Representative of Germany,

dated 14 May 2009, registered at the Secretariat General on 15 May 2009 - Or. Engl.

In accordance with Article 27, paragraph 2.a, of the Convention, the Federal Republic of Germany declares that the central authority responsible for mutual assistance requests in the absence of applicable international agreements is the Ministry of Foreign Affairs (address: Werderscher Markt 1, 10117 Berlin)