Security, privacy and safety

Basic knowledge | a module of the CUMILA project | www.cumila.eu

Imprint

This document is part of the project "CUMILA - Curriculum guide of media and information literacy for adults".
Name of the module: : "Security, privacy and safety"
KA204-45D50F70
More informationen at https://www.cumila.eu

Publisher / Cooperation Partner:
Medienkompetenz Team e.V.
Sophienstr. 120
76135 Karlsruhe – DE

Akademie für Politische Bildung und demokratiefördernde Maßnahmen
Hauptplatz 23
4020 Linz – AT

CIDET - Centre for the innovation and development of education and technology, S.L
Carrer Pintor Ribera 18
Entresuelo, local 3
12004 Castellón - ES

About this module:

Responsible organisation	**CIDET**
Grafik & Layout	Ann-Kathrin Giuriato
Autoren:	Roger Esteller Curto, Daniel Nübling, Helmut Moritz

It should be noted that, despite careful editing, all information in this document is provided without guarantee and any liability on the part of the publishers and the authors is excluded. .

Co-funded by the
Erasmus+ Programme
of the European Union

Disclaimer:
The European Commission's support for the production of this publication does not constitute an endorsement of its contents, which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

.

Inhaltsverzeichnis

1. Digital identity

Our identity is unmistakable. In real life, we can prove our identity by means of our fingerprint or our identity card. Nowadays, however, everyone also has a digital identity, which enables us to identify ourselves on the internet. This can be done, for example, via a digital signature, an e-mail account or a social media account. And even those who always try not to leave any traces on the internet will not be able to prevent their personal information from ending up on the net in a roundabout way. For example, when other people publish their own personal information such as names, videos, photos or other personal data on the internet. Thus, someone can even have a digital identity without being aware of it.

In this chapter, we will explore the questions of how far we can identify people in the digital world? How do digital identities arise from the personal information we leave behind on the internet (whether consciously or unconsciously)? What risks are associated with this and what value do they have? This should help us to be more careful with personal data and to protect it from unwanted access.

Digital identity		
He/she understands the importance of a digital identity. Especially when dealing with data and creating or sharing content on the internet. He/she knows the risks when dealing with other digital identities.		
Knowledge	**Skills**	**Competences**
He/She • knows the risks in dealing with digital identities • recognises the need to protect their own digital identity • knows the existing methods for verifying an identity •	He/She can • manage their own digital identity and use it for their own purposes. • name and use individual methods for determining identity	He/She is able to • create and maintain a digital identity. • identify and verify the digital identities of other people

1.1 Our second "I"

Sherry Turkle, a psychologist and sociologist and professor at MIT, tries to understand the impact that the internet has on people and society in her book "Second Self: Computers and the Human Spirit". Technical devices like computers and mobile phones are not simply tools that connect us to other people. Through the data we reveal about ourselves and the way we present it to the outside world, we also create a projection of ourselves in the digital world and in this way shape our sense of identity as a second self.

The studies by Turkle and other researchers show us the complexity of the relationship between man and machine. It starts with the fact that on the internet we leave the role of the simple, passive reader and become an active participant who shapes his or her own appearance and impact.

Creating our own identity already starts when we create an account and interact with others (e.g. via email). It is further consolidated as soon as we start publishing our own information (e.g. via our own weblog) and actively participate in communities (e.g. In forums or social networks). The beautiful picture from our last holiday or our pet, the quoted sentence from our favourite author - each of these pieces of information flows into our digital identity.

Our own identity is also shaped by the participation of other people. The picture of us in our friend's public photo album where we are tagged, comments from friends on our social media profiles, the publication of our achievements on the sports club's website: we may have control over what information we publish about ourselves, but we have only limited control over what information other people reveal about us.

AVATAR
The first step towards our individual representation on the internet is the avatar we use as a profile picture. An avatar is the symbol or picture that we use in the digital world, e.g. the classic profile picture on an online service. This picture gives other people a first impression of us and already says a lot about us.

Because of this uncontrollability, a healthy amount of caution is required, but at the same time a lot of opportunities open up.

On the internet today, it is easier than ever to create new identities.

Through our "digital self" we build a new (digital) identity that may well be different from our first (real) one. People can even create more than one identity online, and these do not necessarily have to be related to the real identity. This is not necessarily wrong or forbidden, but rather offers us freedoms to do what we want and let our personal development benefit from it.

Whether it's a gamer account in an online game, a profile on a dating portal, an anonymous account in an online forum - these are all identities that open up possibilities for me on the internet, and I don't have to reveal personal information about them directly.

The internet allows us to create new identities that are perhaps more in line with our way of thinking, bolder, better looking than our true selves.

1.2 Building identities

Through our actions on the internet, we nurture our online identities. This can be observed particularly well in social networks. The photos we post online, the posts we write, share or comment on, the groups we join: all this is information that sharpens our identity.

Social networks are also built on the fact that we network with other people. When we comment publicly on a post, other profiles can see this and respond to it. This puts us in contact with other identities. We have the possibility to follow the activities of other profiles and to comment on them. This builds networks with people of the same interest.

If there is a lively exchange via the social networks with individual online profiles, we are inclined to create our own idea of the person behind it on the basis of the information available to us. The more intensive the exchange, the more we experience the identity of the person we are communicating with as real and friendly. On the social network Facebook, all identities we have linked to are called "friends". The link to another account is created via a "friend request" that has to be accepted. The Instagram network uses a different concept. Here, as a basic setting, everything is public and we can follow other profiles. Instead of friends, we speak here of "followers" - which is far more accurate. Because we will probably never meet the people behind our new online acquaintances face to face. The connection between our identities is only based on a common interest.

Being friends with someone in real life is very different from being friends on the internet. On the internet, we find friends mainly according to specific interests. We don't even have to know the names of our friends' profiles. The exchange usually takes place exclusively online via the corresponding network. The internet allows us to be in contact, to share, to discover, to learn, to create and to enjoy. And all this without any personal contact. We decide what we share and when. The connection is exclusively the common interest.

But the link with other profiles is also part of our own identity. Who we communicate with, which profiles we follow and in which circles we move, in turn says a lot about ourselves. Because of all the information about us, it is possible to create a concrete profile about our identity. This information is used by the providers of the corresponding platforms. The main source of income for the big social networks like Facebook is the sale of advertising. It is precisely because our identities are enriched with so much information that our identity can be assigned to a concrete target group. We are out in nature a lot and comment a lot on the profile pages of the hiking club? We publish a lot of pictures with us and our family? So we could soon have advertisements for children's backpacks or family holidays on the farm displayed.

But identities are not only formed on social networks. Wherever we have an account, we can assume that our activities are stored. the more actively we use the corresponding service, the more extensive our profile becomes. Ever wondered about the accuracy of the products suggested by the online shop? Or about matching advertisements on Google? Ultimately, the decisions of the respective system to show us this information are based on data collected through our behaviour.

1.3 Trust (in identities)

The possibility of establishing one's own new digital identity on the internet offers many opportunities. In the protection of anonymity, some find it easier to open up to others and seek help and advice. Whistleblowers or politically persecuted people can share their knowledge with less danger.

However, anonymity also carries risks. If no one knows my true identity, I don't have to fear the consequences of my actions. Inhibitions fall and the tone in forums and social networks becomes harsher. Discussions turn into arguments in which individual participants are personally insulted.

Fraudsters create false identities and try to make contact, get information or get me to "like" and "share" products and information. If we do not know the person from our "real life" and can thus ensure that he or she is behind the corresponding profile or email, there always remains a residual risk that our counterpart is not who he or she claims to be.

When I receive a contact request from a profile with the name of a person I know: How can I be sure that the person I know is really behind the profile? Ultimately, this is purely a question of trust. Is it possible for me to view the person's profile and can I find enough photos and other information there to confirm the person's identity? What other profiles is the person connected to online? All this information helps me to confirm the identity of the profile.

Trusting connections are created by linking identities. The popular phrase "your friends are also my friends" comes into play especially in social networks. If a profile is already networked with other profiles I am friends with, the probability increases that this is also the person the profile represents. The identity is ensured by the community.

The supposed familiarity with an identity brings with it the danger that we become careless and possibly act without reflection. With the amount of information we put on the internet today, the fact that other people know something personal about us is no proof of identity. Moreover, accounts on social networks have often been taken over by third parties. There are also cases where strangers have created online profiles of other people and posed as them. The person does not have to be an IT expert to do this. All that is needed is an e-mail address. And these can also be created or even misused without further ado. With a stolen email address and some additional information, it is quite easy to create a genuine-looking email that can be used to try to obtain further personal information or even money. At first glance, so-called phishing emails look like they come from our own bank or the online shop we recently ordered from. In reality, however, it has been created by a fraudster whose sole aim is to direct us to a fake website where we are then supposed to enter our customer or account details.

"Trust no one" may sound exaggerated in this context, but a healthy degree of scepticism is something we should fundamentally retain in all our activities in the digital world.

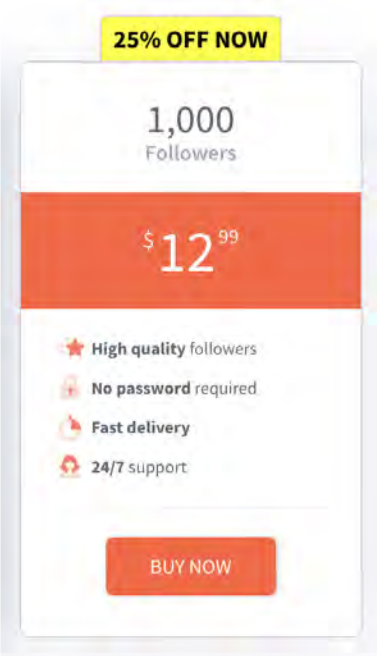
1.4 Fake identities

There are hardly any rules for creating an email address or a profile on a social network. There is also no identity verification. It is therefore possible to create email addresses or accounts on websites under a false name. The large networks make an effort to remove false profiles (fake profiles) as soon as they are recognised as such. According to Facebook's terms of use, these are also not permitted. However, until they are removed, they are online and active for some time.

Facebook alone has been deleting an average of 1.5 billion fake accounts every quarter since 2019.[1] The fake identities are used for different purposes - mostly with fraudulent intentions. For example, fake competitions are published, links to fraudulent websites are shared or attempts are made to establish contacts via the profiles in order to obtain personal data.

