

Rechtliche Aspekte aus offenen Accesspoints

Referat vom 30. September 2005

Prof. Ursula Sury
Rechtsanwältin in Luzern und Zug
Dozentin an der HSW Luzern

Agenda

1. Einführung
2. Darf jedermann Accesspoints anbieten?
3. Sicherheitspflichten von Accesspoint-Anbietern
4. Informationspflichten von Anbietern
5. Sicherheitspflichten von Accesspoint-Benutzern
6. Grenzen der Legalität beim Wardriving
7. Zusammenfassung

1. Einführung

- Was ist ein Accesspoint? (1)
 - Antenne bzw. Sendestation, die drahtlos Signale über Funkwellen ausstrahlt
 - Schaltstelle im WLAN
 - ⇒ Möglichkeit des drahtlosen Zugangs zum Internet für Laptop-Benutzer über WLAN-Technologie, Anschluss an Ethernet
 - ⇒ WLAN: Wireless Local Area Network
 - oft: öffentlich angeboten (sog. Hotspots, PWLAN)

1. Einführung

- Was ist ein Accesspoint? (2)
 - Empfang im Umkreis von maximal 100-300 Metern
 - ⇒ durch Richtfunkantenne kann Reichweite jedoch erhöht werden
 - i.d.R. im 2.4 GHz-Frequenzbereich, geringe Sendeleistung
 - integrierte Funktionen (z.B. Kabelmodem, LAN-Anschluss, Sicherheitssoftware)

1. Einführung

- Was ist ein Accesspoint? (3)
 - relativ neu im IT-Bereich, viele Anbieter (z.B. Swisscom, Sunrise, Cablecom)
 - Einsatz für Privat- und Firmennetze
 - Zahlreiche öffentliche Hotspots in grösseren Städten (z.B. an Flughäfen, Bahnhöfen, in Hotels, Restaurants)
 - Zukunft: „Wimax Mobile“

1. Einführung

- Problematik von Accesspoints (1)
 - offenes, vielfach ungeschütztes System
 - ⇒Zugang für jeden beliebigen Benutzer
 - ⇒evtl. Zugang zu vertraulichen Daten des WLAN-Besitzers (jedoch örtliche Einschränkung auf den Empfangsbereich)
 - ⇒kriminelle Aktivitäten können dem Benutzer angerechnet werden (Anonymität des Täters)
 - zu geringes Sicherheitsbewusstsein bei den Benutzern
 - ⇒blindes Vertrauen in die Technik, fehlendes technisches Wissen, Priorität: Geschwindigkeit

1. Einführung

- **Problematik von Accesspoints (2)**
 - Gefahr des (anonymen) Missbrauchs durch fremde Personen (z.B. „Hacker“, Viren, Phising-Fallen, Spam, Passwort-Spionage)
 - rechtliche Aspekte sind noch wenig abgeklärt (bisher wenige Prozesse bzw. Präzedenzfälle)

1. Einführung

- **Wichtigste rechtliche Begriffe (1)**
 - Fernmeldeanlagen: Geräte, Leitungen oder Einrichtungen, die zur fernmeldetechnischen Übertragung von Informationen bestimmt sind oder benutzt werden (FMG 3 lit. d)
 - Fernmeldetechnische Übertragung: elektrisches (...) Senden oder Empfangen von Informationen über Leitungen oder Funk (FMG 3 lit. c)
 - Informationen: für Menschen (...) oder Maschinen bestimmte Zeichen, Signale, Schriftzeichen, Bilder, Laute und Darstellungen jeder anderen Art (FMG 3 lit. a)

1. Einführung

- **Wichtigste rechtliche Begriffe (2)**

- Fernmeldedienst: fernmeldetechnische Übertragung von Informationen für Dritte (FMG 3 lit. b)
- Funkanlage: Einrichtung, die zum Senden und Empfangen von Informationen über Funk an einem gegebenen Ort erforderlich ist (FAV 2 I lit. a)
- Anbieten: jedes auf das Inverkehrbringen von Fernmeldeanlagen gerichtete Verhalten (FAV 2 I lit. e)

1. Einführung

- **Wichtigste rechtliche Begriffe (3)**

- Inverkehrbringen: die entgeltliche oder unentgeltliche Übertragung oder Überlassung von Fernmeldeanlagen (FAV 2 I lit. f)
- Inbetriebnahme: das erstmalige Erstellen und Betreiben einer Fernmeldeanlage (FAV 2 I lit. g)
- Betreiben: das Benützen von Fernmeldeanlagen (FAV 2 I lit. i)

