# Teil I:
# Rechtliche Rahmenbedingungen

Lukas Jung, Marc Narres-Schulz, Oliver Sänger, Tobias Zeimetz

25. Januar 2017

# Aufgabe 1

## Welche Gesetze sich mit dem Thema befassen

Zum Thema Netzwerksicherheit bzw. auch Internetsicherheit, befassen sich mehrere verschiedene Gesetze. Diese lassen sich grob in drei Kategorien unterteilen:

- EU-Gesetze
- Deutschlandweite Gesetze
- Hochschulgesetze

Auf EU-Ebene greift zu diesem Thema nur die Grundrechtecharta. Doch dort fehlt es an genaueren Gesetzten und es heißt lediglich nach *Artikel 8 der Grundrechtecharta*:

> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Was genau unter „Recht auf Schutz“ gemeint ist und der genauere rechtliche Rahmen wird den einzelnen Ländern überlassen. In Deutschland befassen sich das Bundesdatenschutzgesetz (BDSG) und das Gesetz über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten (ZKDSG) mit diesem Thema.
Das BDSG umfasst alles was die Privatsphäre personenbezogener Daten betrifft auch im Kontext polizeilicher Überwachung. Einzelne Paragraphen können hier leider nicht aufgezählt werden, da dass BDSG einen zu großen Umfang besitzt. Daher lässt sich das BDSG in sechs Abschnitte unterteilen:

- In (§§ 1–11) werden allgemeine und gemeinsame Bestimmungen erläutert.
- In (§§ 12–26) wird die Datenverarbeitung für öffentliche Stellen geregelt.
- In (§§ 27–38a) wird die Datenverarbeitung für private Stellen geregelt.
- In (§§ 39–42) werden Sondervorschriften geregelt.
- In (§§ 43–44) werden Straf- und Bußgeldvorschriften geregelt.
- In (§§ 45–48) werden Übergangsvorschriften genannt.

Das ZKDSG schützt Zugangskontrolldienste und zugangskontrollierte Dienste rechtlich gegen unerlaubte Eingriffe. Unter dem Begriff zugangskontrollierte Dienste versteht man im ZKDSG Rundfunkanbieter, Teledienste oder auch Mediendienste. Die Zugangskontrolldienste bezeichnen hier die technischen Verfahren oder Vorrichtungen, die die erlaubte Nutzung eines zugangskontrollierten Dienstes ermöglicht. Vereinfacht ausgedrückt, soll also mit dem ZKDSG verhindert werden, dass sich Dienstleistungen und Services wie beispielsweise Premiere oder digitable Abos von Zeitschriften usw. erschlichen werden können. Als letzter Punkt muss für den Fall der Forschung und Lehre auch noch das Hochschulgesetz für Rheinland-Pfalz berücksichtigt werden.

- §3 Freiheit von Kunst und Wissenschaft, Forschung, Lehre und Studium

Dort heißt es, dass die Gesetze des Landes und Bundes die Rahmenbedingungen für Forschung und Lehre bilden. Das heißt, dass neben den bereits erwähnten Gesetzen wenigerechtliche Einschränkungen oder Gesetze hinzukommen dürfen. Beschlüsse der zuständigen Hochschulorgane in Fragen der Forschung sind insoweit zulässig, als dass sie die Forschung und Lehre in ihrer Freiheit nicht beeinträchtigen. In diesem Kontext bedeutet Freiheit jedoch nicht, dass Hochschulen von geltenden Gesetzen befreit sind. Es bedeutet viel mehr, dass sie neben den bestehenden Gesetzen des Landes und Bundes nur geringfügig behindert werden dürfen.

