Rechtliche Bestimmungen beim Informationsaustausch in Netzwerken

Du hast jetzt Maßnahmen zur Verringerung der Risiken bei der Nutzung digitaler Kommunikationsformen kennengelernt. Man muss man immer die Risiken und Gefahren im Auge behalten.
In diesem Zusammenhang wurden auch Beispiele und Inhalte zu rechtlichen Bestimmungen besprochen.

Mobbing

Mobbing ist kein eigener juristischer Tatbestand. Verhaltensweisen von Mobbingtätern werden aber vom geltenden Strafrecht erfasst. Das sind Delikte wie beispielsweise:

- Körperverletzung (§ 223 StGB), Beleidigung (§ 185 StGB), üble Nachrede (§ 186 StGB), Verleumdung (§ 187 StGB) oder Nötigung (§ 240 StGB). (Stand: September 2016)

> *Am 22. August 2009 meldete die dpa (Deutsche Presse-Agentur) die erste Verurteilung wegen Cyber-Mobbings. Das betraf eine 18-jährige Britin, die ein anderes Mädchen über Jahre hinweg verbal und körperlich bedroht hatte.*
> *Zuletzt hatte die Täterin ihre ehemalige Schulkameradin in dem sozialen Netzwerk Facebook mit dem Tod bedroht. Dafür musste sie drei Monate in eine Jugendstrafanstalt. Darüber hinaus durfte die Verurteilte fünf Jahre lang weder Kontakt zu ihrer Bekannten aufnehmen noch Kommentare über sie im WWW verbreiten.*

Datenschutzgesetze

Ein besonders schützenswertes Gut sind **personenbezogene Daten**. Das sind Angaben über persönliche oder sachliche Verhältnisse eines bestimmten Menschen.
Personenbezogene Daten sind z. B.: Standortdaten, Gesundheitsdaten, Finanzdaten, Informationen über die Herkunft, politische, religiöse, gewerkschaftliche, sexuelle Orientierung/Gesinnung oder Augenfarbe.
Fotos sind geschützt, wenn für eine bestimmte Person eines dieser Merkmale offensichtlich ist. Daraus folgt das **Recht am eigenen Bild**: Jeder darf darüber bestimmen, ob ein Bild von ihm veröffentlicht wird – es sei denn, man ist nur zufälligerweise auch mit auf dem Bild (z. B. auf dem Foto einer Sehenswürdigkeit).

A Bearbeite das Arbeitsblatt 18, Seite 1: Beispiele zum Datenschutz

Welchen Wert haben Daten? Das kann niemand wissen, denn er hängt stark von der Nutzung der Daten ab. Soviel aber ist klar: Gut vernetzte Unternehmen, die Handel mit Werbenetzwerken, Versicherungen oder Geldinstituten usw. betreiben, gehören zu den Wertvollsten der Welt. Auch App-Programmierer, die Daten an Kriminelle verschachern, können damit durchaus Geld verdienen.

- Personenbezogene Daten können auch für **Identitätsdiebstahl** missbraucht werden: Mit geeigneten Daten kann sich jemand Online für eine andere Person ausgeben. In dessen Namen kann er dann z. B. Warenbestellungen ausführen oder Straftaten begehen. Das könnten Beleidigungen sein oder gefälschte Veröffentichungen, um das Opfer lächerlich zu machen.

Rechtlich ist die Veröffentlichung von Informationen ohne Einverständnis des Betroffenen eine Verletzung des **Persönlichkeitsrechts**. Gesetzlich wird dieses Recht in mehreren Stufen geregelt:

- In der **Datenschutz-Grundverordnung** (DSGVO) der Europäischen Union werden Grundsätze für die Speicherung und Verarbeitung personenbezogener Daten innerhalb der EU festgelegt.
  Geregelt werden insbesondere der Schutz vor einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung und die Gewährleistung des freien Datenverkehrs innerhalb des Europäischen Binnenmarktes.
  Die Datenschutz-Grundverordnung gilt auch für Firmen außerhalb der EU, die Daten von EU-Bürgern speichern und verarbeiten.
  Einzelne Klauseln der DSGVO können in nationalen Gesetzen der Mitgliedsstaaten konkreter geregelt oder eingeschränkt werden.

Diese **Datenschutzgesetze** umfassen in Deutschland:

- Das **Bundesdatenschutzgesetz** (BDSG), in dem der Datenschutz für den **privaten Bereich** (Privatpersonen und Wirtschaftsunternehmen) und für die **Bundesbehörden** geregelt wird.
- Die **Datenschutzgesetze der Länder** für Landes- und Kommunalbehörden.

Die Einhaltung der Datenschutzgesetze wird duch **Datenschutzbeauftragte** kontrolliert:

- Der Bundesbeauftragte für den Datenschutz hat die Aufsicht über die öffentlichen Stellen des Bundes sowie über Unternehmen der Telekommunikations- und Postdienstleistungsbranche.
- Die Landesbehörden und alle anderen privaten Unternehmen unterliegen der Kontrolle durch die Landesdatenschutzbeauftragten.
- Unternehmen, deren Tätigkeit einer besonderen Kontrolle bedarf, müssen einen betrieblichen Datenschutzbeauftragten bestellen.

International anerkannte Datenschutzprinzipien, die in den deutschen Datenschutzgesetzen gewährleistet werden, sind:

- Das Prinzip der **Zulässigkeit und Rechtmäßigkeit** der Erhebung und Verarbeitung von Daten betrifft die Einhaltung der Grundrechte (Würde des Menschen, Persönlichkeitsrecht).
- Nach dem Prinzip der **Richtigkeit** müssen zu verarbeitende Daten überprüft werden.
- Das Prinzip der **Zweckgebundenheit**: Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden und müssen nach einer bestimmten Frist gelöscht werden.
- Das Prinzip der **Verhältnismäßigkeit** bezeichnet den Schutz vor übermäßigen Eingriffen als Merkmal eines Rechtsstaates: Ein Eingriff in die Grundrechte muss *zweckgebunden* sein und daraufhin geprüft werden, ob er *geeignet*, *erforderlich* und *angemessen* ist.
- Das Prinzip der **Transparenz** besagt, dass jeder wissen soll, wer welche Daten über ihn verarbeitet und beinhaltet auch ein **Auskunftsrecht** des Betroffenen.
- Das Prinzip der **individuellen Mitsprache** und des Zugriffsrechts für die Betroffenen.
- Prinzip der **Nichtdiskriminierung**: Besonders sensible Daten, die zur Diskriminierung des Betroffenen führen können, dürfen nur unter bestimmten Voraussetzungen verarbeitet werden (z. B. ethnische Zugehörigkeit oder weltanschauliche Überzeugungen).
- Nach dem Prinzip der **Sicherheit** müssen technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes ergriffen werden, z. B. dass nur berechtigte Personen auf die Daten zugreifen können.
- Prinzip der **Haftung**: Betroffene können evtl. Schadenersatzforderungen geltend machen.
- Prinzip einer unabhängigen **Datenschutzaufsicht** und gesetzlicher Sanktionen.
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

Die wichtigsten **Prinzipien** des Datenschutzes betreffen den Grundsatz der Verhältnismäßigkeit:

- **Datensparsamkeit** und **Datenvermeidung**
- **Zweckbindung**
- **Erforderlichkeit**: Es sollen nur die Daten erhoben werden, die für die Erfüllung der Aufgabe unbedingt nötig sind.
  Daten sind also zu löschen, sobald sie nicht mehr benötigt werden.

A Bearbeite das Arbeitsblatt 18, Seite 2