On a larger scale, it is not individual profiles that are created, but a whole network of hundreds or more fake identities. The fake profiles are then used to support other profiles, pages or topics.

You have a restaurant and want more positive reviews on a rating portal? Then buy them. You want more "likes" or "followers" on your profile in a social network? Then they simply pay for additional clicks. There are websites where hundreds or thousands of accounts can be bought. And even if this option sounds tempting, it is not advisable. The big providers are very keen to recognise such bought opinions and to take action against them.

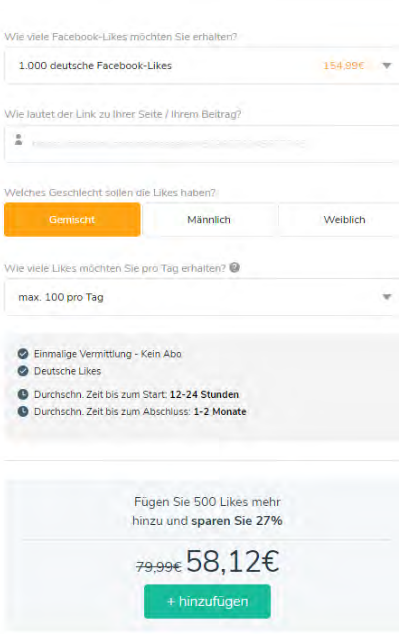


25% OFF NOW

1,000
Followers

$12.99

- High quality followers
- No password required
- Fast delivery
- 24/7 support



Wie viele Facebook-Likes möchten Sie erhalten?
1.000 deutsche Facebook-Likes 154,99€

Wie lautet der Link zu Ihrer Seite / Ihrem Beitrag?

Welches Geschlecht sollen die Likes haben?
Gemischt | Männlich | Weiblich

Wie viele Likes möchten Sie pro Tag erhalten?
max. 100 pro Tag

- Einmalige Vermittlung - Kein Abo
- Deutsche Likes
- Durchschn. Zeit bis zum Start: **12-24 Stunden**
- Durchschn. Zeit bis zum Abschluss: **1-2 Monate**

Fügen Sie 500 Likes mehr hinzu und **sparen Sie 27%**

~~79,99€~~ 58,12€

Links: For just under 13$ you get 1,000 Instagram followers.
Right: For 1,000 German Facebook likes you already pay over 150€. 100 are offered for 19.99€.

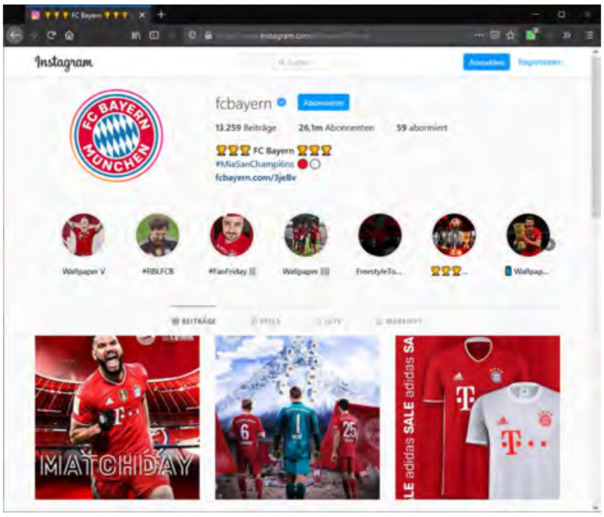
Fake profiles are also used for political purposes. With them it is possible to bring certain opinions and news to the public. The more a topic is discussed, shared and commented on, the more people are reached. Information with a lot of interaction is identified by the networks' automated systems (the "algorithms") as important and "more valuable". Thus, these are given priority and are more likely to be placed in the channels of other users. In this way, targeted attempts can be made to influence public opinion by sharing and commenting more on certain topics over a longer period of time. The fake profiles are controlled and managed automatically via programming. No real persons are needed to become active here.

But how can we distinguish fake identities from real ones? Unfortunately, this is hardly possible, because there is no such thing as one hundred percent certainty. Even the well-known profile of a friend who suddenly sends us strange messages could be manipulated.

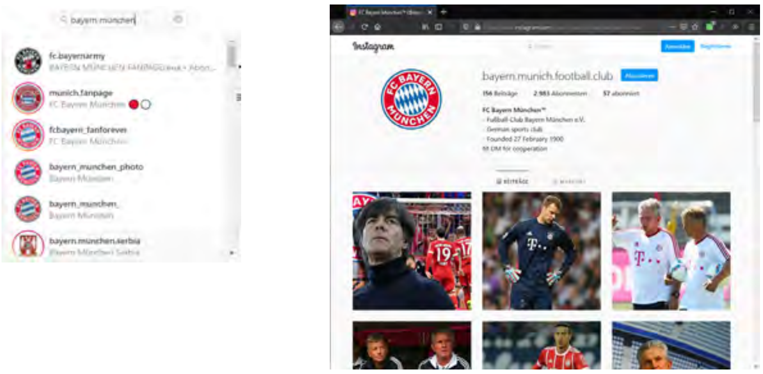
have been made. Here, too, we are left to develop a healthy degree of scepticism and a feeling for how trustworthy a message or a particular profile is.

Important people such as politicians, artists or brands and companies have the option of verifying their profile on the major social media. A verified profile is usually marked with a blue tick. This indicates that the network provider has verified the identity of the owner of the profile. This does not mean that such a profile is safe from abuse, but it at least shows us that the profile is a real identity of the profile owner.

Facebook estimates that fake accounts accounted for about 5% of global monthly active users on Facebook in Q3 2020. 1.5 billion accounts were reverted in Q2 2020 to 1.3 billion in Q3 2020.[29]



The official Instagram account of the football club "Bayern Munich".
It has a blue tick and 26 million subscribers. (Source: Screenshot Instagram.com, 10.04.2021)



Links: If you search for "Bayern München", you will find more profiles.
Right: Among others, the profile "bayern.munich.football.club" can be found here. This profile does not have a blue tick and also only has just under 3,000 followers. This does not have to be a fake profile, but it is not the official profile of the football club. Presumably, this is a profile created by a fan
(Source: Screenshot Instagram.com, 10.04.2021)

1.5 Options for confirming identity

Since we usually move anonymously through the internet, we need ways to authenticate ourselves online. There are various methods for verifying an identity in the digital space. Some of these solutions only ensure that it is a real person, others identify the person by other personal characteristics, such as the phone number.

Companies also use this type of identity confirmation to protect access to our accounts and profiles. They are used at the latest when a suspicious login has been detected. For example, if our login behaviour deviates from our previous behaviour.

1.5.1 Captcha

Captchas are intended to ensure that the visitor to a website is a human being and that the website is not being processed automatically by a programme.

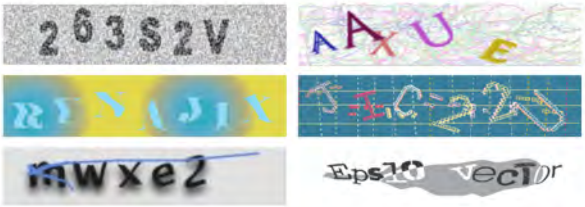
Originally, captchas were represented as a series of numbers and letters, with the representation distorted or with effects. The task of the website visitor is now to enter the string into an input field as confirmation. Since it is difficult for automated processes to identify the symbols correctly, the captcha is a good way to avoid automated, non-human access.

Today, there are different types of captchas. There are arithmetic and comprehension tasks, or also picture series with the task of selecting individual pictures on which a certain object is depicted. All of these are tasks that can only be solved by humans, since a basic understanding of the task is necessary to solve them.

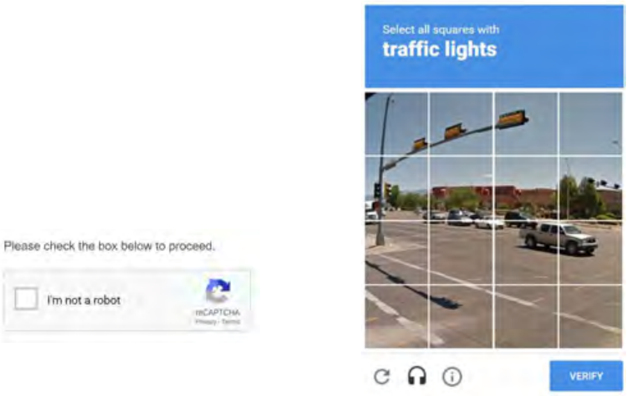
Captchas can be very annoying, but it is a way to avoid misuse and abuse of websites and online applications.

Captchas, however, only prevent automated abuse. A human fraudster is still able to create an account under a false name and impersonate another person.

CAPTCHA steht für "Completely Automated Public Turing test to tell Computers and Humans Apart".
The Turing Test was founded by Alan Turing in 1950. The test checks the ability of a machine to exhibit intelligent behaviour that is equally indistinguishable from that of a human being. The test procedure was outlined by Turing as follows: We converse with a keyboard and screen with two interlocutors whom we cannot see. One of the interlocutors is a human being, the other a computer. If, even after intensive questioning, we cannot say for sure which interviewee is a human being and which is a machine, then the machine has passed the test and is said to have an ability to think that is indistinguishable from a human being.



This is a typical captcha. Additional image interference and distortion is intended to prevent automated image recognition and ensure that only humans can read the characters



Please check the box below to proceed.

□ I'm not a robot

reCAPTCHA

Select all squares with **traffic lights**

VERIFY

Links: A simple method of identification by a separate mouse click.
Right: Another captcha method; identification of elements in a photo (traffic light).

1.5.2 E-mail account

Our email account is our digital mailbox. The associated email address is unique. This makes our email address an important element in identifying us online.

When creating a new account on a website, in almost all cases we are asked for an existing email address. Usually, after successful registration, we receive a confirmation email to our address with a link that we have to click on. With this, the provider checks whether we are actually the owner of this email address or whether we have access to it.

And once we have registered with the provider, the login will in future usually be done via a combination of email address and an individual password. And even if registration is also possible via a user name of our own choosing, the email address serves as a means of identification between us and the provider and, above all, for important functions such as resetting our own password should we ever forget it.

1.5.3 Telephone number or credit card

In addition to an email address, online providers also like to ask for the telephone number or credit card number. An e-mail address can also be created anonymously and quickly deleted again. However, telephone numbers and credit cards are always linked to a person in the European Union.