2. Darf jedermann Accesspoints anbieten?

- Grundsatz: **Faktisch** kann jedermann einen Accesspoint anbieten und betreiben (Privatperson, Unternehmen)
- Aber: **Rechtliche** Einschränkungen:
 - FMG (Konzessionspflicht, Aufsicht BAKOM)
 - FAV (Voraussetzungen für Anbieten und Inverkehrbringen von neuen Anlagen)
 - FKV (beschränkte Frequenznutzung)
 - FDV (Konzessionspflicht, weitere Pflichten)
 - Verordnungen des BAKOM

2. Darf jedermann Accesspoints anbieten?

- FMG 4: Konzessions- und Meldepflicht
 - Wer einen **Fernmeldedienst erbringt** und dabei erhebliche Teile der für die Übertragung benutzten Fernmeldeanlagen unabhängig betreibt, benötigt eine (**Dienste-**) **Konzession** (Abs. 1)
- FDV 2: Umfang des Fernmeldedienstes
 - Keinen Fernmeldedienst erbringt namentlich, wer Informationen **innerhalb** eines Gebäudes überträgt (lit. a)

2. Darf jedermann Accesspoints anbieten?

- FMG 22: Konzessionspflicht
 - Wer das **Funkfrequenzspektrum benutzen** will, benötigt eine **Funkkonzession** (Abs. 1)
 - Der Bundesrat kann für Frequenznutzungen von geringer technischer Bedeutung (...) **Ausnahmen** vorsehen (Abs. 3)

2. Darf jedermann Accesspoints anbieten?

- FKV 8: Ausnahmen von der Konzessionspflicht
 - Von der Konzessionspflicht **ausgenommen** sind Frequenznutzungen mit Funkanlagen, die auf bestimmten **Sammelfrequenzen** benützt werden (Abs. 1 lit. a)
 - Das Bundesamt bestimmt diese **Sammelfrequenzen** (Abs. 2)

2. Darf jedermann Accesspoints anbieten?

– Verordnung des BAKOM über
Frequenzmanagement und
Funkkonzessionen:

- Frequenznutzungen nach FKV 8 I lit. a sind
Frequenznutzungen **mit Funkanlagen eines
drahtlosen Netzes** nach der unten stehenden
Tabelle (Art. 2 I lit. e):

Frequenzbereich (Sammelfrequenzen)	Maximale Leistung (Gesamtwert) oder Feldstärke (Höchstwert)
2400 - 2483.5 MHz	100 mW EIRP
5150 - 5350 MHz (indoor-use)	200 mW EIRP
5470 - 5725 MHz (indoor-use)	1 W EIRP

2. Darf jedermann Accesspoints anbieten?

- Fazit: Accesspoint-Anbieter brauchen
keine Funkkonzession, jedoch allenfalls
eine **Dienstkonzession** (beim Erbringen
eines Fernmeldedienstes nach FMG 4 I)
- Bedingung: Accesspoint darf nur mit der
vorgeschriebenen Sendeleistung
betrieben werden (Überschreitung jedoch
selten, WLAN hat i.d.R. geringe
Sendeleistung)

3. Sicherheitspflichten von Accesspoint-Anbietern

– Grundsatz: Jedermann kann faktisch einen Accesspoint anbieten und betreiben

- Privatpersonen (zu Hause)
- Unternehmen (für sich selber oder für Drittpersonen)

3. Sicherheitspflichten von Accesspoint-Anbietern

- Weshalb sind Sicherheitsmassnahmen bei Accesspoints überhaupt nötig?
 - Accesspoints sind offene, ungeschützte Systeme
 - unbeschränkte Benutzerzahl
 - externe Angreifer können anonym auf persönliche Daten der Benutzer zugreifen
 - ⇒ Schäden jeglicher Art können entstehen, vor allem bei Benutzer-Unternehmen (Datenverlust, Viren, Spam, ungeschützte Inhalte, Passwortmissbrauch etc.)

