Rechtliche Regelungen

Staatliche Behörden

Auch staatliche Behörden tendieren zu unbegründeten Datensammlungen. Die folgende Auswahl von Urteilen des Bundesverfassungsgerichts, in denen bereits verabschiedete Gesetze zumindest in Teilen für verfassungswidrig erklärt wurden, spricht für sich selbst:

- 03.03.2004 - Großer Lauschangriff: Das Gesetz ist zu großen Teilen verfassungswidrig.
- 27.07.2005 - Vorbeugende Telekommunikationsüberwachung: Das vorbeugende Abhören von Telefonen ohne konkreten Tatverdacht ist nur unter strengen Voraussetzungen zulässig.
- 04.04.2006: Die Rasterfahndung nach den Terroranschlägen vom 11. September 2001 war rechtswidrig. Zulässig ist sie nur bei „konkreter Gefahr für hochrangige Rechtsgüter".
- 13.06.2007 - Kontostammdaten: Justiz, Finanzbehörden und Sozialverwaltung dürfen auch heimlich Daten von Banken abrufen, also ohne den Betroffenen zu informieren. Das muss aber „im Einzelfall erforderlich sein und sich auf eine eindeutig bestimmte Person beziehen".
- 27.02.2008 - Grundrecht auf Computerschutz: Online-Durchsuchungen („Bundestrojaner") werden eingeschränkt. Das heimliche Ausspähen des Computers ist nur dann zulässig, wenn „Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen". Eine Befugnis des nordrhein-westfälischen Verfassungsschutzes sei nichtig.
- 11.03.2008 - Automatisierte Kennzeichenerfassung: Eine automatisierte Massenkontrolle von Autokennzeichen per Videokamera ist nur mit klaren gesetzlichen Grenzen rechtmäßig. Polizeibefugnisse in Hessen und Schleswig-Holstein seien verfassungswidrig.
- 02.03.2010: Das Gesetz zur Neuregelung der Telekommunikationsüberwachung aus dem Jahr 2008 („Vorratsdatenspeicherung") ist verfassungswidrig.

Fallbeispiel: ***Einschränkung rechtsstaatlicher Prinzipien***

Datenschützer Betzl: Neuer Etappensieg der Terroristen
"Mit den jüngsten Anschlagsversuchen in Großbritannien haben die Terroristen erneut den Ruf nach Online-Durchsuchungen und strengeren Sicherheitsgesetzen ausgelöst. Damit haben sie einen weiteren Etappensieg bei ihrem Kampf gegen die verhassten liberalen, freiheitlichen und rechtstaatlichen Gesellschaftsordnungen des Westens errungen," so Bayerns Datenschützer Betzl, und weiter: "Morde und Attentate erschüttern die abendländischen Gesellschaftsordnungen. Aber die Furcht vor weiteren Attentaten darf nicht reflexartig in den Versuch münden, mehr Sicherheit durch immer neue Freiheitseinschränkungen zu bekommen. Jeder, auch ein Datenschützer, will in Frieden und Sicherheit leben und will, dass Terroranschläge schon im Vorfeld verhindert werden. Dies darf jedoch nicht dazu führen, dass jeder Bürger ohne Ausnahme zu einer sog. "Risikoperson" wird, die einer lückenlosen Überwachung unterliegt. Online-Durchsuchungen gehen hier eindeutig einen Schritt zu weit." Betzl rät: "Bevor die Bundesregierung auf den Festplatten nach Terrorplänen sucht, sollte sie sich lieber um die neuen Geoinformationssysteme kümmern. Diese Systeme ermöglichen es jedem Internetnutzer, metergenaue dreidimensionale Angriffs- und Fluchtpläne für jeden beliebigen Ort auszuarbeiten."
München, 03.07.2007; Karl Michael Betzl; Der Bayerische Landesbeauftragte für den Datenschutz

1. Welche Maßnahmen sind teilweise verfassungswidrig bzw. gefährden die „freiheitlichen und rechtstaatlichen Gesellschaftsordnungen"?