Online services that ask for this information want to ensure that the user is a real person. As a general rule, this information should only be given out after careful consideration. Do I know the company asking for this information? Am I sure that my data is safe with the provider and will not be passed on to third parties? If you are unsure, you should first read the provider's data protection conditions.

Telephone numbers in particular are often used as an additional component when verifying identity via two-factor authentication.

.

1.5.4 Two-factor authentication

For a long time, websites only used usernames and passwords to ensure that we were legitimate to use the service in question. In this case, once someone got hold of our login details, they had unrestricted access to our account. Two-factor authentication (2FA) adds another layer of security to an account.

It describes a proof of identity by means of a combination of two different factors. In addition to the combination of user name and password, an SMS with a PIN, for example, is sent to a stored mobile phone number. This results in a double check of the identity. Since 2019, the use of two-factor authentication has been mandatory for the use of payment services via an EU directive. But it is also increasingly offered by providers of other services as an additional, optional security mechanism.

Two-factor authentication is mandatory for many services. One of them is credit card payment over the internet. In the EU, it is mandatory that the merchant ensures that the use of the credit card is legitimate. This is possible via an additional step in the authentication process, such as the transmission of a PIN to the customer's mobile phone.

Theoretically, it is also possible to extend the authentication to more than just two factors. This is called multi-factor authentication. The more factors are checked, the more secure the proof of identity is on the one hand, but on the other hand the login process becomes more extensive and longer.

To prevent fraud attempts, providers may require further authentication if they detect suspicious login attempts. If we normally access our online account exclusively from home and then suddenly access it from abroad because we are on holiday, the system may detect a suspicious login attempt and require us to provide additional verification, e.g. in the form of our date of birth, a security question or other information that we have stored in the account.

Additional steps in the authentication should therefore not be seen as annoying queries, because they serve the security of our data.

1.5.5 Digital certificates (e-identity)

A digital certificate is an electronic proof of authenticity issued by a certification authority. In IT, digital certificates are used where the identity of a communication partner or source must be clearly established - for example, in the encryption of e-mails. The same technology is used for electronic proof of identity in the virtual world. [2]

There are government and private sector solutions for electronic identity procedures. In the private sector, it is usually banks or IT companies that provide us with a digital ID that we can use to identify ourselves online, e.g. for online banking.

In the public sector, it is mainly about the digitalisation of administrative processes. In the future, it will no longer be necessary to go to the counter in person and sign our name there. Instead, we will be able to carry out administrative procedures online. The digital identity card will serve as proof of identity. Just as we identify ourselves today with our passport or identity card when crossing the border or going to the bank, we can also do this online with our digital ID.

The European Union's initiative to standardise national IDs is enshrined in Regulation 910/2014.

Digital IDs can eliminate the need for usernames and passwords in operations that require our identification. Our identity is verified via the electronic ID. It is also no longer necessary to sign on paper. By verifying our digital ID, we can submit our signature electronically.

Keypad that contains a card reader. The card contains a chip that stores our digital ID

1.5.6 Biometric data

In addition to the personal data already described, the collection and use of biometric data is also becoming increasingly important. According to the portal datenschutz.org, biometric data "by definition describe personal or person-related information on physical, physiological or behavioural characteristics of an identifiable person". This includes physical characteristics that can be clearly assigned to a person, such as the geometry of the face, the background of the eyes, the timbre of the voice, a dental impression, but also handwriting.

In addition to the unique assignment to a person, biometric data can also be used for authentication. The most widespread method is certainly the unlocking of a smartphone by fingerprint. But some classic computers also already have fingerprint scanners. Research is also being conducted in this area on newer techniques such as the fingerprint of the knuckle or even the tip of the tongue. This may sound strange at first - but if we imagine how difficult it is to obtain the print of the tip of another person's tongue with malicious intent, the aspect of security naturally plays a major role here.

The GDPR classifies biometric data such as DNA, facial geometry or even fingerprints as special categories of personal data. Therefore, they may only be processed in exceptional cases or by consent. Certain biometric data such as facial geometry may even only be collected under certain conditions, for example by the police, and must be effectively protected against unauthorised access.[3]

2. Challenges of the digital world

The digital world offers enormous advantages and conveniences. But we also encounter risks on the internet. These are manifold and also vary in their level of danger. Ultimately, however, they always represent an attack on our privacy and our data. The dangers range from the unwanted disclosure of our data to deletion and destruction.

It is important to know the dangers and their effects. Because if we understand the underlying mechanisms, most risks are avoidable or we can at least minimise them through appropriate behaviour.

Basic tips for protecting our data:

- Adapt behaviour when dealing with digital media - a healthy amount of caution and scepticism is appropriate, especially when dealing with messages from strangers or email attachments
- Use of secure passwords and 2-factor authentication
- Use of anti-virus software and a software firewall
- Updating all important programmes - especially the operating system and the internet browser
- Checking the data protection settings of the online services used - especially in the social networks.
- Regular data backup

Risks on the internet		
He/she knows risks that can affect our privacy and the security of our data and knows strategies to minimise these risks		
Knowledge	**Skills**	**Competences**
He/she can • identify common risks on the internet and know ways to minimise them. • describe the possible effects of knowingly or unknowingly publishing data on the internet.	He/she is able to • understand the common risks and implement appropriate protective measures • recognise dangers and act accordingly. • Assess the value of their own data	He/she is able to • take measures to increase the security of one's own data and privacy on the Internet • develop strategies to protect privacy and one's own data. • to deal with one's own data in a self-determined manner

2.1 Risks on the internet

2.1.1 From data collectors

Our data is valuable. And ultimately, many providers and services want our data. They try to get our email address and other contact details so that, in the most harmless case, they can send us advertising. In the worst case, someone tries to access our data with malicious intent in order to gain access to our accounts.

But how do third parties get hold of our data? This does not necessarily have to be via malware. Especially in social networks, people try to tempt us into action. When we like and comment, we show that our profile is active and that a real person is hiding behind it.

On Facebook in particular, there are many fake competitions that only aim to get our e-mail address. The operators then sell these to advertising partners for a profit. This initially leads to a higher volume of advertising mails and even to advertising calls. It becomes dangerous when our data is deliberately used to obtain further information (e.g. via phishing). The website Mimikama lists over 150 such identified "fake sweepstakes" for the year 2020 alone.[4]

Otherwise, all information that we leave publicly on the internet is also publicly accessible: comments in online forums, on public Facebook pages or even information on our own website. All this information can be collected and analysed. We cannot foresee what effects this may have in the long term. It is not the one small piece of information about us that is problematic, but the accumulation of many pieces of information that can be linked and put in relation to each other.

So-called data brokers collect all kinds of information and then sell our data to other companies. These companies advertise that they have over 250 characteristics about a person.

In addition to information about ourselves, including marital status, level of education, shopping habits and much more, characteristics such as "consumerist" are also stored here. According to its own information, the Bertelsmann Group company "AZ Direct" has profile data on over 70 million people and 41 million households. So it affects us all.[5]

There is no complete protection against data collectors. We can only be more sensitive with our data. We should only ever disclose the data that is needed in the respective application. [6]

2.1.2 SPAM & Phishing

SPAM - Who doesn't know them, the unpleasant e-mails that land in the inbox again and again: Advertisements of uninteresting products, dubious business offers or other unsolicited emails. At the end of 2019, the share of these unsolicited, mass-sent advertising emails was 57% of all email traffic worldwide. And even the best spam filters don't always manage to filter out all unwanted spam emails.[7]

Where does the term "SPAM" come from?
Spam is initially a brand name for canned meat. In the 1970 sketch by the British comedy group Monthy Python, which lasts only three minutes, the word spam is mentioned over 130 times. The word is increasingly incorporated into the conversation and is mentioned so often that it becomes almost impossible to have a sensible conversation. This flooding of the conversation with the word spam parallels the unsolicited emails that are sent en masse every day without being asked and clog up our digital inbox..

The senders of such e-mails are called spammers. They get hold of our e-mail addresses in different ways. Once we have taken part in a competition, we have entered our e-mail address there and agreed to it being used by the advertising partner without us noticing, and our e-mail address ends up in an address database, which is then sold again. But automated programmes that systematically search the internet for email addresses are also used.

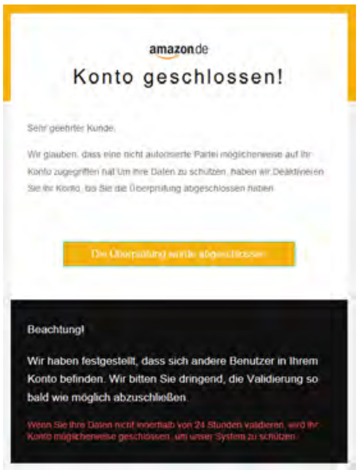
Spam is annoying, but what are the dangers of these emails?

Commercial advertising emails promote products and services in which we have no interest. This type of advertising may clutter up our inbox, but is usually harmless. Nevertheless, we should avoid opening attachments or links in these emails. A link to a website, for example, can transmit an identifier that the spammer can use to identify us. In this case, we confirm that our address is a real e-mail address in use.

Cases of so-called **advance fee fraud** also land in our e-mail inbox. Here, attempts are made to mislead us into certain actions under false pretences: The rich entrepreneur who is dying and wants to give away his fortune;the bank that is looking for the heir of a rich deceased entrepreneur and offers the inheritance in millions. These are all variants of this scam, which has been around since the late 1980s. The best-known variant is the so-called "Nigeria Connection". African businessmen promise large sums of money if we help them move huge amounts of dollars out of the country. Whoever responds to such e-mails is first asked to pay a fee for costs incurred.[8]

Spam is also used to spread **malware**. Viruses, Trojans and other malware are hidden in supposedly harmless attachments. If we open the attachment, the malware is installed on our computer.
Therefore, as a matter of principle, attachments in e-mails from unknown senders should not be opened. And even with known senders, a healthy degree of caution is advisable. It can never be ruled out that another e-mail box has been compromised and is being misused for sending spam.

Equally dangerous is so-called **phishing**. The term is based on the English word "fishing". Here, the fraudsters try to "fish" our passwords and access data. The bait is first of all an email that looks as real as possible, which in its layout and design has been modelled on a real email from the company in question. Our bank informs us that new security rules require us to submit our data again for authorisation. Or an online shop informs us about a routine security check that we have to carry out within 48 hours. All these e-mails link to a fake website and the data we provide ends up directly with the fraudster. The fraudster is then able to plunder our account or steal our identity. This method can also be used to get malware onto our computer.[9]



amazon.de

Konto geschlossen!