## Welche Strafrechtlichen Vorschriften es gibt

Im Strafgesetzbuch (StGB) gibt es einige Paragraphen die sich mit dem Thema Datensicherheit befassen. Zuerst folgt eine Auflistung von diesen Paragraphen und anschließend folgt eine detaillierte Erklärung. Im StGB befassen sich folgende Paragraphen mit dem Thema:

- §202 Verletzung des Briefgeheimnisses
- §202a Ausspähen von Daten
- §202b Abfangen von Daten
- §202c Vorbereiten des Ausspähen und Abfangen von Daten (auch bekannt als "Hackerparagraph") in Verbindung mit §149 Wertzeichenfälschung
- §202d Datenhehlerei
- §303a Datenveränderung
- §303b Computersabotage
- §303c Strafantrag

Begonnen wird mit einer Erläuterung zu Paragraph §202 (Briefgeheimnis). In diesem steht:

> (1) Wer unbefugt
>
> 1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
> 2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
>
> wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.
> (2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.
> (3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

Wenn man in Artikel 10 des Grundgesetzes (GG) nachschlägt, kann man lesen dass als Brief jede schriftliche Mitteilung zwischen einem Absender und einem Empfänger angesehen wird. Daher unterliegen (neben einer Postkarte) auch E-Mails dem Briefgeheimnis gemäß einer Entscheidung des Oberlandesgerichts Karlsruhe [OLG Karlsruhe, 10.01.2005, 1 W 152/04]. Es kann jedoch auch Ausnahmeregeln geben wie beispielsweise Firmen-Mails. Ist im Vertrag geregelt, dass die E-Mails ausschließlich zum Firmenbetrieb dienen und nicht privat genutzt werden dürfen, darf ein Arbeitgeber die E-Mails mitlesen.
Der nächste Paragraph im StGB ist §202a (Ausspähen von Daten). In diesem heißt es:

> (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.
> (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Wie man Punkt (1) entnehmen kann, ist es verboten sich Zugang zu Inhalten zu verschaffen, welche normalerweise nicht für einen bestimmt wären. Somit ist es also Strafbar sich mittels SQL-Injection zugriff auf eine Datenbank zu verschaffen. Das liegt daran, dass man die Zugangssicherung umgehen musste. Auch wenn diese sehr schwach ist, reicht vom StGB her um eine gültige Sicherung vor dem Zugriff Anderer darzustellen. Ebenfalls zählen hier Verfahren wie Keylogger. Dabei handelt es sich um nichts anderes als sich Zugang zu Daten zu beschaffen, in dem man das Opfer infiziert, und anschließend dessen Passwörter ausspäht.
Der Absatz (2) grenzt den Begriff der Daten ein, in dem es diese als elektronisch oder magnetisch festschreibt und somit auf den Computer fixiert.
Als nächstes wird auf Paragraph §202b (Abfangen von Daten) eingegangen. Dieser lautet:

> 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.

Unter „unbefugter Beschaffung“ versteht man das Beschaffen von Daten ohne vorherige Erlaubnis des Eigentümers. Des Weiteren ist von „nichtöffentliche Datenübermittlung“ die Rede. Darunter versteht man verschlüsselte Funknetzwerke und auch Übertragungen durch Kabel oder andere Wege. Das bedeutet aber auch, dass das mitlesen von unverschlüsselten Daten nicht Strafbar ist, da es sich hierbei um eine „öffentliche Datenübermittlung“ handelt. Ausnahmen in welchen man auch „öffentliche Datenübermittlungen“ nicht mitlesen oder abfangen darf, bilden Datenverarbeitungsanlagen. Das heißt ein Router, welcher offenes WLAN-Netz betreibt, kann im weitesten Sinne als Datenverarbeitungsanlage bezeichnet werden, da es die Daten zwischen den Computern und den Servern regelt.
Der eigentliche „Hackerparagraph“ ist §202c und besteht aus zwei Absätzen. Der Paragraph lautet wie folgt:

> (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
>
> 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 zwei Jahren oder mit Geldstrafe bestraft.
> (2) Nach Absatz 1 wird nicht bestraft, wer freiwillig
>
> 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.
>
> (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.

