Gesellschaftliche Aspekte bei der Nutzung des „Web 2.0“

Im Zusammenhang mit dem „Web 2.0“ ergeben sich noch weitreichendere Konsequenzen als unmittelbare Sicherheitsrisiken bei der Nutzung von IoT-Geräten und Internetdiensten wie z. B. Kurznachrichtendiensten, E-Mail oder bei Waren- und Geldgeschäften.

Zu beachten sind vielmehr persönliche und gesellschaftliche Aspekte beim Umgang mit Internetdiensten. Jeder hat die Möglichkeit, beliebige Informationen verzögerungsfrei zu veröffentlichen.

- Das hat Konsequenzen im Hinblick auf **den Einzelnen**, der – oft vermeintlich anonym – Informationen über seine persönlichen Verhältnisse veröffentlicht. Auch die Suchtgefahr spielt eine bedeutende Rolle sowie rechtliche Bestimmungen: Verstöße gegen das Urheberrecht, das Persönlichkeitsrecht und das Strafrecht wie beispielsweise in schweren Fällen von Cybermobbing.
- Die Meinungsbildung **gesellschaftlicher Gruppierungen** kann beeinflusst bzw. manipuliert werden und moderne Kommunikationsmittel ermöglichen durch das Sammeln und Verarbeiten von Daten erhebliche Eingriffe in die Privatsphäre.

Unseriöse Angebote und Betrug (vgl. Arbeitsblatt 1.4–16, S. 1)

- *Untergeschobene Vertragsabschlüsse* („Abofallen“), z. B. bei Online-Routenplanern.
- *Betrug bei Einkäufen mit Vorkasse* („Eingehungsbetrug“).
- *Gefälschte Angebote* z. B. zur Vermietung einer Wohnung oder auch zum Verkauf eines Autos.

Gefährliche Produkte

- Die *weltweite Vernetzung* macht es möglich, dass Waren ausgeliefert werden, die europäischen Sicherheitsstandards nicht entsprechen.
  Das betrifft z. B. gefährliche Elektroartikel oder gesundheitsgefährdende Materialien.
  (vgl. Arbeitsblatt 1.4–16, S. 2)

Belästigung

- Cybermobbing: Fortgesetztes Ausgrenzen, Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mit modernen Kommunikationsmitteln. (vgl. Arbeitsblatt 1.4–16, S. 4)
- Persönlichkeitsrecht: Werden persönliche Daten, Fotos oder ähnliches ohne Zustimmung des Betroffenen veröffentlicht, verstößt man damit gegen das **Persönlichkeitsrecht**.

Suchtgefahr

Die **Suchtgefahr** ist ein weiteres wichtiges Thema im Zusammenhang mit der Nutzung von Internetdiensten. Sie betrifft nicht nur Computerspiele:

„Die Nutzung des Internets und von PC- Spielen ist alltäglich und selbstverständlich geworden. Diese Entwicklung wird sich fortsetzen und zu einer steigenden Zahl von Online- und Computerspielsüchtigen führen.
Nach verschiedenen Studien gelten bereits heute 3 bis 7% der Internetnutzer als 'onlinesüchtig', ebenso viele werden als stark suchtgefährdet eingestuft. Im Blickpunkt steht dabei die ausufernde Teilnahme an Onlinespielen oder Chats ebenso wie der oft exzessive Konsum von 'Onlinesüchtigen', die durch das Surfen oder Spielen Schule, Beruf und soziale Kontakte vernachlässigen.“ (Bundesministerium für Gesundheit am 04. Mai 2009)

A Bearbeite das Arbeitsblatt 07: Persönliche Aspekte beim Umgang mit Internetdiensten

Datenverlust

- Durch **Sabotage**, z. B. Verschlüsselungstrojaner (vgl. Lerninhalte 1.8–04, S. 1)
- Durch **technische Defekte** und natürliche Alterung bei Datenträgern (vgl. Lerninhalte 1.8–04, S. 2), aber auch durch Benutzerfehler wie versehentliches Löschen von Dateien.