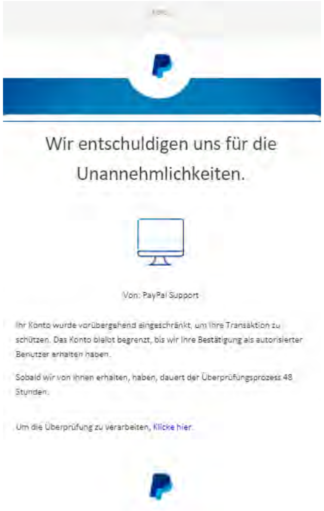
Sehr geehrter Kunde,

Wir glauben, dass eine nicht autorisierte Partei möglicherweise auf Ihr Konto zugegriffen hat. Um Ihre Daten zu schützen, haben wir Deaktivieren Sie Ihr Konto, bis Sie die Überprüfung abgeschlossen haben.

Beachtung!

Wir haben festgestellt, dass sich andere Benutzer in Ihrem Konto befinden. Wir bitten Sie dringend, die Validierung so bald wie möglich abzuschließen.

Wenn Sie Ihre Daten nicht innerhalb von 24 Stunden validieren, wird Ihr Konto möglicherweise geschlossen, um unser System zu schützen.



Wir entschuldigen uns für die Unannehmlichkeiten.

Von: PayPal Support

Ihr Konto wurde vorübergehend eingeschränkt, um Ihre Transaktion zu schützen. Das Konto bleibt begrenzt, bis wir Ihre Bestätigung als autorisierter Benutzer erhalten haben.

Sobald wir von Ihnen erhalten, haben, dauert der Überprüfungsprozess 48 Stunden.

Um die Überprüfung zu verarbeiten, Klicke hier.

LINK: This is not a genuine email from Amazon, but a spam email. Anyone who clicks on the button is redirected to a fake website where we are asked to enter our user names and password.
RIGHT: Fake e-mail from the payment service provider Paypal.
(Source: Verbraucherzentral.de (https://twitter.com/vznrw_phishing)

How can I protect myself?

The most important step to protect yourself from spam is to be prudent in handling your own data and especially your own e-mail address. When choosing your own e-mail address, make sure that you do not disclose your full name. It has also proven useful to set up a second independent e-mail address for legal transactions on the Internet.

From a technical point of view, virus protection programmes, anti-spam filters and regular updates of the operating system and the software used are among the most important measures.

Spam constitutes an invasion of privacy and is illegal. Consumers have a right to have their personal data deleted and can also demand a cease-and-desist declaration from the sender of an advertising e-mail. Phishing e-mails in particular can constitute a criminal offence. Accordingly, criminal charges may also be considered.

In Germany, affected consumers can complain to the eco association.[10] In Austria, a complaint can be filed with the competent telecommunications office if the sender is from Austria.[11]

Otherwise, unfortunately, action can only be taken under the regulations of the spam's country of origin. In many cases, however, the true identity and country of origin of the spammer will not be ascertainable. Therefore, in many cases, a complaint unfortunately remains without effect.

How can I recognise a spam & phishing email?

Spammers often use false subject lines such as "Re: Your registration" or "Class reunion" and fake sender addresses. They pretend to be friends, work colleagues or reputable companies in order to create a personal connection with the recipient and get them to open the mail.

We should be suspicious of the following features and check the email carefully: [12]

- **Check the sender of the e-mail.** Even if the name of my bank or a company I know is displayed as the sender, it is advisable to take a second look at the details. Often, similar-sounding e-mail addresses are used. It is also important to look closely at the domain of the e-mail address (i.e. the part after the @ sign). Instead of the kundendienst@meinehausbank.com, perhaps write meinehausbank123@hotmail.com. In every e-mail programme, there is the option of displaying the details of a sender. It soon turns out that the e-mail from the customer service of an online retailer was actually sent via the e-mail address "infomail01@acshfg.ru", which definitely does not belong to the company.
- **Check e-mails contained in the e-mail.** Most e-mail programs already show the addresses of the websites that are hidden behind a link when you move the mouse over it. This also makes it possible to see whether the link really refers

to the website referred to in the text. Very important: Do not click on the link, but just move the mouse pointer over it for a moment. This allows the link to be displayed and checked

- **Grammatical and spelling errors.** Spam e-mails are often not written in our national language and are instead translated using automatic translation services. This also leads to errors in the character set time and again. The text also often contains special characters or Cyrillic letters.
- **Missing name.** As a rule, we are addressed by our name in emails. Banks, online shops and other online services rarely use general phrases like "Dear customer". But we should not rely on this, as it is quite possible that the fraudsters already know our name and also write to us directly with our first and last name.
- **Unexpected e-mail.** An e-mail reaches us completely unexpectedly? And our bank has never sent us e-mails before? That can also be a characteristic of a fraudulent e-mail.
- **Request to open a file.** We should always be suspicious of e-mails with file attachments. Especially if the sender asks us to open the file or alternatively provides a link to download it.
- **Urgent need for action.** Often we are given a deadline in which we have to act, otherwise our account will be blocked or something similar. This is meant to put us under pressure and make us act quickly. Caution!

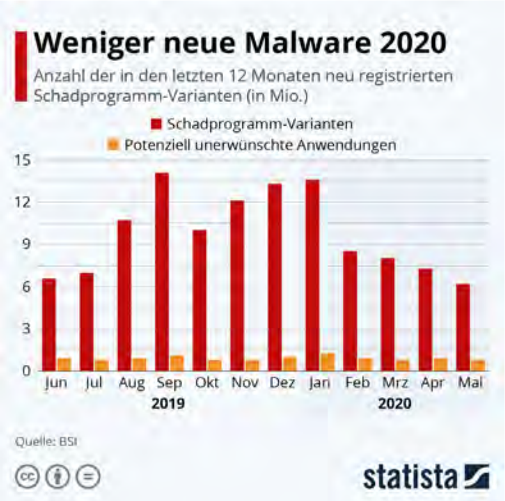
The damage caused by spam and especially phishing attacks can be quite high. However, if you remain a little vigilant and do not trust every e-mail unreservedly, you can protect yourself from this type of fraud.

2.1.3 Viruses, Trojans and other malware

Types of malware

Malicious software (also called malware) is at the top of the list of threats from the Internet. Even though the number of newly registered malware programs has decreased significantly in spring 2020, there are still over 6 million malware variants. So caution is still advisable..[13]

Colloquially, we call all types of malware a "virus". However, computer viruses are only one type of malware. In addition, there are many other variants such as Trojans, worms or ransomware. It is also complicated because not every harmful programme can be clearly assigned to a certain class of malware. What all these variants have in common, however, is that they are computer programmes that were developed to execute unwanted and possibly harmful functions on the end devices of those affected.



The chart shows the number of malware variants that were newly registered in the last twelve months (in millions) (Source: Statista.de)

Computer Viruses & Worms

A computer virus is a programme that causes damage to the computer by damaging important system files, wasting resources or even deleting files. Like a real virus, individual programmes can duplicate themselves and copy themselves to other computers. Unlike the biological virus, however, the computer virus does not "just happen". Computer viruses are programmed by humans and deliberately attack computers and entire networks.

Anyone who catches a virus was not careful enough. Computer viruses can spread in different ways. We ourselves always play a decisive role in the most common ways in which our digital infrastructure can become infected with a virus.

- **E-mails** - these are one of the most popular means of spreading computer viruses worldwide. Most often, viruses are spread via e-mail attachments. Behind a seemingly harmless file with an innocuous name is actually the virus programme we run by opening the attachment. But even an e-mail itself can already carry malware.
- **Instant messaging** - Viruses can also be spread via messaging services such as Skype, WhatsApp and Co. In this case, the virus is spread via chat messages that contain an infected link.
- **Software downloads** - Software or apps can also contain viruses. The supposedly free software contains a virus that is simply installed during the installation. There are also fake anti-virus programmes. Advertisements on websites try to make us believe that a virus has been found on our computer. At the same time, we are offered the corresponding "anti-virus software". But instead of ridding the computer of viruses, the programme infects our computer.
- **Missing software updates** - Time and again, security vulnerabilities are discovered in common software products. In order to close these, the manufacturers regularly publish updates. Those who do not keep their software up to date run the risk of malware being infiltrated onto their home computers via these vulnerabilities.

While the conventional computer virus relies on users passing on an infected file, a computer worm can duplicate itself after the corresponding programme has been run once. Computer worms spread actively over networks without infecting foreign files.

The impact of malware varies.

- The "Stoned" virus only randomly displays the message "Your computer is stoned. Legalize marijuana!" on the screen, but does not destroy any files.
- The "Ika-Tako virus" disguises itself as a music file. As soon as the file is played, the virus replaces all image files on the infected computer with pictures of squids.
- The malware "Loveletter" (also known as ILOVEYOU virus) spread by e-mail in 2000 and infected 45 million computers within 24 hours. Anyone who opened the attachment of the supposed love letter activated the virus, which then automatically deleted all files with certain file extensions.[14]
- In 2003, "Sobig-F" infected a total of 2 million computers. It infected the Windows operating system and automatically sent e-mails from the infected computer to any recipient. Thus, the malware caused one million e-mails per 24 hours. Due to the mass of e-mails sent, many computers were affected. In Washington D.C., data traffic was not possible for a short time due to the virus. Air Canada even had to cancel some flights because of Sobig.F. The damage was estimated at over 37 billion US dollars.[15]
- In 2004, "MyDoom" also infected 2 million computers. This worm also sent itself from infected computers to all contacts it found on the corresponding computer. Due to the massive mail dispatch, it slowed down the entire Internet by about 10%.
- The computer worm "Linux.Wifatch" was discovered in 2014. It infects internet routers without the user's consent. But instead of harming you, it acts as a kind of security service. It does not destroy files, but changes the configuration, removes malware and secures the routers against further infections. A benign virus, so to speak. [16]

Trojan

Who doesn't know it: the Trojan horse. A wooden horse as a gift, but in which the enemy warriors hid. The same principle applies to Trojan software. Behind the harmless legitimate software, malicious software is actually hiding. Believing that we are installing a certain application, we bring the actual malware onto our computer.