3. Sicherheitspflichten von Accesspoint-Anbietern

- CH-Recht: Wenige Bestimmungen über konkrete Sicherheitspflichten
 - Pflichten *beim Anbieten und Inverkehrbringen* von Fernmeldeanlagen (Sicherheitsanforderungen, Benutzerinformationen, Konformitätserklärung, technische Angaben etc.)
 - *internationale* Sicherheitsstandards (z.B. Richtlinien des EU-Rates, IEEE-Standards)
 - gewisse Pflichten gemäss FMG, FDV und BÜPF
- Praxis: oft interne Sicherheitsregeln beim Anbieter (IT-Governance)

3. Sicherheitspflichten von Accesspoint-Anbietern

- Fazit: Benutzer bestimmt i.d.R. das Sicherheitsniveau
- Weshalb?
 - interne IT-Weisungen des Anbieters sind für die Benutzer nicht verbindlich
 - Anonymität der Benutzer (offene Systeme, zahlreiche Benutzer)
 - Anbieter muss auf Sicherheitsbewusstsein der Benutzer zählen (Anbieter hat keine direkten Eingriffsmöglichkeiten, z.B. Bahnhof)

3. Sicherheitspflichten von Accesspoint-Anbietern

- Gefahr für Anbieter: Benutzer sorgt nicht für genügende IT-Sicherheit
 - ⇒ Benutzer kann nicht beweisen, dass nicht er, sondern ein Fremder für den Schaden verantwortlich ist
- Einzige Möglichkeit des Anbieters: System auf aktuellem Security-Niveau halten
- traurige Realität: viele unverschlüsselte Accesspoints (Beispiel Mailand: 72 %)

3. Sicherheitspflichten von Accesspoint-Anbietern

- Interne Sicherheitspflichten (1)
 - grundlegende Verhaltens- und Sorgfaltspflichten (IT-Governance)
 - ⇒ z.B. Pflicht zur Umsetzung von **präventiven** Sicherheitsmassnahmen
 - IT-Governance als Teil von Corporate Governance
 - Verantwortung bei Management/Vorstand
 - wichtige Führungsaufgabe

3. Sicherheitspflichten von Accesspoint-Anbietern

- Interne Sicherheitspflichten (2)
 - Grund: Gefahren und Risiken für Anbieter
 - ⇒ zivil- und strafrechtliche Haftung bei Pflichtverletzungen und bei Schäden, die durch die Anwendung der IT entstanden sind (z.B. bei AG: Haftung aus OR 752 ff.)
 - Lösung: Riskmanagement
 - Realität: Anbieter weisen i.d.R. lediglich auf Sicherheitsrisiken hin (reicht i.d.R. für Einhaltung der Sorgfaltspflicht)

3. Sicherheitspflichten von Accesspoint-Anbietern

- Wie können Accesspoints gesichert werden? (1)
 - Einsatz von technischen Schutzvorkehrungen (Virenschutz, Firewalls, Passwortschutz, Domainnamen etc.)
 - Konfiguration und Verwaltung des WLAN bzw. des Accesspoints
 - Zugangssicherung (z.B. MAC-Adresse)
 - Sicherheitspakete (z.B. VPN-Client, WPA, WPA2)

3. Sicherheitspflichten von Accesspoint-Anbietern

- Wie können Accesspoints gesichert werden? (2)
 - günstigen Standort des Accesspoints wählen (Mitte des zu versorgenden Systems)
 - ⇒ Merke: Funkstrahlen können auch durch die Wände in weitere Umgebung gelangen (Gefahr!)
 - Unternehmen: Sensibilisierung von Mitarbeitern (z.B. Förderung des Sicherheitsbewusstseins mittels E-Learning-Tools)
 - Grundregel: vorbeugen ist besser als heilen!

4. Informationspflichten von Anbietern

- kaum Informationspflichten (analog Sicherheitspflichten)
 - Beispiele: FDV 64 (Dienstesicherheit), BÜPF 15 (Pflichten der Anbieterinnen)
- evtl. Informationspflicht aufgrund der IT-Governance (analog Sicherheitspflichten)
- Realität:
 - ⇒ Anbieter stellen den Benutzern verschiedene Sicherheitssoftware zum Download zur Verfügung
 - ⇒ Anbieter weisen den Benutzer in den AGB/BGB auf Sicherheitsrisiko hin

4. Informationspflichten von Anbietern

- Beispiel Swisscom: Bietet VPN-Client kostenlos zum Download an
 - ⇒VPN: Virtual Private Networks
- Beispiel Cablecom: Hinweis in AGB oder BGB auf fehlende Sicherheit und Eigenverantwortung des Benutzers