Spionage

- Typische Programme zur Spionage sind (vgl. Lerninhalte 1.8–04, S. 3):
  - **Spyware** sendet Daten eines Benutzers ohne dessen Wissen an einen Empfänger.
  - **Sniffer** zeichnen den Datenverkehr eines Netzwerks auf, um gesendete Daten auszuspionieren.
  - **Keylogger**, kontrollieren Tastatureingaben und können damit beispielsweise Passwörter mitlesen, bevor sie verschlüsselt werden können.
- Ein möglicher Weg ist z. B. auch **Dumpster Diving**: Hier wird Abfall nach Informationen durchsucht.
- Durch **Hacking** werden bei Internetanbietern laufend Daten entwendet.
- **Identitätsdiebstahl** (vgl. Lerninhalte 1.8–04, S. 12)

Veröffentlichung von Informationen

A Bearbeite das Arbeitsblatt 08: Veröffentlichung von Informationen im „Web 2.0“

- Die Kommunikation im Internet ist aufgrund der vermaschten Struktur sehr stabil und ermöglicht die Kommunikation zwischen Milliarden angeschlossener Geräte.
  Das bietet **Chancen** wie z. B. Informationen aus Ländern zu erhalten, in denen die Menschenrechte missachtet werden oder aus Regionen, die von Naturkatastrophen heimgesucht werden. Auch die persönliche Kommunikation zwischen Menschen wird erleichtert, z. B. durch Kurznachrichtendienste.
- Genauso schnell, stabil und dauerhaft können aber auch **Falschinformationen** veröffentlicht werden, die auch den Anschein gut belegter Wahrheit vermitteln können.
  Im Arbeitsblatt wurde nur ein Beispiel für den Wahrheitsgehalt von Informationen besprochen. Klar werden soll: „Fake News ist eine Aufgabe für die gesamte Gesellschaft, auch für Sie ... Es wäre fatal, wenn nur diejenigen den Diskurs bestimmen, die am lautesten schreien und die Facebook & Co. am geschicktesten für ihre Zwecke instrumentalisieren. Dann beherrschen am Ende „alternative Fakten“ die Diskussion und nicht die realen.“ (c’t 2017, Heft 16, S. 73)
- Die *Kriterien für die Beurteilung des Wahrheitsgehalts von Informationen* kann man im Alltag nicht *immer* umfassend nachvollziehen. Genau diese Fragen solltest du dir aber *immer wieder* stellen:
  - Wer ist der **Verfasser**? Hast du von dem Verfasser schon einmal gehört? Ist er Experte? Welchen Ruf genießt er? Informationen, die *anonym* verbreitet werden, sollten dich misstrauisch machen.
  - Wer ist der verantwortliche **Herausgeber**? Handelt es sich um eine anerkannte Organisation oder um eine persönliche Homepage? Gibt es einen Auftritt auch außerhalb des Internets?
    Mit Whois- oder DNS-Abfragen kannst du zumindest feststellen, auf wen die Domain registriert ist. (z. B. https://www.heise.de/netze/tools/whois/ oder ./dns)
  - Wie **aktuell** ist die Information?
  - Bemüht sich der Autor um eine **Trennung von Information und Wertung**?
  - Handelt es sich um **Werbung**? Dann darfst du keine objektive Information erwarten.
  - Sind die Behauptungen im Dokument durch **unabhängige Quellen** belegbar?
- **Ein Aufruf „an alle“** in sozialen Netzwerken kann teuer werden (vgl. Arbeitsblatt 1.4–16, S. 3):
  Ein 20-jähriger Auszubildender hatte in Facebook zu einer Feier auf dem Gelände des Konstanzer Strandbads aufgerufen. Da dies sein finanzieller Ruin gewesen wäre, musste er nicht den kompletten entstandenen Schaden begleichen, sondern „lediglich“ ein paar Tausend Euro bezahlen.
- Dasselbe gilt für **Vergehen gegen das Urheberrecht** (vgl. Arbeitsblatt 1.4–16, S. 3): Ein 13-Jähriger hatte in einem Filesharing-Netzwerk lediglich ein Spiel heruntergeladen. Dafür wurde er zu einer Schadenersatzzahlung von über 1.000 € verurteilt.
  Bietet man Software zum Upload an, wird dieser „Spaß“ noch teurer. Erhält man dafür auch noch Geld, wird dies strafrechtlich relevant und kann auch in eine Gefängnisstrafe münden.

Speicherung und Verarbeitung von Informationen

- Bearbeite das Arbeitsblatt 09, S. 1 – 2: „Gesellschaft 2.0?“
  - ➔ So richtig überraschend ist es nicht, dass Spione das tun, wofür sie bezahlt werden – nämlich zu spionieren. Das Ausmaß der Spionagemaßnahmen, die im Zusammenhang mit dem NSA-Skandal bekannt wurden, war dennoch überraschend.