Spyware

A spyware is an application that runs covertly on our computer and spies on our behaviour. In the most harmless case, it merely observes our surfing behaviour. More critical are programmes that log our keystrokes (so-called keyloggers). This allows passwords, credit card details and other personal data to be tapped. The malware then sends this data to the respective spyware programmer.

Ransomware

This type of malware encrypts data on the infected system and demands a ransom from the victim - although payment of the demanded sum does not necessarily lead to the decryption of the data. Attack targets are often companies, factories or public authorities. In some cases, entire networks are repeatedly attacked. Ransomware is still considered one of the biggest threats. 30% of German companies state that they have already been affected by a ransomware attack. [17]

Adware

This extremely annoying type of malware floods its victims with unwanted advertising. It is often installed as part of free software. The malware takes root in the operating system and displays advertisements even when the corresponding application is not open.

Web-based malware - drive-by-downloads

A "drive-by download" describes an unintentional and unconscious downloading of malware onto the computer. Nowadays, websites are rarely purely static. In most cases, programme codes are also transmitted with the actual website. It is possible to transfer malware to the computer via these. This is mainly possible through security gaps in our browser or in browser plug-ins we use. Our browser is the security risk here. Therefore, it is advisable to update your browser regularly and thus close any known security gaps.[18]

How do I protect myself from malware?

One of the most important protective measures is the use of antivirus software. Once installed, the software helps to detect any malware. It is important to understand that an antivirus programme can only ever protect against currently known computer viruses. The software must be updated regularly.

Other precautions, such as securing the home network, regularly updating the operating system and the installed software, as well as using a software firewall, are also important components of one's own protection concept.

Even if the aforementioned tools protect us, we must not forget that they are only the last line of defence. The real protection against computer viruses begins with our own behaviour. With a certain degree of caution, we can already protect ourselves well from being attacked by malware.

Firewall
(fire protection wall, fire wall)
A software firewall is a programme that monitors and filters the data traffic of your own computer. It prevents access from outside and is a protection against attacks by worms. It is recommended by the German Federal Office for Information Security (BSI) as a protective measure for Internet use
.

- **Beware of e-mails from unknown senders** - Why would a strange person write us an e-mail? How did the person get our address?
- **Beware of email attachments** - We should not open an email attachment that we are not 100% sure what it is. Even an email from a company we know with an attached invoice can be fake. If we are not expecting an invoice, it makes sense to take a closer look at the email first, and if in doubt, first check with the sender by phone.
- **Don't open every link** - This is especially true for messages that reach us via social networks. We should always be sceptical if we receive a message without context or are asked to click on a link.
- **No hysteria** - We are just on a website and are suddenly surprised with a message that our computer is not secure or already infected by malware? First of all, keep calm. If in doubt, first switch off the computer and, after a restart, have the computer checked via the antivirus programme.
- **Be careful with software downloads** - There is good free and no-cost software. Nevertheless, before downloading, we should make sure that the software can be used without danger and that the website from which we want to download the software is also trustworthy. The rule here is: if in doubt, refrain from downloading

2.1.4 Permissions of apps and software

As soon as we install software on our computer, it gains access to our computer and the data on it. If the installed software is malware, it is quite possible that the application collects information about us in the background and forwards it without our knowledge. However, it does not always have to be malware. The Windows operating system also collects data about its users. But not in secret, but with our consent. The corresponding settings can be found in the system control and in the data protection settings. [19]

On our smartphone or tablet, apps need certain permissions to function properly. A photo editing app needs access to our photos, the navigation app needs access to our location and the online messenger needs a connection to the internet. The access required by the individual app is displayed during installation (Android) or the first start (Apple). In addition, the corresponding information can already be found in the description of the app in the respective app stores.

What permissions do my already installed apps have?
On Apple's iPhone or iPad, the information can be found in the settings under the menu item "Privacy". There, under the individual data categories (e.g. calendar, reminders, etc.), all apps that have requested access are listed. This can be activated and deactivated for each individual app.
For smartphones with the Android operating system, the information can be found under "Apps & Notifications" in the settings. Here, the permissions and notifications for the individual apps can be accessed and changed. With newer Android versions, the "Permissions Manager" can also be found there. All apps are listed here according to their respective permissions. [30]

But who pays attention to exactly what permissions an app asks for? Are we aware of what we are giving our consent to when an app asks us for consent? Why does the weather app need access to our contacts? Why does a social network need to access our camera as well as our address book? And why does the new smartphone game want access to our microphone? Shouldn't we be sceptical about such requests?

Of course, apps need access to certain information on our smartphone. And we cannot always see whether the requested authorisation is really necessary. Nevertheless, we should critically question individual permissions. Especially when it comes to accessing our files, calendar entries, contacts or information about our physical activity and body sensors, we should take a closer look.

In 2018, the New York Times came across the software component "Alphonso", which was used in numerous apps in both the Google Play Store and the Apple Store. If the corresponding app gains access to the microphone, the software eavesdrops on us by regularly recording all ambient sounds. The aim here is to identify television commercials and programmes in order to display corresponding advertisements on the smartphone. Inevitably, normal conversations are also recorded. Shockingly, at the time this became known, there were already around 1,000 apps and games in the Google Play

Store alone that had integrated Alphonso.[20]

Even more frightening, however, is the result of a study published by the International Computer Science Institute in 2019. According to the study, it is possible for apps on an Android smartphone to access certain information without having the corresponding permissions. At the time of the study, more than 1,000 Android apps were identified that bypassed the system in this way. While Google promised to fix the problem with the next Android version (which was released towards the end of 2019), this shows that we cannot always rely on technology. Especially in the software sector, vulnerabilities are found again and again, which are then exploited by third parties

Even if it is tedious, we should check the permissions granted to apps and revoke them if necessary. This can lead to certain functions of the app no longer being available, but it also makes it possible to determine which permissions are really necessary. If an app requires too many permissions or if the requested permissions seem too far-reaching, we should carefully consider whether we really need the app in question and whether we would not rather look for better alternatives.

2.1.5 Micro payments and micro transactions

Micropayments are payments of small amounts. These can be amounts from one cent to five euros, whereby there is no uniform limit.

Behind the principle is the sale of subscriptions or smaller individual items. We pay for the activation of an article on the website of the online magazine or directly own a subscription to the online edition of our daily newspaper. We buy a single piece of music digitally or pay monthly for the music flat rate of a streaming provider. Even apps or games can be offered as part of a monthly subscription. In addition, computer games often offer the possibility to purchase visual features of a game character for a fee. Small amounts can also be spent to purchase special items, new episodes and other advantages in games that the player cannot obtain in the normal way.

The principle of micro payments is widespread in supposedly free smartphone games. These games are usually designed to be playable for weeks and months. To progress in the game, the player must collect certain resources over a longer period of time. Without the use of real money, the player progresses only with difficulty or extremely slowly. The game offers small advantages or the helpful resources in exchange for small amounts of money in its own shop. Appropriate discounts and advertising encourage the player to invest the small amount of a few euros. Often, payment is not made directly with real money, but a diversion is offered via a separate currency that only exists in the respective game (in-game currency). The paid supplements are not bought directly, but first a certain amount of in-game currency, which is then in turn spent in the game shop. An example of this are Poké coins for "Pokemon Go" or jewels for "Clash Royale". The diversions via the in-game currency disguises the real costs. Also, many of these games use mechanisms from the field of gambling to bind the player more closely to the game and create a certain dependency.

For the providers, micro-transactions are a lucrative business. A virtual object is sold, the production of which is usually possible without great production effort. It only has to be produced once and can be copied an infinite number of times.

The danger here is that we quickly lose control of the many smaller amounts and subscriptions. And all the small amounts can add up to larger sums.

In 2019, sales through in-app purchases amounted to around 1.2 billion euros in Germany alone.[31]
99 percent of the market-leading game apps are initially playable for free (free-to-play). Costs are incurred, for example, to acquire additional "lives", to accelerate game progress or to dress one's own game character. Almost every second euro spent on computer and video games in Germany is spent on these free-to-play offers.[32] The most popular titles with the highest global revenues in 2019 include games such as Fortnite (#1, $1.8 billion in revenue), Candy Crush Sage (#5, $1.5 billion in revenue), and Pokemon Go (#6, $1.4 billion in revenue)[33]

2.1.6 Data theft

Anyone who stores their data on their own computer at home is also responsible for their own security. It is possible to secure one's own computer against unauthorised access by taking appropriate precautions. And we can also estimate the probability of a burglar gaining access to our home and stealing our computer including the hard drive.

However, there is also information about us that is not our direct responsibility. This includes all our personal information that we have deposited with countless online services. This includes our emails, our files and photos with the cloud provider or the user account in the popular online shop. In some cases, this data cannot even be managed by us; like the financial data that our bank or the tax office stores about us.

The respective companies and institutions are responsible for the protection of this data. Although we can also contribute to security by protecting our account (e.g. by choosing a secure password), the responsibility for technical security lies with the provider. And even with larger companies, data breaches or data theft can occur, where data either becomes publicly accessible or is stolen by third parties.

Some examples of major incidents in the past:

During the 2006 US election campaign, 20,000 internal emails of Democratic presidential candidate Hillary Clinton were leaked to the public. This hack of the Clinton email server caused a lot of sensation. This hack of the Clinton email server during the US election campaign caused quite a stir. The emails were from the time when Hillary Clinton was US Secretary of State and contained transcripts of conversations that she should no longer have had according to the regulations on handling classified information.

In 2011, there was a data breach at Sony: attackers captured information from more than 75 million users of the Playstation Network online service. Addresses, passwords and even credit card numbers were stolen. As a result, Sony shut down the online service for 23 days.

On 3 October 2013, the company Adobe announced that intruders had been able to capture the encrypted access data and credit card details of around three million users. A short time later, it became known that a second database with user names, passwords and password hints was also affected. This contained 153 million data records. The captured login data appeared on the Internet as a download.

In May 2014, eBay reported that unknown persons had copied a large part of the online platform's customer database. The attackers accessed the company network and the customer database via hacked employee access. Affected were 145 million customer records with name, email address, postal address, telephone number, date of birth as well as the encrypted password.

In 2014, private photos of predominantly female celebrities were published in several waves, all of which were stolen from the Apple service iCloud. These were private images stored in the private iCloud accounts of those affected. The images were sold online for money.