5. Sicherheitspflichten von Accesspoint-Benutzern

- Sicherheitspflichten von privaten Benutzern (1)
 - Benutzer hat i.d.R. selber für Sicherheit zu sorgen
 - ⇒lediglich „Sicherheitspflichten“ gegenüber anderen Benutzern (z.B. Verbot von Aktivitäten, welche die Netzwerksicherheit gefährden) oder gegenüber Anbieter (z.B. „Netiquette“)

5. Sicherheitspflichten von Accesspoint-Benutzern

- Sicherheitspflichten von privaten Benutzern (2)
 - Benutzer trägt Sicherheitsrisiko zwar selber, jedoch ist Anbieter evtl. aufgrund IT-Governance haftbar
 - ⇒ IT-Governance der Unternehmen entlastet unter Umständen den Benutzer (bei Sorgfaltspflichtverletzung)

5. Sicherheitspflichten von Accesspoint-Benutzern

- Sicherheitspflichten von Unternehmen
 - Grundsatz: Benutzer-Unternehmen muss für eigene Sicherheit sorgen
 - ⇒ IT-Governance (Verantwortung gegenüber Stakeholdern)
 - Anbieter evtl. haftbar wegen Verletzung der Sorgfaltspflicht

6. Grenzen der Legalität beim Wardriving

- Was ist Wardriving?
 - Eindringen in ungeschützte, drahtlose Netzwerke (z.B. WLAN) durch private Personen (sog. Wardriver)
 - mit Hilfe eines speziellen Equipments (Laptop, spezielle Software, Antenne, GPS)
 - Hinweis für Netzwerkbetreiber

6. Grenzen der Legalität beim Wardriving

- Rechtliche Konsequenzen (1)
 - Merke: Rechtliche Beurteilung ist nur anhand des konkreten Einzelfalles möglich
 - Kriterien für die Beurteilung:
 - Aktivitäten der Wardriver?
 - Ziele der Wardriver?
 - Verwendete Wardriving-Software?
 - etc.

6. Grenzen der Legalität beim Wardriving

- Rechtliche Konsequenzen (2)
 - Erfüllung strafrechtlicher Tatbestände?
 - Betrügerischer Missbrauch einer Datenverarbeitungsanlage (StGB 147)?
 - Urkundenfälschung (StGB 251)?
 - Unbefugte Datenbeschaffung (StGB 143)?
 - Unbefugtes Eindringen in ein Datenverarbeitungssystem (StGB 143^{bis})?
 - Datenbeschädigung (StGB 144^{bis})?

6. Grenzen der Legalität beim Wardriving

- Rechtliche Konsequenzen (3)
 - Verstoss gegen das Datenschutzrecht?
 - Verletzung des Urheberrechts?

6. Grenzen der Legalität beim Wardriving

- Betrügerischer Missbrauch einer Datenverarbeitungsanlage? (1)
 - Tatbestandselemente:
 - Missbrauch einer Datenverarbeitungsanlage (unrichtige, unvollständige oder unbefugte Verwendung von Daten)
 - Herbeiführen einer Vermögensverschiebung zum Schaden einer Drittperson
 - Absicht der unrechtmässigen Bereicherung

6. Grenzen der Legalität beim Wardriving

- Betrügerischer Missbrauch einer Datenverarbeitungsanlage? (2)
 - Fazit: Tatbestand i.d.R. **nicht** erfüllt
 - fehlende Bereicherungsabsicht des Wardrivers
 - fehlende Vermögensverschiebung zum Schaden einer Drittperson

6. Grenzen der Legalität beim Wardriving

- Urkundenfälschung? (1)
 - Tatbestandselemente:
 - Fälschung von Urkunden (StGB 110 Ziff. 5)
 - ⇒ beim Wardriving: Fälschung von Daten
 - Absicht der Vermögensschädigung bei einer Drittperson
 - Absicht des unrechtmässigen Vorteils

6. Grenzen der Legalität beim Wardriving

- Urkundenfälschung? (2)
 - Fazit: Tatbestand i.d.R. **nicht** erfüllt
 - fehlende Absicht der Vermögensschädigung bei einer Drittperson
 - fehlende Absicht des unrechtmässigen Vorteils