2. Ergänze die Angaben zu Verstößen gegen den Datenschutz in den Beispielen unten.
   (vgl. auch Gesetzestexte auf Seite 3)
   - Verstöße gegen das Datenschutzgesetz:

     In Fallbeispiel 1 und 2:

   - Straftaten nach dem Strafgesetzbuch (StGB):

     In Fallbeispiel 1:

     In Fallbeispiel 2:

Fallbeispiel 1: ***Weitere Spähaktionen bei der Deutschen Bahn***
Am 11. 02. 2009 legte die Bahn einen Zwischenbericht über die Ordnungsgemäßheit der Maßnahmen zur Korruptionsbekämpfung in den Jahren 1998 bis 2007 vor. In der Folge wurden Informationen zu weiteren Spähaktionen bei der Bahn veröffentlicht:
- *Bereits im Jahr 1998 wurde ein maschineller Datenabgleich vorgenommen.*
- *2002 wurden Daten von rund 770 Führungskräften und deren Partnern untersucht.*
- *2003 und 2005 wurden Daten von jeweils rund 170.000 Beschäftigten ausgewertet.*
- *2005/2006 wurden erneut Daten von Führungskräften abgeglichen.*

Am 27. 03. 2009 berichtete das Nachrichtenmagazin Spiegel über weitere Fälle illegaler Überprüfung der Belegschaft durch die Bahn, die mit Korruptionsbekämpfung gar nichts zu tun hatten. Vielmehr sollten Informationsabflüsse zu Presse, Politik und Wissenschaft untersucht werden:
- *Zwischen 2005 und 2008 wurden täglich bis zu 150.000 E-Mails der rund 70.000 bis 80.000 Nutzer des konzerninternen Netzwerks gefiltert. Dabei wurden unter anderem E-Mails von Bundestagsabgeordneten, Verkehrsexperten und Journalisten gerastert.*
- *Nach einer Meldung der Süddeutschen Zeitung vom 27. 03. 2009 wurden E-Mails, in denen die Namen bestimmter Journalisten auftauchten, ohne Wissen der betroffenen Mitarbeiter automatisch an eine interne Kontrollstelle weitergeleitet.*
- *Während des Lokführerstreiks im Jahr 2007 wurden zwei Informationsschriften der Gewerkschaft Deutscher Lokomotivführer (GDL) an die Lokomotivführer nicht nur gelesen, sondern gelöscht.*

Die Deutsche Bahn war und ist nicht das einzige Unternehmen, das Mitarbeiter mit Hilfe illegaler Praktiken ausspionierte. In diesem Fall war aber die Häufung und das Ausmaß der Gesetzesverstöße bemerkenswert. Ein weiteres Beispiel:

Fallbeispiel 2: ***Verstöße im Zusammenhang mit der Deutschen Telekom***
Am 14. 05. 2008 übergab der Vorstand der Deutschen Telekom der Staatsanwaltschaft Material über Verstöße gegen das Fernmeldegeheimnis und gegen datenschutzrechtliche Bestimmungen innerhalb des Konzerns: In einem am 28. 04. 2008 eingegangenen Fax forderte ein Berliner Beratungsunternehmen noch 440.000 Euro für den Abgleich von Telefondaten zwischen Aufsichtsratsmitgliedern und Journalisten. Es stellte sich heraus, dass durch diese Maßnahme in den Jahren 2005 und 2006 undichte Stellen im Vorstand und Aufsichtsrat festgestellt werden sollten.
Am 04.10.2008 wurde bekannt, dass Anfang 2006 über 17 Millionen Datensätze von T-Mobile-Kunden gestohlen worden waren. Bekannt wurde das erst, als im Internet Kontaktdaten von Prominenten angeboten wurden, deren Verbreitung in kriminellen Kreisen eine Gefährdung ihrer Sicherheit darstellen würde. Die Daten enthielten geheime Telefonnummern und Privatadressen von Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern.

Gesetzestexte zur Aufgabe 1

Grundgesetz:

Auszug aus dem Grundgesetz der Bundesrepublik Deutschland, Stand: 09/2017; Artikel 10
(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt."

Strafgesetzbuch:

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses (StGB, Stand: 09/2017)
„(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt
1.eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2.eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt..."

Bundesdatenschutzgesetz:

Bundesdatenschutzgesetz (BDSG) in der Fassung vom 30.06.2017 § 26:
Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

...

(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt."

Die Fallbeispiele sind auch deshalb besonders gravierend, weil nicht nur gegen das eine oder andere Gesetz verstoßen wurde, sondern gleichzeitig gegen das *Grundgesetz, der rechtlichen und politischen Grundordnung der Bundesrepublik Deutschland!*

Rechte der Arbeitgeber

Es muss auch das Recht jedes Betriebes sein, geschäftsschädigenden Praktiken auf den Grund zu gehen. Dafür dürfen aber keine Mittel verwendet werden, die noch über das hinausgehen, was die Polizei darf. Einige Beispiele dazu werden in den folgenden Aufgabenstellungen geklärt.