Absatz 1 besagt, dass wer sich auf irgendeinem Weg mittels Überwindung der Zugangssicherung zu einem System zugriff verschafft, macht sich Strafbar. Des Weiteren ist auch das Verkaufen der Mittel für den Zugang oder das Herstellen solcher Mittel unter Strafe. Was vor allem ein Problem bei sogenannten „Hackertools“ darstellen könnte. Laut StGB gilt hier, wenn die Tools dazu genutzt wurden um einen Angriff auszuführen, so waren die Tools vorbereitender Natur. Dadurch haben sich auch die Entwickler solcher Tools in Deutschland strafbar gemacht. Was auch dazu führt, dass Gruppen wie der Chaos Computer Clubs (CCC) gegen dieses Gesetz sind. Schließlich werden solche Tools auch dazu verwenden, um die eigene Netzstruktur auf Sicherheit zu überprüfen. Vor allem ist zu kritisieren, dass allein entscheidend sei, dass ein Programm oder eine Information genutzt werden könnte, in fremde Computer einzudringen und keine Ausnahmeregelungen bestehen, die den Einsatz für legale Zwecke erlaubt. Nach Absatz 2 gilt, wer eine Tat anfängt diese aber nicht zu Ende führt, das heißt bevor er Daten stiehlt, manipuliert, sich unerlaubt Zugang verschafft etc., macht sich nicht strafbar. Wird der Angriff jedoch nicht erfolgreich ausgeführt oder andere Angreifer führen den Angriff fort, macht man sich dennoch strafbar. Auch hier lässt sich wieder die Problematik von „Hackertools“ erkennen, da der Zweck solcher Tools nicht berücksichtigt wird.
Als nächstes wird §149 (Wertzeichenfälschung) genauer Betrachtet. Hierbei wird unter anderem gesagt, dass das entwickeln eines Computerprogramms zum fälschen von Geldmitteln oder Wertzeichen unter Strafe steht. Auch hier gilt, dass die reine Herstellung eines solches Tools strafbar ist, nicht nur die

Ausführung der Fälschung. Hier gibt es, wie bereits zuvor, keine Unterscheidung für den Zweck der Tools. Wenn beispielsweise BitCoin als legitimes Geldmittel anerkannt wären, würde und sich Strafbar machen wenn man Tools entwickelt um diese auf Sicherheit zu überprüfen. Dadurch wird auch hier Sicherheit nicht zwangsläufig gefördert sondern vielmehr verhindert, dass eine erhöhte Sicherheit gewährleistet wird.
Ein weiterer Paragraph der sich mit dem Schutz von Benutzerdaten befasst ist §202d (Datenhehlerei). Dieser besagt, dass auch das verkaufen von rechtswidrig erlangten Daten strafbar ist. Bei der Wahl des Strafmaßes muss jedoch darauf geachtet werden, dass dieses nicht höher ist als das Strafmaß für das illegale erlangen der Daten.
Auch §303a (Datenveränderung) ist ein wichtiger Paragraph für die Datensicherheit. Er besagt, dass jegliches Abänderung von Daten, die nach §202a rechtswidrig ist, strafbar ist. Hier zählt wie bisher auch wieder, dass allein der Versuch dazu schon strafbar ist. Was die Vorbereitung einer Tat angeht greift die Regelung wie bei §202c.
Computersabotage nach §303b ist das Stören einer fremden Datenverarbeitungsanlage (DVA), die für einen anderen von wesentlicher Bedeutung ist. Hierbei ist sowohl der betriebliche Sinn als auch der private Sinn einer DVA gemeint. Unter einer betrieblichen DVA könnte beispielsweise ein Server verstanden werden wohingegen eine private DVA bereits ein Router sein kann.
In §303c (Strafantrag) wird geregelt wie die Straftat verfolgt wird. Dort heißt es, dass nur in Fällen mit „besonderem öffentlichen Interesse“ die Strafverfolgungsbehörde die Tat selbstständig verfolgt. In allen anderen Fällen muss ein Geschädigter einen Antrag stellen. Zwar bezieht sich §303c nur auf §303, §303a und §303b jedoch unter Berücksichtigung von §202a. Somit handelt es sich in den oben aufgezählten Fällen um ein Antragsdelikt.