Diebstahl von Daten

Viel wichtiger als die technischen Details von Methoden zur Spionage ist die Tatsache, dass es gelungen ist, massenhaft Daten des amerikanischen Geheimdienstes NSA zu stehlen. Daraus folgt:

- Daten können selbst bei ausgeklügeltsten Sicherheitsvorkehrungen entwendet werden.

Die Motive von Edward Snowden mögen aus menschenrechtlicher Sicht positiv gewesen sein.
Wer garantiert aber, dass nicht Ziele verfolgt werden, die der Gesellschaft oder Menschen schaden?
Das kann jemand sein, der sich persönlich bereichern will oder ein totalitärer Staat, der die Informationen zur Unterdrückung von Menschen oder zur Destabilisierung anderer Staaten nutzt.

- Bearbeite das Arbeitsblatt 09 S. 3

Der gläserne Bürger

Für das Jahr 1983 war in Deutschland eine Volkszählung geplant. Die Verfassungsklage dagegen stützte sich vor allem auf die Ausführlichkeit der Fragen, die Rückschlüsse auf die Identität der Befragten zugelassen hätten. Somit wäre der Datenschutz unterlaufen worden. Dahinter stand die Befürchtung des so genannten *Gläsernen Bürgers* und damit die Angst vor einem *Überwachungsstaat*.

- Das **Volkszählungsurteil** (BVerfG, 1 BvR 209/83 vom 15. 12. 1983) ist deshalb bedeutsam, weil das Bundesverfassungsgericht darin das **Grundrecht auf Informationelle Selbstbestimmung** formulierte, das sich aus der *Menschenwürde* (Artikel 1 des Grundgesetzes) ableite.

Die dritte industrielle Revolution führte zu einer weitreichenden Neugestaltung des Umgangs mit Daten: Durch Datenverarbeitung können unterschiedliche Datenbestände kombiniert werden. Dadurch lassen sich *Profile* erstellen. Diese Befürchtung ist in dem Begriff *gläserner Bürger* enthalten: Durch die Kombination von Daten in anderen Zusammenstellungen können sich auch neue Sinnzusammenhänge ergeben. Die mit Hilfe von EDV erstellten Profile haben oft mit der Wirklichkeit nichts zu tun. Sie sind also einerseits deshalb so gefährlich, weil sie oft falsch sind**: Informationen können aus Daten nur in einem Sinnzusammenhang gewonnen werden**. Darüber hinaus sind sie andererseits innerhalb von Sekundenbruchteilen weltweit verfügbar und können nochmals weiterverarbeitet werden.
Das sind Gründe dafür, dass massenhaftes Sammeln von Daten als Gefahr für demokratische Gesellschaften angesehen wird. In diesem Zusammenhang wird von einem **Überwachungsstaat** gesprochen.

- Merkmale einer **Demokratie** sind beispielsweise freie Wahlen, Gewaltenteilung oder Achtung der Menschenrechte. Voraussetzung dafür sind z. B. Meinungs- und Pressefreiheit.
  Die **Gewaltenteilung** beinhaltet die Legislative, Exekutive und Judikative, also Trennung in:
  - Gesetzgebung (Parlament)
  - Vollziehende Gewalt (Regierung und Behörden, z. B. Staatsanwaltschaft, Polizei, Finanzämter)
  - Rechtsprechung (Gerichte mit unabhängigen Richtern)

  Die **Unschuldsvermutung** gilt als eines der Grundprinzipien einer demokratischen Grundordnung: Ein Mensch ist solange unschuldig, bis seine Schuld in einem rechtmäßigen Verfahren nachgewiesen wird. Ein Unschuldiger muss nicht seine Unschuld beweisen, sondern eine Strafverfolgungsbehörde muss seine Schuld nachweisen. Das beinhaltet auch, dass ein Strafverfahren nur bei Vorliegen eines Anfangsverdachts eingeleitet werden darf.
- Im Gegensatz dazu herrschen in **Diktaturen** einzelne Personen oder Gruppen. Die Überwachung der Bürger ist eines der Merkmale einer Diktatur, das zu der Unterdrückung der Menschen beiträgt.