3. Ergänze die Zulässigkeit folgender Aktionen eines Arbeitgebers nach den Gesetzestexten vorne:
   - Heimliche Kontrollen im Arbeitsverhältnis _____
   - Das heimliche Abhören oder Aufzeichnen von Telefonaten oder das Öffnen privat vertraulich adressierter Post _____
   - Wenn in einem Betrieb die private Nutzung des Internet erlaubt ist oder geduldet wird und der Arbeitnehmer einen privaten E-Mail-Account nutzt, darf der Arbeitgeber _____

     die Internetnutzung oder E-Mails überwachen.
4. Gib zu den folgenden Aufgabenstellungen deine Einschätzung an:
   - Wenn die private Nutzung des Internet in einem Betrieb verboten ist, darf der Arbeitgeber _____

     auf E-Mails und die Internetnutzung zugreifen, als wäre es Geschäftspost.
   - Wenn der konkrete Verdacht einer Straftat besteht, darf der Arbeitgeber _____

     auch Spionagesoftware einsetzen, um einen Arbeitnehmer zu überwachen.

*Fallbeispiel: **Sammlung von Krankendaten***

Im Jahr 2009 gerieten einige Arbeitgeber in die Kritik, weil sie Krankendaten gesammelt hatten, z. B. der Lebensmittel-Discounter Lidl, die Deutsche Post, die Deutsche Bahn und der Autohersteller Daimler (Meldungen vom 04. 04., 13. 06., 04. 08. und 28. 10. 2009).

5. Arbeitgeber dürfen personenbezogene Daten eines Beschäftigten erheben, verarbeiten oder nutzen, wenn dies _____

   Bei besonders sensiblen Daten, etwa dem Grund einer Krankheit, ist eine Datenerhebung _____

*Fallbeispiel: **Videoüberwachung***

- *Am 26. 03. 2008 wurde bekannt, dass der Lebensmittel-Discounter Lidl mit Hilfe von Miniaturkameras in den Filialen z. B. erfassen ließ, wann und wie häufig Mitarbeiter auf die Toilette gehen oder wer mit wem möglicherweise ein Liebesverhältnis hat.*
- *Am 21. 04. 2008 wurde bei der Fastfood-Kette Burger King die Versammlung zur Gründung eines Betriebsrates mit Videokameras aufgezeichnet.*

6. Die Überwachung von Geschäftsräumen mit einer Videokamera ist erlaubt, wenn _____
7. In Räumen eines Betriebs, die nur von Mitarbeitern genutzt werden, ist Videoüberwachung nur zulässig, _____

   der Sachverhalt auf andere Weise nicht geklärt werden kann _____

Computerkriminalität

Kriminalität in Datennetzen erfindet das Begehen von Straftaten nicht wirklich neu. Strukturell handelt es sich um Teilbereiche traditioneller Formen der Kriminalität, wie sie leider schon sehr lange auftreten.

- Von Computerkriminalität wird gesprochen, wenn für Straftaten Computer als Tatmittel oder als Gegenstand der strafbaren Handlung benutzt werden.

Für Computerkriminalität gibt es kein eigenes Gesetzbuch. Vielmehr wird sie durch das Strafgesetzbuch (StGB) abgedeckt.

Nach der *polizeilichen Kriminalstatistik* zählen zur Computerkriminalität:

- Betrug mittels rechtswidrig erlangter Debitkarten (umgangssprachlich: EC-Karten) mit PIN
- Computerbetrug (§ 263a StGB)
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (z. B. PINs und Passwörter)
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB)
- Datenveränderung, Computersabotage (§§ 303a, 303b StGB)
- Ausspähen von Daten (§ 202a StGB)
- Softwarepiraterie (privat oder in Form gewerbsmäßigen Handelns)
- Herstellen, Überlassen, Verbreiten oder Verschaffen von Programmen, die zum Vorbereiten des Ausspähens und Abfangens von Daten dienen („Hackerparagraf“: § 202c StGB).

Ferner zählen zur Computerkriminalität im weiteren Sinne alle Delikte, bei denen die EDV zur Planung, Vorbereitung oder Ausführung eingesetzt wird.