The record-breaking attack on Yahoo at the end of 2014, in which data from 500 million users was tapped, was a case in point. Yahoo, however, had only informed about this in 2016.

In 2014, a database containing 500 million customer records was stolen from Yahoo. However, the theft only became known in 2016. A few months later, however, Yahoo had to admit to a much larger data theft: The data of three billion accounts had already been stolen in 2013.

In January 2019, private data of German politicians and celebrities were published. The data came from various sources. In addition to sources, some of which were publicly accessible, data was also stolen from hacked email and social media accounts as well as cloud services. Private email addresses and mobile phone numbers of those affected were published, as well as bank data and private addresses. In several cases, even private chats with family members were published.

All these examples show that no company is protected from theft. And the number of attacks on companies and public institutions is increasing.[21] In Germany alone, cybercrime caused costs of approximately 87.7 million euros in 2019.[22]

If the worst comes to the worst, the only thing we can do as victims is to change our password or block our bank accounts and credit cards (if these are also affected). We can only take preventive measures by limiting the amount of personal information we disclose to a minimum.

Social Engineering & Social Hacking

Social engineering refers to the emotional manipulation of people to elicit certain behaviours. Closely related to this is social hacking. Here, an attacker tries to influence or deceive a person in such a way that control can be gained over their computer system. The attempt is made to obtain information through direct social contact. The perpetrators fake identities and gain the trust of their victims in order to obtain the desired information. Social hacking is often the first step in data theft. Since technical systems are usually well protected, the attackers make people their own as the weakest link in the data protection chain. For example, the attacker could call a company employee under a pretext, pretend to be a technician and ask for confidential access data. In order to make the call more credible, the attacker has informed himself well about the company in advance or possibly already learned certain internal details through another social hacking action, which he now uses. If, for example, the attacker reports on a project currently running in the company, the call becomes more credible for the person affected.

2.1.7 Data loss

We are responsible for our data. This is especially true for the home computer. A hard disk can break. An external hard drive has a maximum lifespan of 10 years. A built-in, internal hard drive usually only has a lifespan of between 5 and 10 years. And the life of a USB stick is also limited. This is given as a maximum of 30 years. But we should not rely on these values. Especially newer SSD hard drives as well as USB sticks have a limited number of write cycles. This means that the more often they are used, the shorter the life span.

Regular backups of one's own data are extremely important. And we should think about the topic before the first data loss occurs. Anyone who has lost their hard drive with the holiday pictures from the last few years knows how it feels. Unfortunately, we always think about data backup only when it is already too late. With a little luck, it is still possible to recover destroyed data on a hard drive, but such a recovery is quite expensive and success cannot be guaranteed. Therefore, only a functioning backup concept can help.

And even our data in the cloud is not protected against loss, as the incident at the Strasbourg data centre of the company OVH in March 2021 showed. A major fire completely destroyed a five-storey data centre with space for around 12,000 servers. A total of 3.6 million websites disappeared from the network as a result. Those who did not create an additional backup of their data lost their data irrevocably. Such a major fire is of course rather the unfortunate exception, but it shows how quickly data can be lost.

We are responsible for our data. And we have to think about the security of our data before data loss occurs. Otherwise, an old wisdom from the IT sector will be shouted at us:

No backup? No mercy!

2.2 Our data on the web

In all our activities, we leave traces. When we surf the internet, we create a digital footprint. Even when we call up a simple website, our browser exchanges information with the website we visit: Information about our IP address, the browser we use, whether we use a tablet or a computer, what brand it is from, and much more.... All this information may not seem important to us at first glance, but it provides enough material to draw initial conclusions about our person. If information is collected via so-called cookies across several websites we visit, this data can be used to draw a more concrete picture of us.

"What do I have to hide?" is usually the first reaction to this fact. And certainly individual pieces of information are not decisive in themselves. But when a lot of information is collected over a longer period of time and linked to different data sources, you quickly get a complex picture of a person. This ranges from preferences to their political views. If this information is used to display advertising tailored to our individual needs, we may not mind. But what if this data is used to evaluate our person, for example to rate our creditworthiness? And even if the information available about us is not correct: Once we have been automatically pigeonholed, it is difficult to get out of it. The question we should ask ourselves is: "What am I revealing about myself?

Malte Spitz, German politician and activist at "netzpolitik.org", dared an experiment in 2009: He gained access to the data of his mobile phone provider. In the period from August 2009 to February 2010, his mobile phone revealed information more than 35,000 times. Each of these is insignificant and harmless in itself. However, in cooperation with the newspaper "Die Zeit", the data was enriched with information publicly available on the net (e.g. messages on Twitter, blog posts, etc.). In this way, a clear picture of the person Malte Spitz emerged: habits and preferences suddenly become clear and allow conclusions to be drawn about his person and his private life.[23]

The example shows what data reveals about us and what is possible with the analysis of data. And the more data is collected about us, the more accurate and detailed the profile that can be created about us without our knowledge.

For a long time, there have been offers that deliberately offer us something in return for the transmission of our data. Health insurance companies, for example, offer tariffs in which we can receive a bonus if we regularly transmit our health data and can thus prove, for example, that we have exercised to a certain extent. Data has become an important commodity. By collecting data and linking different data sources, new insights can be gained. What models of use exist for our data? Can data also be used against us? Only if we know the mechanisms and effects of such data evaluations is it at all possible for us to recognise risks and deal with our data in a self-responsible and self-determined manner.

2.2.1 The value of our data

Why should anyone be interested in my data?
First of all, certain bodies need certain information for different reasons. A retailer needs my address to be able to send me goods. At my sports club, I leave my phone number so that I can be reached in urgent cases.

But there is also data that is automatically collected about me: My bank knows the movements on my account, my mobile phone provider stores the numbers I call and who call me, as well as the call duration and also my location data. I consented to most of this processing when I signed a contract with the respective provider. As a rule, we do not know what happens to the data. Nor does the processing of my data always have to be to my disadvantage. I may not complain to my favourite online shop if it suggests suitable items to me based on my previous purchases and comparison with other customers

But the more data a company has collected about me, the more concrete conclusions can be drawn about my person and the more valuable this data is. This value usually becomes clear when a company is sold or goes public. Facebook paid the equivalent of 55 US dollars per user when it took over WhatsApp. For Instagram, it was just under 20 US dollars. Both services are free to use.

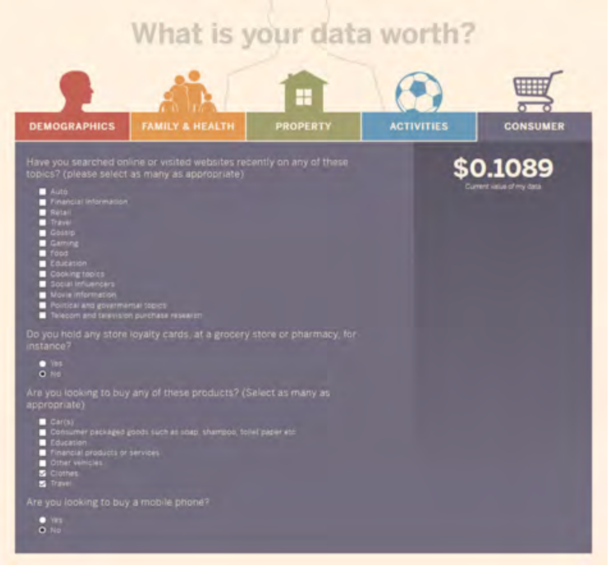
And Google also earns $34 per user per quarter.[24] And this despite the fact that we pay nothing for using Google's services. How does that work?

The answer lies in advertising. In 2019, Facebook made $69.66 billion in revenue from advertising alone.[25] Google even of over 130 billion.[26] This is mainly due to the data that is collected about us. The more data we reveal about ourselves, the more concretely companies can form a picture of us. This in turn enables them to sell advertising tailored to us. You are a company and want to advertise in the target group of single young women between 25 and 29 with a certain average income? No problem!

But it's not always just about advertising. Navigation devices transmit their position to the control centre, which then predicts the likelihood of traffic jams and shows the corresponding warning on our display. Operators of internet applications observe user behaviour and thus know when the services are used by many people. Accordingly, this data can be used to provide more computing capacity at peak times. All this is based on the observed user data.

As early as 2013, a study showed that it is possible to draw conclusions about highly sensitive personal characteristics of a person based on easily accessible information such as Facebook likes. Be it sexual orientation, ethnicity, religious and political views, age, gender and other personality traits. The researchers were able to create psycho-demographic profiles based on Facebook likes. The model was able to correctly distinguish between gay and straight men in 88% of cases and between Democrats and Republicans in 85% of cases.

It is difficult for us to assign a concrete value to the individual data. What is the value of the movement profile that my smartphone automatically creates? What is the value of knowing who I have had regular email contact with over the last few months? The value of data is not universal and is very abstract. It is highly dependent on the quality and purpose and other circumstances. Data is therefore more like raw materials. We need to be aware that our data can be valuable to others.



Have you searched online or visited websites recently on any of these topics? (please select as many as appropriate)

□ Auto
□ Financial information
□ Retail
□ Travel
□ Gossip
□ Gaming
□ Food
□ Education
□ Cooking topics
□ Social influencers
□ Movie information
□ Political and governmental topics
□ Telecom and television purchase research

Do you hold any store loyalty cards, at a grocery store or pharmacy, for instance?

○ Yes
● No

Are you looking to buy any of these products? (Select as many as appropriate)

□ Car(s)
□ Consumer packaged goods such as soap, shampoo, toilet paper etc
□ Education
□ Financial products or services
□ Other vehicles
☑ Clothes
☑ Travel

Are you looking to buy a mobile phone?

○ Yes
● No

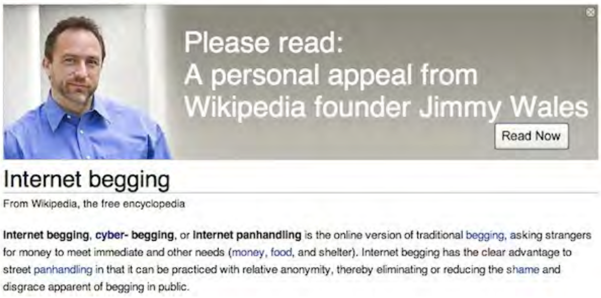
How much is our data worth? The Financial Times website illustrates this with its own configurator.
Source: https://ig.ft.com/how-much-is-your-personal-data-worth/ (englische Sprache)

2.2.2 Nothing is free - we trade performance for data

At the beginning of the popularisation of the internet in our households, we used the internet to read the news and magazines. We could get information without paying instead of going to the newsstand and buying a newspaper. Since then, printed newspapers have dwindled, putting the traditional business model in jeopardy. It was nice to get information online for free, but it was not a sustainable business model for media companies.