### Besondere Bedingungen für die Universität Trier

Für die Universität Trier gelten neben den Hochschulgesetzen keine weiteren besonderen Bedingungen. Im Bezug auf die Datensicherheit gibt es dort einen speziellen Paragraphen:

- §3 Freiheit von Kunst und Wissenschaft, Forschung, Lehre und Studium

Dort heißt es, wie bereits erwähnt, dass die Gesetze des Landes und Bundes die Rahmenbedingungen für Forschung und Lehre bilden. Das heißt, dass neben den bereits erwähnten Gesetzen wenigerechtliche Einschränkungen oder Gesetze hinzukommen dürfen. Beschlüsse der zuständigen Hochschulorgane in Fragen der Forschung sind insoweit zulässig, als dass sie die Forschung und Lehre in ihrer Freiheit nicht beeinträchtigen. In diesem Kontext bedeutet Freiheit jedoch nicht, dass Hochschulen von geltenden Gesetzen befreit sind. Es bedeutet viel mehr, dass sie neben den bestehenden Gesetzen des Landes und Bundes nur geringfügig behindert werden dürfen.

### Welche Bedingungen die Universität selbst stellt

Die besonderen Bedingungen gehen aus der Teilgrundordnung der Universität Trier, Der Benutzerordnung der CIP- und Poolrechner der Abteilung Informatik, sowie der Dienstanweisung über den Datenschutz und die Datensicherung an der Universität Trier hervor.

## Aufgabe 2

Funknetzwerke, so genannte WLANs, sind nicht nur bei Unternehmen beliebt, auch immer mehr Haushalte nutzen diese und sparen sich u.a. die Verlegung von notwendigen Kabeln. Mittlerweile gibt es viele Haushaltsgeräte eine solche Funkverbindung verwenden um Daten auszutauschen. Auch Smartphones oder Tabletts verwenden diese Technik. Der folgende Abschnitt beschäftigt sich mit dem rechtlichen Schutz des Funknetzes und was für Konsequenzen eine nicht gesicherte Verbindung haben kann.

### Rechtlicher Schutz von Funknetzwerken gegenüber der Nutzung Dritter

WLAN unterliegen gesetzlichen Regelungen. WLAN-Angebote müssen zahlreiche Vorgaben erfüllen. Hierbei regelt das Telekommunikationsgesetz (TKG) welche Voraussetzungen gegeben sein müssen, um