Beispiele für Gesetzestexte des Strafgesetzbuches vom 15.05.1871, zuletzt geändert am 20.11.2015:

§ 202a Ausspähen von Daten
(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.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten („Hackerparagraph“)
(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.

§ 263a Computerbetrug
(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu 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.
(2) § 263 Abs. 2 bis 7 gilt entsprechend.
(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...

Methoden und Formen der Computerkriminalität treten in unterschiedlichen Kombinationen auf. Beispielsweise kann ein Schadprogramm verwendet werden, um an vertrauliche Daten zu gelangen, mit denen dann ein Diebstahl ausgeführt wird.

8. Ordne die Vorgehensweisen den Formen von Computerkriminalität zu und erläutere die Beispiele.

   - **Spionage**: Meist kriminelle Methoden, um unberechtigt an Daten zu gelangen. (Zugangsdaten und weitere persönliche Daten wie Adresse, Bankverbindung, Kreditkartendaten usw.)

     Form von Computerkriminalität:

     - mittels Social Engineering (zwischenmenschliche Beeinflussung):
       - Beim **Phishing** werden
         Es wird oft in Kombination mit Pharming bzw. Spoofing angewandt.
         Unter Spoofing (Verschleierung) versteht man
       - Dumpster Diving bedeutet,
     - mittels Software, z. B. **Trojaner**:
       - Spyware
       - Sniffer
       - Besonders gefährlich sind Keylogger,
   - Unter **Hacking** versteht man im Zusammenhang mit der Sicherheit von Netzwerken,

     Form von Computerkriminalität:

     Beispiele für Methoden des Hackings:

- Software und Hardware („Hacking-Gadgets“) fallen nicht automatisch unter den Hackerparagrafen. Sie dienen oft vorrangig zu Analyse- und Testzwecken – und können auch dafür verwendet werden, in Datennetzen zu spionieren. Menschen mit einem gestörten Verhältnis zu fremdem Eigentum oder zu gesunder Neugier müssen sich also nicht im Darknet umsehen, um an Hacking-Tools zu kommen. Sie können oft legal bezogen werden. Die Bandbreite reicht von kostenlosen Tools zur Netzwerk-Analyse wie DroidSheep, mit dem auch Sitzungscookies für Internetdienste übernommen werden können, bis hin zu WLAN-Routern, die unter anderem für Man-in-the-Middle-Attacken vorbereitet sind, z. B. WiFi Pineapple für etwa 100 US $ (Stand: 09/2017). Auch deren Nutzung ist oft denkbar einfach. Strafbar wird dann erst die Nutzung für kriminelle Zwecke.
  Entsprechend hoch ist daher das Risiko, von einem (unter-)durchschnittlich begabten Menschen, der gar keine Ahnung davon hat, was er tut, ausspioniert oder geschädigt zu werden.

9. Erläutere den Begriff **Man-in-the-middle-Angriff**:

10. Ordne die Vorgehensweisen den Formen von Computerkriminalität zu und erläutere die Beispiele.

- **Sabotage**: Schadprogramme führen unerwünschte Funktionen aus, die teilweise zur mutwilligen Zerstörung fremden Eigentums führen.

  Form von Computerkriminalität:

  - Ein **Computervirus** ist ein Programm,

  - **Würmer** verbreiten sich im Gegensatz zu Viren, indem sie Sicherheitslücken

Fallbeispiel: Im Mai 2004 hatte ein damals 17-jähriger Schüler zwei Würmer namens Sasser und Netsky entwickelt, die weltweit Computer zum Absturz brachten. Der Gesamtschaden wurde auf mehrere Millionen Euro geschätzt. Z. B.

- *fielen bei der amerikanischen Fluglinie Delta Airlines einige Flüge aus,*
- *waren etwa 1200 Rechner der Europäischen Kommission betroffen,*
- *wirkte sich der Wurm bei der Postbank auf etwa 300.000 Rechner aus.*

Geltend gemacht wurden „lediglich“ 130.000 Euro von 142 Geschädigten.

Der Computerfreak wurde wegen Datenveränderung, Computersabotage und Störung öffentlicher Betriebe angeklagt. Er wurde er am 8. Juli 2005 vom Jugendschöffengericht des Landgerichts Verden zu einer Jugendstrafe von einem Jahr und neun Monaten auf Bewährung und 30 Stunden gemeinnütziger Arbeit verurteilt.
Von den Folgen der Entschädigungszahlungen dürfte er aber noch länger betroffen gewesen sein.