6. Grenzen der Legalität beim Wardriving

- Unbefugte Datenbeschaffung? (1)
 - Tatbestandselemente:
 - Beschaffung von gespeicherten oder übermittelten Daten
 - Daten sind nicht für den Wardriver bestimmt (unbefugte Datenverwendung)
 - Daten sind gegen unbefugten Zugriff besonders gesichert
 - Absicht der unrechtmässigen Bereicherung

6. Grenzen der Legalität beim Wardriving

- Unbefugte Datenbeschaffung? (2)
 - Fazit: Tatbestand i.d.R. **nicht** erfüllt
 - Wardriver greifen auf Netzwerke zu, die eben gerade nicht besonders gesichert sind
 - fehlende Absicht der unrechtmässigen Bereicherung

6. Grenzen der Legalität beim Wardriving

- Unbefugtes Eindringen in ein Datenverarbeitungssystem? (1)
 - Tatbestandselemente:
 - Eindringen in ein fremdes Datensystem (kann auch drahtlos erfolgen, z.B. mit Antenne)
 - Daten sind nicht für den Wardriver bestimmt (unbefugte Datenverwendung)
 - Daten sind gegen unbefugten Zugriff besonders gesichert
 - keine Bereicherungsabsicht

6. Grenzen der Legalität beim Wardriving

- Unbefugtes Eindringen in ein Datenverarbeitungssystem? (2)
 - Fazit: Tatbestand i.d.R. **nicht** erfüllt
 - Wardriver greifen auf Netzwerke zu, die eben gerade nicht besonders geschützt sind

6. Grenzen der Legalität beim Wardriving

- Datenbeschädigung? (1)
 - Tatbestandselemente:
 - Veränderung, Löschung oder Unbrauchbarmachen von gespeicherten oder übermittelten Daten ⇒ beim Wardriving: Veränderung der Daten durch den Hinweis an den Administrator
 - Daten sind nicht für den Wardriver bestimmt
 - Vorsatz (Fahrlässigkeit genügt nicht)

6. Grenzen der Legalität beim Wardriving

- Datenbeschädigung? (2)
 - Fazit: Tatbestand i.d.R. **nicht** erfüllt
 - fehlende Veränderung von Daten
⇒ wird erst dann bejaht, wenn der Informationsgehalt der Daten in einer für den Datenberechtigten **unerwünschten Form** verändert wird

6. Grenzen der Legalität beim Wardriving

- Datenbeschädigung durch Programme? (1)
 - Tatbestandselemente:
 - Herstellung, Einführung, Anbieten etc. von Computerprogrammen, die zur Datenbeschädigung verwendet werden sollen
 - Vorsatz oder Eventualvorsatz \Rightarrow Wardriver weiss oder nimmt in Kauf, dass diese Programme zur Datenbeschädigung verwendet werden

6. Grenzen der Legalität beim Wardriving

- Datenbeschädigung durch Programme? (2)
 - Fazit: Tatbestand i.d.R. **nicht** erfüllt
 - Programme: Zweck der Datenbeschädigung fehlt \Rightarrow Wardriver benutzen nicht spezifische Hacksoftware, sondern sog. Netzwerkanalysatorensoftware
 - fehlender Vorsatz: Wardriver-Organisationen weisen explizit darauf hin, dass ihr Eintritt nur aus Forschungszwecken erfolgt

6. Grenzen der Legalität beim Wardriving

- Verstoss gegen Datenschutzrecht? (1)
 - DSG 4: Grundsätze
 - Personendaten dürfen nur rechtmässig beschafft werden (Abs. 1) und nur zu dem Zweck bearbeitet werden, der (...) gesetzlich vorgegeben ist (Abs. 3)
 - ⇒Merke: Gemäss Art. 3 lit. e DSG gilt **jeder Umgang** mit Personendaten als Datenbearbeitung

6. Grenzen der Legalität beim Wardriving

- Verstoss gegen Datenschutzrecht? (2)
 - DSG 12: Persönlichkeitsverletzungen
 - Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen (Abs. 1)
 - DSG 13: Rechtfertigungsgründe
 - Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht (...) gerechtfertigt ist (Abs. 1)