We grow up with the internet and got used to getting things for free, and then we thought that's how it should be. Nothing could be further from reality and now we are faced with how media companies, in order to maintain quality, require us to subscribe to some sections of the website or they limit the amount of pages we can access online.

Wikipedia also asks for donations from time to time - you probably know a banner that appears on Wikipedia once a year for a few days:



Please read:
A personal appeal from
Wikipedia founder Jimmy Wales

Internet begging

From Wikipedia, the free encyclopedia

Internet begging, **cyber- begging**, or **Internet panhandling** is the online version of traditional begging, asking strangers for money to meet immediate and other needs (money, food, and shelter). Internet begging has the clear advantage to street panhandling in that it can be practiced with relative anonymity, thereby eliminating or reducing the shame and disgrace apparent of begging in public.

A request for donations on the website www.wikipedia.org

If we, as internet users, want to continue to have access to high-quality news at any time, we have to say goodbye to the widely existing attitude that news on the internet has to be free of charge. Otherwise, the only options left to publishers are to become financially dependent - but this contradicts the principle of "independent journalism" - or to reduce the quality of what they offer. At the moment, for example, one observes that news portals are increasingly blocking users with activated AdBlockers - these are additional programmes that suppress advertisements. After all, how are the editorial offices supposed to finance their work if even the source of income from advertising disappears? It is to be expected that in the near future we will only be able to read a fraction of the news freely, and for all further contributions at least a login with deactivated ad blocker, or else a subscription will be required. The free press is the fourth estate in a democracy - we should ask ourselves what it is worth to us and how much economic pressure we want to put on this important authority.

2.2.3 Metadata

Metadata contains additional information about characteristics of data. The metadata of a book includes the name of the author, the ISBN number, the year of publication and the edition. This is information that can be assigned to the book as an object but does not describe the content of the book. In the digital world, metadata usually remain hidden from us. They are hidden in the files, for example. The file of a digital photo, for example, contains information about the camera with which it was taken, all the technical settings of the shot (e.g. information about the focal length, ISO, exposure time) as well as information about the time and place of the shot (if a GPS signal was available when the picture was taken). All this information is automatically saved in the image file. When we make a phone call, our phone provider learns, among other things, our location and the location of the person we are talking to, as well as the duration of the call. And even when we merely call up a website, information about us is transmitted via our browser. [27]

By metadata in the context of our data on the internet, we mean the inventory and traffic data of a user.

- Inventory data: This is the data that a telephone or internet provider stores, sometimes permanently, about its users. This can be: Address, account data, IP addresses, passwords, telephone numbers and everything that is required to provide the service.

- Traffic data: This is data that accumulates when a service is used and usually has to be deleted after a certain period of time. This includes, for example, who I connected to by phone or internet, which browser I used or at what time this took place

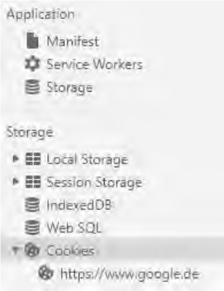
And it is the traffic data that tells more about us than we might suspect - in particular the browser we use with the configuration and location that we automatically transmit based on our IP. In the worst case, a website can, for example, recognise that we have not yet carried out the last security update and just reveal a vulnerability. Ultimately, it is even quite likely that we transmit so much information with our browser alone that we are already clearly identifiable.

This can be tested with the "Cover Your Tracks" test of the "Electronic Frontier Foundation". This checks the metadata transmitted by the browser and determines whether this tends to be a unique combination. For example, the time zone transmitted, the browser plug-ins installed, the screen size, the fonts installed, the language set, the operating system, the memory available, JavaScript support - and these are just some of the parameters - are interpreted. The sobering result: even the metadata of our browser is enough to recognise us unambiguously.

.

2.2.4 Cookies

Since the General Data Protection Regulation (GDPR) came into force in 2018, websites must inform their visitors about the cookies used and the purposes for which they are used by the website operator. Therefore, most internet users have certainly already come into contact with the term "cookies", although probably only very few know what these are and what purpose they have.



Cookies can be stored by websites in the browser memory. The illustration shows the application area of the Google Chrome browser after a single visit to the Google homepage.

Cookies are small text files that websites store in the visitor's browser. The most basic use of cookies is to track our activities within the website we have just accessed. This is valuable information for the website operator. They are not aimed at collecting and passing on our interests, but rather the website owner wants to know which pages of his online offer are visited most often, when visitors return, how many minutes are spent on the website or which was the last page we visited. This is usually statistical information that does not reveal any deep personal information. Many cookies are therefore harmless and a support for the website operator to be able to design his offer in a more user-friendly way.

There are also "technically necessary" cookies that are used, for example, to carry out the ordering process in an online shop. In this case, the website temporarily remembers the user and the products in the shopping basket via the cookie so that it can access them at a later time. Information such as the set language or other basic settings can also be saved via the cookie.

Ultimately, however, cookies are also used to track our surfing behaviour.

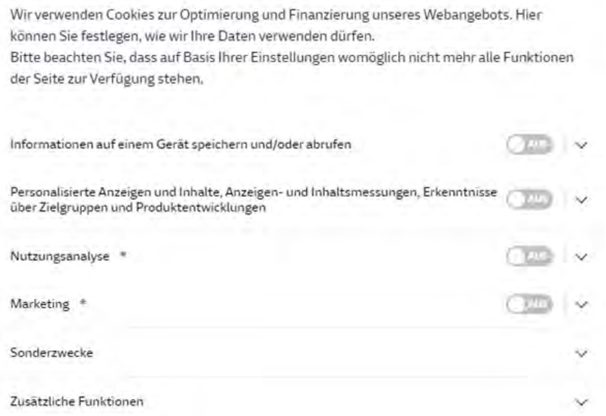
This is how our search queries can be stored in search engines or online shops. If we search for a hotel in Paris or for a new refrigerator, we will find that we are suddenly shown advertisements on other websites that refer to this information. These are cookies with the purpose of so-called "personalised ads and content".

Cookies therefore make it possible to identify us on the basis of the browser and the information available about it - or more precisely: to recognise our previous actions.

Whether we are reading the news, buying products or searching for information, if websites store cookies on our device, this information may - with our consent - be passed on to so-called advertising networks (ad networks). Based on our data, these networks offer advertisers the opportunity to show us targeted personalised content and advertising.

Most of all websites on the internet use cookies. Since the introduction of the GDPR, all websites must inform us about the use of cookies and obtain our consent to process our data. Therefore, on websites we are first asked for our consent to the use of cookies.

The website operators thus fulfil their obligation, but for us it is still not always clear what data is collected from us when we visit the website and what happens to it. Anyone who has taken the trouble to look at the details of a so-called cookie banner will see that it is certainly possible to specifically release our information. However, the handling is usually complicated. Therefore, many click away the corresponding messages and thus usually accept the use of cookies. But do we actually know what we have agreed to?



Wir verwenden Cookies zur Optimierung und Finanzierung unseres Webangebots. Hier können Sie festlegen, wie wir Ihre Daten verwenden dürfen.
Bitte beachten Sie, dass auf Basis Ihrer Einstellungen womöglich nicht mehr alle Funktionen der Seite zur Verfügung stehen.

Informationen auf einem Gerät speichern und/oder abrufen

Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen

Nutzungsanalyse *

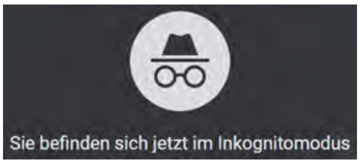
Marketing *

Sonderzwecke

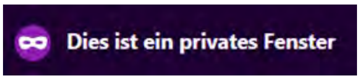
Zusätzliche Funktionen

Cookie information on a news portal (sz.de - screenshot from 30.3.21).
The GDPR requires that information about the purposes of cookies is provided transparently.

If we are concerned about reducing the amount of information transmitted, one possible step is the so-called private or incognito mode of our browsers.



Sie befinden sich jetzt im Inkognitomodus



Dies ist ein privates Fenster

Links: Incognito icon in Google Chrome
Right: Private window in Firefox

Google Chrome and Firefox offer a very simple way to open an incognito window or a private window. In this mode, all cookies and data stored in the browser are removed as soon as we close the window. However, this does not mean that we surf completely anonymously: Any information we submit via a website (email address, credit card details, etc.) or visit in an authenticated context can still potentially be linked to our person. In this context, incognito simply means that all information that the browser can reveal about us is automatically deleted when it is closed.

An example: You want to surprise your partner with a trip and are looking for a hotel via the internet. If you do this via a private window, your booking remains valid - because you have authenticated yourself and transferred credit card data, for example - but your search history can no longer be traced:

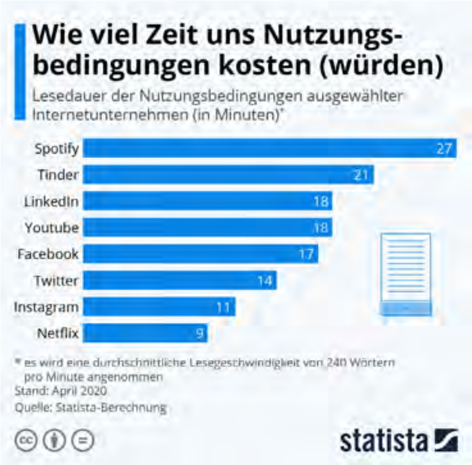
The tracks to the search are covered, and the surprise is not revealed, at least in this way.

2.2.5 Terms of Use - Informed Consent?

When creating a user account, installing a programme or an app, a long text appears that we are supposed to accept in order to be able to use the programme. Depending on the legal situation of the programme, these are the terms of use or the general terms and conditions. From a purely legal point of view, these documents are of great importance because they regulate the services provided as well as the rights and obligations between the provider and the consumer. According to Statista, reading the terms of use of prominent internet applications takes up to 27 minutes - not counting whether they can be understood and whether we can make an informed decision. In addition, we ultimately have no choice but to agree to the terms of use if we want to use the software. In general, the legislator demands that the wording of the conditions must be clear and understandable. But do we actually know what we are agreeing to? Who has ever read the terms of use of a software or app?