11. Mit Hilfe von **Verschlüsselungstrojanern** werden die Daten auf Datenträgern verschlüsselt. Um den Schlüssel zu erhalten, wird ein Lösegeld gefordert (vgl. Lerninhalte 1.8–04, S. 1: Datensicherheit).

> *§ 253 Erpressung (StGB, Stand: 09/2017)*
> *(1) Wer einen Menschen rechtswidrig mit Gewalt oder durch Drohung mit einem empfindlichen Übel zu einer Handlung, Duldung oder Unterlassung nötigt und dadurch dem Vermögen des Genötigten oder eines anderen Nachteil zufügt, um sich oder einen Dritten zu Unrecht zu bereichern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.*

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) rät davon ab, Lösegeld zu bezahlen (Stand: Dezember 2016).

- Nenne die sinnvollste Maßnahme gegen diese und jede Art von Datenverlust.

12. **Denial-of-Service-Angriffe** beinhalten Straftatbestände wie Nötigung oder räuberische Erpressung. Sie werden durch Viren, Würmer oder Trojaner vorbereitet, die unbefugte Zugänge zu Computern und anderen elektronischen Geräten durch eine Backdoor (Hintertür) ermöglichen.

Erläuterung:

> *Fallbeispiel: Am 11.02.2009 wurde ein Tagesschau-Chat mit der Präsidentin des Zentralrats der Juden in Deutschland, Charlotte Knobloch, mit DDoS-Attacken (Distributed Denial of Service) gestört. Der Chat war daraufhin für einige Minuten nicht mehr erreichbar. Sie hatte sich u. a. für ein Verbot der NPD ausgesprochen und den Vatikan kritisiert, weil Papst Benedikt XVI die Exkommunikation des Bischofs Williamson aufgehoben hatte.*
> *Williamson hatte im Jahr 1989 den Holocaust geleugnet und das im November 2008 bekräftigt.*

- *Organisierte Kriminalität* mit dem Schwerpunkt auf (Schutzgeld-) Erpressung liegt vor, wenn mehr als zwei Beteiligte arbeitsteilig Straftaten begehen.

> *Fallbeispiel: „**Schutzgelderpressung im Internet**“ (vgl. c't 7/2001, S. 28)*
> *Angriffe von Hackern wie z. B. der Diebstahl von Kreditkarteninformationen waren bis zum Ende des 20. Jahrhunderts fast ausschließlich Aktionen von Einzeltätern.*
>
> *Dann wurden aber die Möglichkeiten der Internet-Sabotage im Zusammenhang mit dem organisierten Verbrechen erkannt. Der Stellenwert dieser Entwicklung wurde von dem amerikanischen FBI im Jahr 2001 so hoch eingestuft, dass es erstmals in seiner Geschichte detaillierte Informationen zu laufenden Ermittlungen veröffentlichte.*
>
> *Das FBI warnte E-Commerce-Anbieter vor osteuropäischen Gruppierungen, die Daten entwendeten, um die Unternehmen anschließend zu erpressen.*
> *Laut FBI geschah das im Stil von Schutzgelderpressungen: Hacker-Gruppierungen nutzten Sicherheitslücken von E-Commerce-Sites aus, um an Daten zu gelangen.*
> *Anschließend boten die Hacker den Betreibern der Sites einen kostenpflichtigen „Sicherheitsservice“ an: Sie könnten dem Unternehmen gegen Bezahlung garantieren, dass ihre Kundendaten nicht von „anderen Hackern“ gestohlen und missbraucht bzw. weitergegeben würden.*
>
> *Nach FBI-Angaben waren schon im Jahr 2000 über 40 Opfer in den USA betroffen.*

Diebstahl und **Betrug** finden häufig mit Hilfe von unberechtigt erlangten Daten statt. Die Möglichkeiten sind so vielfältig, dass hier ein paar Beispiele genügen müssen:

§ 242 Diebstahl (StGB, Stand: 09/2017)
(1) Wer eine fremde bewegliche Sache einem anderen in der Absicht wegnimmt, die Sache sich oder einem Dritten rechtswidrig zuzueignen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar."

§ 263 Betrug (StGB, Stand: 09/2017)
„(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.
(2) Der Versuch ist strafbar.
(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren..."