WLAN-Netze überhaupt anbieten zu dürfen. Auch für den Beitrieb selbst gelten Anforderungen an den Datenschutz und die Datensicherheit.
Die Nutzung von WLAN fällt unter §3 Nr. 16 TKG, d.h., der Telekommunikation. Bei gewerblichen Angeboten liegt sogar eine Telekommunikaktionsdienstleistung gemäß §3 Nr. 18 TKG vor. Für WLAN-Angebote sind die Frequenzbereiche von 2,4 GHz und 5 GHz freigegeben. WLAN-Netze sind hierbei nicht die einzigen Anwendungen, die diese Frequenzbereiche nutzen. Etwaige Einschränkungen wie bspw. durch Amateurfunk oder andere Funkanwendungen muss der jeweilige Betreiber hinnehmen.
Als mögliche Straftatbestände kommen das Ausspähen von Daten gem. §202a StGB, der Computerbetrug gem. § 263a StGB sowie das Erschleichen von Leistungen gem. §265a StGB aber auch das Abhören von Nachrichten gem. §§89, 148 Abs. 1 Nr. 1 TKG in Betracht.
Es muss rechtlich unterschieden werden, ob es sich um ein gesichertes (verschlüsseltes) oder ein ungesichertes (unverschlüsseltes) Netzwerk handelt. Zuerst wird das Eindringen in ein gesichertes Netzwerk betrachtet. In diesem Fall kommt eine Strafbarkeit nach §202a StGB in Betracht. Danach macht sich strafbar, wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft. Unter Daten sind dabei alle Informationen zu verstehen, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind, sich also in EDV-spezifischer Form darstellen lassen. Dazu zählt zum einen das bei WEP verwendete Passwort, zum anderen aber auch die im Rahmen des Verbindungsaufbaus vom Router zugeteilte IP-Adresse. Für das Tatbestandsmerkmal „Verschaffen“ reicht schon aus, wenn der Täter Kenntnis von den gesicherten Daten erlangt. Auf die tatsächliche Nutzung des WLAN-Netzwerks, beispielsweise als Internetzugang kommt es dabei nicht an. Das heißt, der Tatbestand des §202a StGB ist bereits dann erfüllt, wenn der Täter vorsätzlich ein verschlüsseltes WLAN-Netzwerk knackt und hierdurch von den geschützten Daten Kenntnis nimmt.
Bei ungesicherten WLAN-Netzwerken liegt die Sache etwas anders. Eine Strafbarkeit nach §202a StGB scheidet in diesem Fall aus, da es an einer besonderen Datensicherung fehlt.
Eine Strafbarkeit wegen Computerbetrugs nach §263a StGB kommt ebenfalls nicht in Betracht. Insoweit muss man danach differenzieren, ob der Netzwerkinhaber mit seinem Provider einen Flatrate-Tarif oder eine Bezahlung nach der jeweils heruntergeladenen Datenmenge vereinbart hat. Denn für den Fall, dass der Netzwerkinhaber einen Flatrate-Tarif vereinbart hat, erleidet er durch das unbefugte Mitsurfen eines Dritten keinen Vermögensschaden. Für den Fall, dass eine Bezahlung nach Datenmenge vereinbart wurde, tritt beim Netzwerkinhaber ein Vermögensschaden in Höhe der über seine eigene Nutzung hinausgehenden und von ihm zu bezahlenden Datenmenge ein. Dem Vorteil des Nutzers steht in diesem Fall jedoch kein Schaden des Betreibers, dem möglichen Schaden des Betreibers kein vom Nutzer angestrebter Vorteil gegenüber. Es fehlt somit an der für §263a StGB erforderlichen Stoffgleichheit.
Eine Strafbarkeit wegen Erschleichens von Leistungen nach §265a StGB kommt schon deshalb nicht in Betracht, weil dessen Schutzbereich sich nur auf öffentlichen Zwecken dienende Telekommunikationsnetze erstreckt. WLAN-Netzwerke, die nur geschlossenen Benutzergruppen zur Verfügung stehen, dienen jedoch nicht öffentlichen Zwecken.
Bleibt eine mögliche Strafbarkeit wegen Abhörens von Nachrichten gem. §§89, 148 Abs. 1 Nr. 1 TKG. Diese scheitert jedoch daran, dass es sich beim Datenverkehr im Rahmen der IP-Zuweisung nicht um Nachrichten im Sinne des §89 TKG handelt.

## Abhören von verschlüsselten Funkdaten

Bereits mit frei verkäuflichen technischen Mitteln ist es möglich, Daten bei der Kommunikation über drahtlose Netze auszuspähen. Es liegt nahe, dass derartige Angriffe (sog. „drive-by-hacking“ oder “war-driving”) rechtlich nicht gestattet sein können. Insbesondere in §89 TKG sowie in §202a StGB finden sich entsprechende Regelungen.

### Abhörverbot nach §89 TKG

Die Vorschrift verbietet das Abhören von Nachrichten mit einer Funkanlage, wenn diese für die Funkanlage nicht bestimmt sind. Hierunter fällt zweifelsohne das „Hacking“ von drahtlosen Funkverbindungen.
Unter einer „Nachricht“ ist nicht nur die an einen menschlichen Empfänger gerichtete Kommunikation zu verstehen. Auch auf den Informationsinhalt kommt es nicht an. Als Nachricht im Sinne dieser Vor-