- Bearbeite das Arbeitsblatt 09, S. 4 – 6: Der gläserne Bürger

Rasterfahndung

Ein Beispiel für das Erstellen von Profilen ist die *Rasterfahndung*. Hier wird ein *Täterprofil* erstellt und mit gesammelten Daten von Personen abgeglichen. Wenn bestimmte Merkmale übereinstimmen, gerät der Betreffende in den Kreis der Verdächtigen. Es ist also zunächst jeder verdächtig, von dem Daten in dem Datenbestand vorhanden sind. Das ist deshalb so bedeutsam, weil damit die *Unschuldsvermutung*, eines der Grundprinzipien einer demokratischen Grundordnung, zu einer *Schuldvermutung* umgekehrt wird.

A Bearbeite das Arbeitsblatt 10, S. 1 – 2: Rasterfahndung

Die Rasterfahndung ist eine polizeiliche Maßnahme der Bundesländer. Zwischen den einzelnen Regelungen der Länder bestehen inhaltliche Unterschiede. Der Gesetzestext für Bayern lautet:

Auszug aus dem Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz - PAG) in der Fassung der Bekanntmachung vom 14. September 1990:
„Art. 44 Rasterfahndung

(1) Die Polizei kann von öffentlichen und nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten bestimmter Personengruppen aus Dateien zum Zweck des Abgleichs mit anderen Datenbeständen verlangen, soweit dies erforderlich ist zur Abwehr
1. *einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, oder*
2. *einer schwerwiegenden Straftat, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass eine solche begangen werden wird...*

(3) 1 Die Maßnahme darf nur durch den Richter angeordnet werden...

(6) 1 Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Unterlagen, soweit sie nicht zur Verfolgung von Straftaten erforderlich sind und nach Abs. 4 Satz 2 Nr. 2 verwendet werden dürfen, unverzüglich zu vernichten.
2 Die Löschung und Vernichtung ist zu dokumentieren.“

- Für die Strafprozessordnung wurde die Rasterfahndung in Deutschland 1992 geregelt.
  Nach § 98a StPO (Strafprozessordnung) dürfen ausnahmsweise, wenn ein konkreter Verdacht für eine Straftat von erheblicher Bedeutung vorliegt, personenbezogene Daten maschinell verarbeitet werden, um Nichtverdächtige auszuschließen.
- Die Rasterfahndung ist also ein letztes Mittel für Strafverfolgungsbehörden, das in ganz wenigen Ausnahmefällen angeordnet werden darf.
  Dieses Verfahren ist so bemerkenswert, weil die **Unschuldsvermutung umgekehrt** wird, die einen **Grundsatz rechtsstaatlicher Strafverfahren** darstellt:
  - Bei konventioneller Strafverfolgung wird gegen konkrete Zielpersonen ermittelt.
  - Bei der Rasterfahndung hingegen sind zunächst alle Personen potentiell verdächtig. Dann werden aus einem Datenbestand nach einzelnen Merkmalen eines Täterprofils Datensätze herausgefiltert.

Die Möglichkeiten automatisierter Abläufe bei der Datenverarbeitung in Netzwerken sind:

- Große Datenmengen können kostengünstig und praktisch unbegrenzt gespeichert werden.
- Beliebig große Datenbestände können nach bestimmten Merkmalen durchsucht und sortiert werden.
- Unterschiedliche Datenbestände können zusammengeführt und kombiniert werden.
- Verarbeitungs-, Such- und Sortiervorgänge lassen sich automatisch wiederholen.
- Daten können ohne Qualitätsverluste schnell und beliebig oft vervielfältigt und übertragen werden. Sie können dadurch auch leicht entwendet werden:

Es muss nicht immer gleich *der Staat* sein, der Daten gläserner Bürger sammelt und rastert.

A Bearbeite das Arbeitsblatt 10, S. 3: Arbeitgeber

Abhandenkommen von Daten

- Datenbestände müssen auch nicht unbedingt immer gestohlen werden. Sie können auch „einfach mal so“ verloren gehen.

Denn der DAU auf Layer 8 ist immer präsent... Dazu lieferten britische Behörden innerhalb eines kurzen Zeitraums Anschauungsunterricht:
(Anmerkung: *DAU* steht für „**D**ümmster **a**nzunehmender **U**ser“; *Layer 8* bzw. Schicht 8 ist in Anspielung auf das OSI-Schichtenmodell derjenige, der die Software bzw. das Gerät bedient.)