- Diebstahl und Betrug finden häufig mit Hilfe unberechtigt erlangter Daten statt (z. B. Geldtransfers mit gestohlenen Zugangsdaten, Diebstahl geistigen Eigentums).
- Beim *Phishing* wird oft gar nicht bemerkt, dass Daten entwendet wurden.
  Diese können verkauft und dann z. B. dazu genutzt werden, das Vertrauen eines Opfers zu erschleichen, um den Verkauf überteuerter Waren zu erreichen.
- Die *Zahlung im Voraus* ist eine beliebte Methode, Internetnutzer zu betrügen:
  Der Käufer erhält eine Rechnung, die er per Banküberweisung begleicht, der Verkäufer liefert erst nach Zahlungseingang.
  Der Käufer hat den Vorteil, dass er keine Bank- oder Kreditkartendaten im Internet hinterlegen muss.
  Der Verkäufer hat die Gewissheit, dass die Zahlung erfolgt.
  Besonders bei Käufen in Nicht-EU-Ländern ist aber die Gefahr groß, auf den Kosten sitzen zu bleiben, wenn der Anbieter nicht liefert.

➢ Wenn Anzahlungen gefordert werden, sollte man zumindest misstrauisch werden!

Beispielsweise die Zahlung über *Western Union*, einem Anbieter für Geldtransfers, ist eine beliebte Methode, arglose Kaufinteressenten abzukassieren.

Fallbeispiel B4: Zu einem extrem günstigen Preis wurde ein Ford Fiesta 1.6 TDCI, nur ein Jahr alt und 15.000 km gelaufen, für nur 4.500 € zum Verkauf angeboten.
Das Auto war angeblich deshalb so günstig, weil der Verkäufer nach England umgezogen war für den Linksverkehr ein rechtsgelenktes Auto brauchte.
Als Voraussetzung für die Abwicklung des Geschäfts forderte der Verkäufer eine Anzahlung von 2.250 € über das Geldtransfer-Unternehmen Western Union.

Der Interessent wurde misstrauisch und holte sich juristische Beratung beim ADAC ein. Dort wird dringend davon abgeraten, Geld im Voraus zu überweisen, wenn man den Verkäufer nicht kennt. Über gefälschte Internetadressen bieten Betrüger Waren an, die es gar nicht gibt und geleistete Anzahlungen sieht ein Interessent oft nie wieder. (vgl. ADAC Motorwelt Heft 2, Februar 2010, S. 16)

13. Gib Beispiel für Methoden des Geldtransfers mit gestohlenen Zugangsdaten an.

Produktpiraterie ist der Verkauf gefälschter Produkte. Insbesondere bei gefälschten Medikamenten kann das zu einer hohen persönlichen Gefährdung führen.
Wenn Geld zur Bezahlung illegaler Kopien urheberrechtlich geschützter Werke geflossen ist, hat das Opfer „nur“ den finanziellen Schaden.

- Produktpiraterie wird häufig als Betrug gewertet, weil Kopien als Originalware angeboten werden.

14. Gib Beispiele für Produktbereiche an, in denen gefälschte Produkte verkauft werden.

Die Veröffentlichung **urheberrechtlich geschützter Daten** ist strafbar!

- In Deutschland ist geistiges Eigentum auch ohne besonderen Hinweis wie z. B. einen Copyright-Vermerk (©) automatisch durch das Gesetz geschützt. Eine Ausnahme bilden nur Werke, die die vom Gesetzgeber geforderte „Schöpfungshöhe“ nicht erreichen.

> *Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG; Stand: 09/2017):*
> *§ 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke*
> *(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.*
> *(2) Der Versuch ist strafbar.*

15. Nenne Beispiele für urheberrechtlich geschützte Daten.

Straftaten gegen die sexuelle Selbstbestimmung treten nicht nur als „Online-Anwendung“ auf.
Datennetze bieten auch eine technische Basis, um konventionelle Straftaten wie z. B. Kinderpornographie „gewinnbringend“ zu begleiten.

16. Geregelt werden Straftaten gegen die sexuelle Selbstbestimmung im Strafgesetzbuch (§ 184b StGB) Verbreitung, Erwerb und Besitz kinderpornographischer Schriften.
    Nenne ein Beispiel für ein Vergehen gegen den (§ 184b StGB.

17. Suche im Internet nach Informationen zu einer Straftat, beispielsweise zu einem Virenbefall.

- **Die Bedrohung durch Computerkriminalität ist vielfältig.**
  - Einerseits muss man sich gegen Angriffe schützen.
  - Andererseits kann man auch durch das eigene Verhalten selbst straffällig werden oder Angriffe provozieren.