6. Grenzen der Legalität beim Wardriving

- Verstoss gegen Datenschutzrecht? (3)
 - Fazit: Eintritt des Wardrivers in ein System mit Personendaten gilt als **Datenschutzverletzung**
 - unrechtmässige Bearbeitung von Personendaten (DSG 4 I i.V.m. DSG 3 lit.e)
 - Verletzung des Grundsatzes der Zweckgebundenheit (DSG 4 III)
 - Widerrechtliche Persönlichkeitsverletzung (kein Rechtfertigungsgrund, DSG 13 I)

6. Grenzen der Legalität beim Wardriving

- Verletzung des Urheberrechts? (1)
 - URG 9: Anerkennung der Urheberschaft
 - Der Urheber oder die Urheberin hat das **ausschliessliche** Recht am eigenen Werk und das Recht auf Anerkennung der Urheberschaft (Abs. 1)
 - URG 2: Werkbegriff
 - Computerprogramme gelten auch als Werke (Abs. 3)

6. Grenzen der Legalität beim Wardriving

- Verletzung des Urheberrechts? (2)
 - URG 10: Verwendung des Werks
 - Der Urheber oder die Urheberin hat das **ausschliessliche** Recht zu bestimmen, ob, wann und wie das Werk **verwendet** wird (Abs. 1)
 - Der Urheber oder die Urheberin eines Computerprogrammes hat das **ausschliessliche** Recht, dieses zu vermieten (Abs. 3)

6. Grenzen der Legalität beim Wardriving

- Verletzung des Urheberrechts? (3)
 - URG 11: Werkintegrität
 - Der Urheber oder die Urheberin hat das **ausschliessliche** Recht zu bestimmen, ob, wann und wie das Werk **geändert** werden darf (Abs. 1 lit. a)
 - Selbst wenn eine Drittperson (...) befugt ist, das Werk zu ändern (...), kann sich der Urheber oder die Urheberin jeder Entstellung des Werks widersetzen, die ihn oder sie in der Persönlichkeit verletzt (Abs. 2)

6. Grenzen der Legalität beim Wardriving

- Verletzung des Urheberrechts? (4)
 - URG 12: Erschöpfungsgrundsatz
 - Hat ein Urheber oder eine Urheberin ein Computerprogramm veräußert oder der Veräußerung zugestimmt, so darf dieses gebraucht oder weiterveräußert werden (Abs. 2)

6. Grenzen der Legalität beim Wardriving

- Verletzung des Urheberrechts? (5)
 - Ausgangslage: Wardriver benutzen beim Eintritt in fremde Netzwerke automatisch auch dort eingesetzte Software (auch wenn es bloss das Betriebssystem ist)
 - Nutzung von fremder Software: explizite **Einwilligung des Urhebers nötig** (Lizenz)
 - Keine Einwilligung \Rightarrow Verletzung von URG 10 I und 12 II e contrario)

6. Grenzen der Legalität beim Wardriving

- Wardriver als „gute Täter“?
 - Tatsache: zahlreiche Netzwerke ungeschützt (Beispiele: Mailand 72 %, Paris und London 33 %, Frankfurt 41 %)
 - Awareness bzw. Sicherheitsbewusstsein ungenügend (Schutz wäre relativ einfach möglich)
 - Fazit 1: Aktivitäten der Wardriver als wichtiger Beitrag zur Erhöhung der IT-Security
 - Fazit 2: Vermeidung und Vorbeugung von Schäden und Problemen wird gewährleistet

6. Grenzen der Legalität beim Wardriving

- Zusammenfassung
 - Grundsatz: Wardriving als wichtiger Beitrag zur Erhöhung der IT-Security
 - Aber: Abhängig von den konkreten Aktivitäten der Wardriver im Einzelfall sind **Rechtsverletzungen möglich**
 - Verstoss gegen Datenschutzrecht
 - Verletzung des Urheberrechts
 - Erfüllung strafrechtlicher Tatbestände (jedoch selten)

7. Zusammenfassung

- Accesspoints i.d.R. offen und ungeschützt (Gefahr des Missbrauchs sehr hoch)
- Sicherheitsbewusstsein fehlt bei Bevölkerung
- Es gibt nur wenige Sicherheits- und Informationspflichten für Accesspoint-Anbieter ⇒ interne Weisungen erforderlich
- Das Anbieten und Betreiben eines Accesspoints bedarf einer Dienstkonzession
- Wardriving verstösst nur gegen das DSGVO und das URG, strafrechtliche Tatbestände werden i.d.R. nicht erfüllt