- Am 20. 11. 2007 wurde bekannt, dass in Großbritannien bereits im Oktober des Jahres zwei CDs der Steuerbehörde mit **25 Millionen Datensätzen** abhanden gekommen waren.
  Die CDs enthielten Namen, Geburtsdaten, Sozialversicherungsnummern und Kontodaten von zehn Millionen Eltern und Erziehungsberechtigten sowie sämtlicher britischen Kinder.
  Die Daten wurden auf CDs gebrannt und auf dem Postweg verschickt.
  Dass auch CDs mit Aufzeichnungen von Gesprächen zwischen einem Steuerzahler und der Hotline verschwunden waren, wurde erst am 24. 11. 2007 bekannt.
- Am 23. 12. 2007 teilte das Gesundheitsministerium mit, eine CD mit Informationen über 160.000 kranke Kinder sei auf dem Weg in eine Londoner Klinik verschwunden.
  Auch gespeicherte Angaben zu zehntausenden erwachsenen Patienten würden vermisst.
- Am 19. 01. 2008 teilte das britische Verteidigungsministerium mit, einem Offizier der Royal Navy sei ein Laptop mit Informationen über rund 600.000 Angehörige und Bewerber der Marine, der Marineinfanterie und der Luftwaffe gestohlen worden.
  Wenig später wurde bekannt, dass ein Autofahrer auf einer Straße in Südwestengland Hunderte von Dokumenten mit persönlichen Daten britischer Bürger gefunden hatte.

Natürlich treten bei „Datenpannen“ immer wieder Verantwortliche zurück.
Wahrscheinlich meinen es Mitmenschen, die bewusst Überwachungsaktionen initiieren und ausführen, nur gut: Die Deutsche Bahn hatte noch am 21. 01. 2009 in einer Pressemitteilung behauptet, der Vergleich mit Fällen von Datenmissbrauch Lidl und Telekom in dem Bericht des Wochenmagazins *stern* sei „blühender Unsinn“. Im Gegenteil agiere sie „beispielhaft im Kampf gegen Wirtschaftskriminalität und Korruption“.

Aber genau das zeigt, wie seelenverwandt Figuren wie der „Wohltäter“ und der „große Bruder“ vielen Menschen in der Informationsgesellschaft sind.

Und es zeigt, wie wichtig es ist, dass die Menschen Möglichkeiten der Datenverarbeitung in vernetzten Systemen kennen, um:

- Risiken für den Einzelnen und für die demokratische Grundordnung einschätzen können.
- Das im Alltag zu berücksichtigen.

- Die Datenverarbeitung in Netzwerken birgt offensichtliche und verdeckte Möglichkeiten, durch die der Einzelne und die Gesellschaft geschädigt werden kann.
  Grundbildung in der Informationsgesellschaft beinhaltet also das Entwickeln der Einsicht, dass Daten zu schützen und zu sichern sind, sowie das Beherrschen von Verhaltensweisen und Techniken dazu.
  - Einerseits gilt es also, Daten vor unbefugtem Zugriff zu schützen.
  - Andererseits müssen Daten vor Verlust gesichert werden. **Auch gebrauchte oder weggeworfene Datenträger sind wahre Fundgruben für Datensammler** (vgl. Lerninhalte 1.8–04, S. 12).