schrift ist vielmehr jede Übermittlung von Signalen auch zwischen Computern ohne direkte menschliche Mitwirkung anzusehen.
Funkanlage ist nach der Definition in §2 Nr. 3 des Gesetzes über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) „ein Erzeugnis oder ein wesentliches Bauteil davon, das in dem für terrestrische/satellitengestützte Funkkommunikation zugewiesenen Spektrum durch Ausstrahlung und/oder Empfang von Funkwellen kommunizieren kann“. Diese Voraussetzungen sind beim Hacking von drahtlosen Verbindungen gegeben.
Verboten ist nach §89 TKG nur das vorsätzliche Abhören von Funkverbindungen. Das unbeabsichtigte Abhören ungesicherter drahtloser Verbindungen ist hingegen nicht von §89 Satz 1 TKG umfasst.
Nicht verhindert werden soll durch die Vorschrift zudem das Aufdecken von Sicherheitsmängeln etwa durch die zuständigen Datenschutzaufsichtsbehörden. Diese sind befugt, auch verdeckt unsichere WLAN-Netze im Rahmen datenschutzrechtlicher Prüfungen aufzuspüren. Die Aufzeichnung von Inhalten sollte im Rahmen derartiger Prüfungen allerdings unterbleiben; sie ist zur Feststellung von Sicherheitsmängeln in der Regel auch nicht erforderlich.
Sowohl der Inhalt der Nachrichten als auch die bloße Tatsache ihres Empfangs dürfen – auch bei unbeabsichtigtem Empfang – gemäß §89 Satz 2 TKG anderen nicht mitgeteilt werden. Dies gilt wiederum nicht für die Unterrichtung zuständiger Datenschutzaufsichtsbehörden. Diesen kann das Fernmeldegeheimnis nicht entgegengehalten werden. Sie sind nach §115 Abs. 5 TKG befugt, Nachrichteninhalte zur Kenntnis zu nehmen.
Sowohl das vorsätzliche Abhören nach §89 Satz 1 TKG als auch die vorsätzliche unbefugte Weitergabe nach §89 Satz 2 TKG sind nach §148 Abs. 1 Nr. 1 TKG mit Strafe bedroht. Im Gegensatz zur ersten Aufgabe, ist hier noch nicht der Versucht strafbar, sondern lediglich die vollendete Tat.

### Ausspähen von Daten nach §202a StGB

Nach dieser Vorschrift ist es strafbar, sich oder einem anderen unbefugt Daten zu verschaffen, die gegen unberechtigten Zugang besonders gesichert und nicht für den Täter bestimmt sind.
Die Vorschrift schützt allein die Verfügungsbefugnis über die Daten, d.h. das Bestimmungsrecht darüber, wem die Daten zugänglich sein sollen. Auf den Inhalt oder die Bedeutung der Daten kommt es nicht an.
Der Täter verschafft sich die Daten beim vorsätzlichen Hacking drahtloser Kommunikation dann, wenn er Daten auf seinem Computer gespeichert hat, die nicht für ihn bestimmt sind. Dieses Merkmal dürfte bei Hacking von drahtlosen Verbindungen in der Regel gegeben sein. Der Versuch ist hingegen wieder nicht strafbar.
Entscheidend für eine Strafbarkeit ist jedoch, ob die Daten bei der Übertragung gegen unberechtigten Zugang gesichert sind. Eine solche Zugangssicherung besteht bei der Übertragung in drahtlosen Netzen insbesondere dann, wenn die Daten bei der Übertragung wirksam verschlüsselt werden. Die vom Gesetz gemeinte Zugangssicherung soll in erster Linie den Zugang zu den Originaldaten, d.h. den Inhalten, verhindern. Das bloße Abgreifen verschlüsselter Daten wäre deshalb wegen der fehlenden Möglichkeit, auf die Inhalte zugreifen zu können, nicht nach §202a StGB strafbar, eine Entschlüsselung dieser Daten würde die Strafbarkeit jedoch begründen.
Nicht gegen unberechtigten Zugang gesichert ist die Datenübertragung insbesondere dann, wenn die Sperren ohne größeren Aufwand überwunden werden können. Werden keine besonderen Sicherungssysteme, d. h. vor allem Verschlüsselungsverfahren, verwendet oder sind diese zum Zeitpunkt ihrer Einrichtung bekanntermaßen und objektiv völlig ungeeignet, ist keine besondere Sicherung gegen unberechtigten Zugang gegeben. Eine Strafbarkeit nach §202a StGB wäre in diesen Fällen zumindest fraglich.
Eine Strafverfolgung ist gemäß §205 StGB nur auf Antrag des Verletzten möglich. Unabhängig von der Frage der Strafbarkeit werden die Anbieter selbstverständlich nicht ihrer Pflichten enthoben, die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz zu treffen und so erfolgreiche unbefugte Zugriffe auf die übertragenen Daten zu verhindern.