Überlassen von Daten

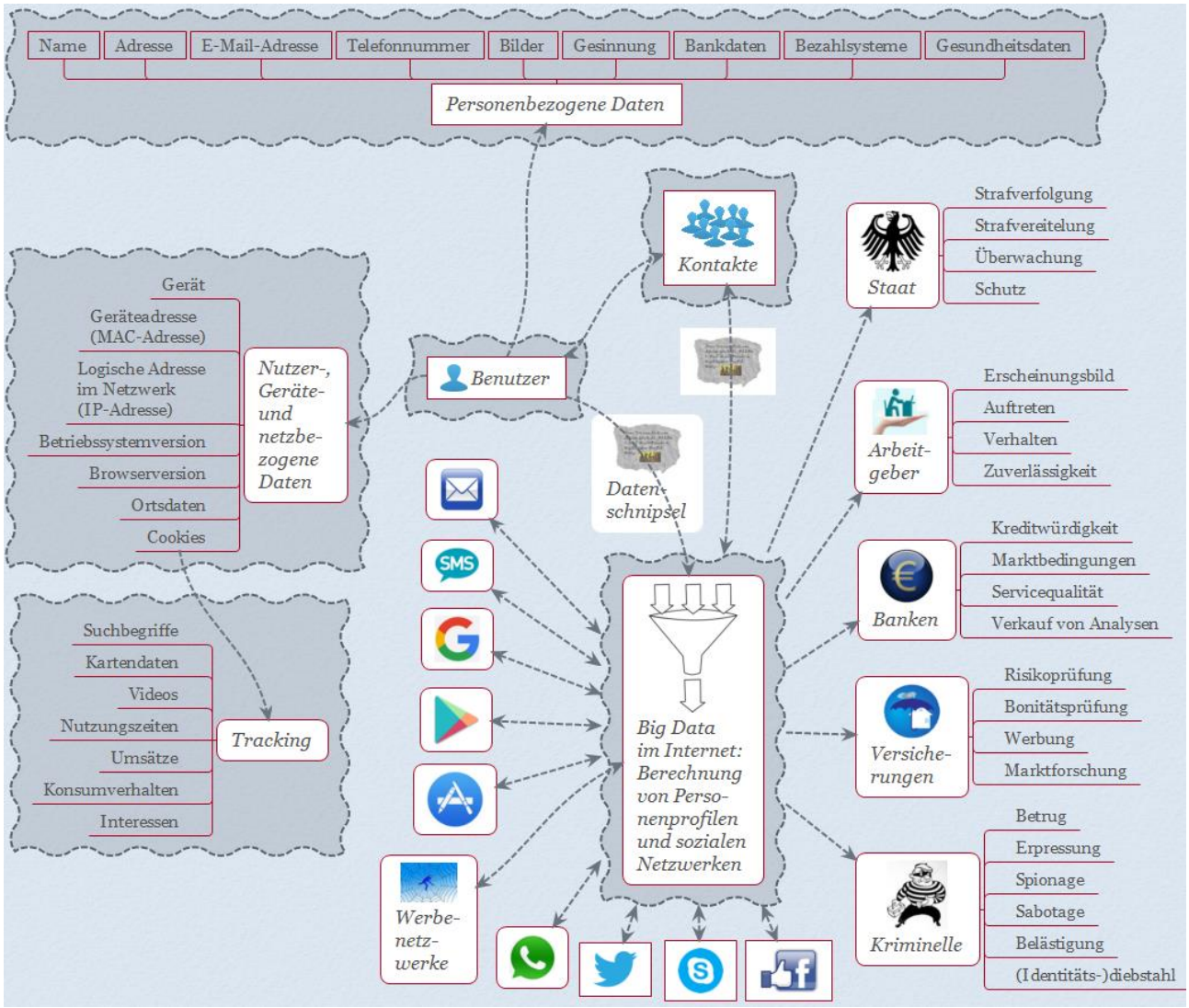
Mit der weltweiten Vernetzung wuchsen auch die Möglichkeiten, Datenbestände zu sammeln und zu kombinieren. Längst ist man nicht mehr auf Daten angewiesen, die durch Kriminelle, staatliche Organisationen oder Arbeitgeber ausspioniert werden. Konsumenten hinterlassen bereitwillig und gedankenlos Unmengen an Daten, die nur eingesammelt werden müssen.

Big data

Unter dem Stichwort *Big Data* werden durch die weltweite Vernetzung einzelne Datenschnipsel aus umfangreichen und vielfältigen Datenbeständen schnell zusammengeführt. Daraus entstehen z. B. Persönlichkeitsprofile, die mit großer Wahrscheinlichkeit korrekte Informationen beinhalten, mit denen Geld verdient werden kann. (vgl. Arbeitsblatt 1-4-18, S. 2 und 1.8-12, S. 6)
Die Daten können aus gestohlenen Datenbeständen stammen oder aus solchen, die abhanden gekommen sind oder von dem Nutzer überlassen wurden. Das sind z. B.:

- Daten, die bei elektronischer Kommunikation anfallen – z. B. Metadaten oder Positionsdaten.
- Aus der Nutzung von Wearables wie Smartwatches, Fitness Tracker, Schrittzähler.
- Soziale Netze und Interaktionen zwischen Nutzern von Social Media.
- Kraftfahrzeugdaten („Vernetztes Auto“).
- Vernetzte Geräte in Wohnungen (Smarthome).
- Von Behörden und Unternehmen erhobene, personenbezogene Daten.
- Daten aus der Nutzung von Payback-, Kunden-, Kredit- oder Debitkarten („EC-Karte“).
- Aufzeichnungen aus Überwachungssystemen.

➢ Eine Zusammenstellung solcher Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person ermöglichen, nennt man **Persönlichkeitsprofil**. In der Grafik sind die Zusammenhänge zwischen der Herkunft von Daten und Interessenten an diesen Daten dargestellt:



A Bearbeite das Arbeitsblatt 10, S. 4: big data