As an April Fool's joke, Gamestation wrote in its T&Cs on 1 April 2010: ***"By placing an order through this website on the first day of the fourth month of 2010 Anno Domini, you agree to grant us a non-transferable option to claim your immortal soul for now and forever. Should we wish to exercise this option, you agree to relinquish your immortal soul and any claim you may have to it within 5 (five) business days of receiving written notice from gamestation.co.uk or any of its duly authorised subordinates."*** Through this, Gamestation now theoretically owns the souls of 7,500 customers.

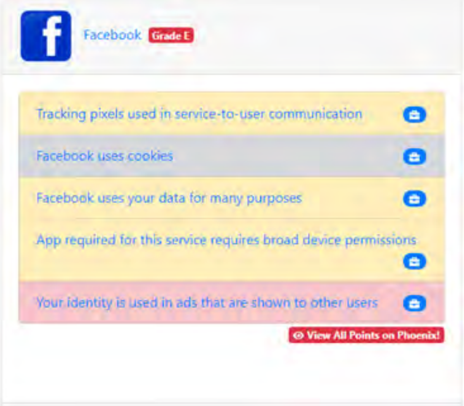
Amazon used the T&Cs of its new game engine Lumberyard for marketing purposes when it launched it. In the US version of the T&Cs, the company referred to the fact that certain usage restrictions would not apply in the event of a zombie apocalypse. The section was hidden towards the end of the more than 50-page Amazon Web Services (AWS) Terms of Service.



Assumed reading time of prominent terms of use in minutes
Source: https://de.statista.com/infografik/21430/lesedauer-der-nutzungsbedingungen-ausgewaehlter-internetunternehmen/

Of course, there are also many positive examples where terms of use are described in an understandable way - even if they may be very long. But there are also many applications where it is difficult to see from the terms of use what is actually legally agreed in the contract between the operator and us, the consumer. Initiatives like "Terms of Service; Didn't Read" try to explain the terms of use in an understandable way so that users can quickly get an overview of what they are agreeing to or may have agreed to in the past.

.



Facebook Grade E

Tracking pixels used in service-to-user communication

Facebook uses cookies

Facebook uses your data for many purposes

App required for this service requires broad device permissions

Your identity is used in ads that are shown to other users

View All Points on Phoenix!

Evaluation of the terms of use on "Terms of Service; Didn't Read" using the example of Facebook. Source: https://tosdr.org/en/service/182 (zuletzt besucht am 30.3.21)

Unfortunately, there is no easy solution to the problem of incomprehensible terms of use - except for an elaborate argument with the written work. If we want to use the app or service, it is mandatory that we agree to the terms of use. Therefore, most users accept without knowing exactly what they have just given their consent to. At least in the end, we can trust legislators and regulators to protect us consumers from abusive terms.

In addition, there are these other recommendations for dealing with terms of use:

- Where possible, we should only trust apps and services that we know have a high number of users. This is not a comprehensive protection against inappropriate terms of use, but at least large companies and service providers are more likely to be regularly monitored by regulators.

- Free services or programmes will probably actually cost nothing, but unless they are publicly provided applications, the service will monetise itself in some other way, possibly through advertising or sharing our data. Caution is advised here.

- In case of suspicion, a quick search can be made on the internet. For example, if we hear that images uploaded to Facebook automatically become Facebook's property, we can find this out relatively easily. Example: Search for "Facebook use of images property" and you will get the relevant information that this is indeed the case.

A very critical example of the exploitation of ignorance about terms of use was published by the New York Times at the beginning of 2018. It involved the software "Alphonso". This software eavesdropped on users by collecting information about which commercials were being heard in the vicinity via the smartphone's microphone. At the time of the report, the software was already integrated into around 1000 smartphone apps (including 250 games alone). And of course, "Alphonso" was able to eavesdrop on more than just commercials.[28] The company's managing director was of the opinion that Alphonso's monitoring was permissible because the users had knowingly accepted the terms of use.

2.2.6 Social-Credit-Systems

A national social credit system is currently being set up in the People's Republic of China, which was originally to be introduced nationwide as early as 2020. The core of the project is a points-based evaluation system that assigns a point value to residents. The system aims to educate citizens to behave in a system-compliant and exemplary manner. Those who behave properly, abide by rules, are credited with points. Bad behaviour - from the government's point of view - is in turn punished with a point deduction. With a higher score, citizens unlock certain benefits, such as access to better schools or jobs, better health care or even discounts on public transport.

However, such a system is only possible through extensive monitoring and the consolidation of different data sources. For this purpose, the Chinese government has granted licences to eight large companies, including big players such as the platform Alibaba.com and Tencent (the Chinese Facebook). Important assessment factors are currently credit history and consumer behaviour (online and offline) as well as activities and rule violations in social media. One's own criminal record and behaviour in road traffic also play a role.

Since 2017, individual pilot projects have been carried out in various cities and even though no concrete date has been set for the nationwide introduction, it is only a matter of time.

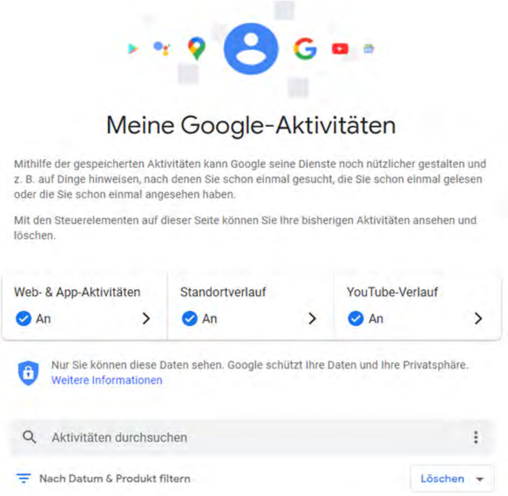
2.2.7 Example Google & Facebook - What they know about us

Example Google

In connection with Google, we usually use the term "data octopus". And indeed, Google stores a lot of information about us. Our search queries, interests, locations, which websites we have visited and which YouTube videos we have watched are stored, at least when we use an active Google account. To get an idea of what information Google has stored about us, it is enough to take a look at the "My Google Activity" section in your own Google account. A lot of information is collected and analysed by Google to improve functions and solve user problems. However, the company still generates a large part of its turnover with advertising space and the possibility for advertisers to place personalised advertising.

So it is worth taking a look at your own Google account...

Google Activity - I know what you searched for last summer...
What keywords did I search for? Which videos did I watch on YouTube? The activity overview provides an overview. Here, the saving of activities can be partially prevented and individual activities can be deleted. We can even search for a specific activity from the past.



Meine Google-Aktivitäten

Mithilfe der gespeicherten Aktivitäten kann Google seine Dienste noch nützlicher gestalten und z. B. auf Dinge hinweisen, nach denen Sie schon einmal gesucht, die Sie schon einmal gelesen oder die Sie schon einmal angesehen haben.

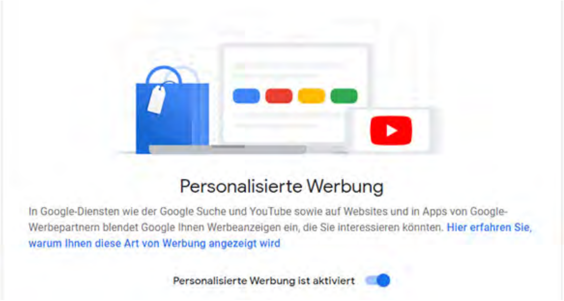
Mit den Steuerelementen auf dieser Seite können Sie Ihre bisherigen Aktivitäten ansehen und löschen.

Web- & App-Aktivitäten	Standortverlauf	YouTube-Verlauf
✓ An	✓ An	✓ An

Nur Sie können diese Daten sehen. Google schützt Ihre Daten und Ihre Privatsphäre.
Weitere Informationen

https://myactivity.google.com/myactivity

Setting for advertising - How is advertising personalised via Google?
Here we can take a look at the personal information Google has collected about us. Google not only generates this information through its own services, but as part of a larger advertising network, it is also the recipient of information provided or identified on other websites. .



Personalisierte Werbung

In Google-Diensten wie der Google Suche und YouTube sowie auf Websites und in Apps von Google-Werbepartnern blendet Google Ihnen Werbeanzeigen ein, die Sie interessieren könnten. Hier erfahren Sie, warum Ihnen diese Art von Werbung angezeigt wird

Personalisierte Werbung ist aktiviert

https://adssettings.google.com/authenticated

Google Location History: These are the places I have visited

An Android smartphone can detect the location of the device and send it to Google, unless the function is disabled in the device settings. The view shows the reported locations on a map and with a timeline.

https://www.google.com/maps/timeline

Google permissions - Who has access to my account?

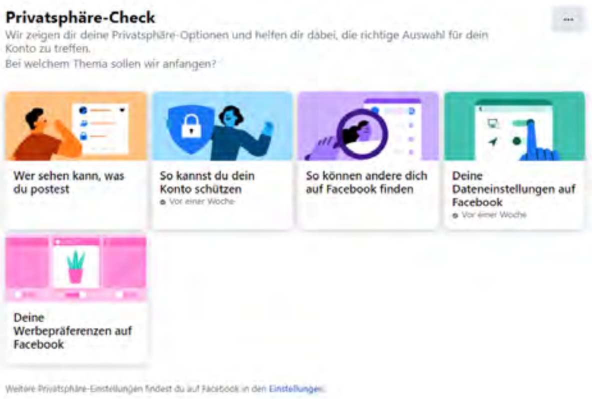
Many tools and services can be linked to Google, giving them access to individual profile information and Google features. Under this menu, we can check which tools currently have access to our Google Account and which services we have signed in to with my Google Account.

https://myaccount.google.com/permissions

Example Facebook: Privacy settings

Facebook has been criticised for years for the way it handles its users' data. The company always seems to be trying to improve this situation and has made more data protection settings available to its users in recent years. However, since Facebook generates its revenue exclusively through the sale of advertisements, it can be assumed that the company will continue to use the data of its users. Nevertheless, every individual should go through the data protection and privacy settings at least once.

Facebook offers comprehensive configuration options in the account settings, but also offers the possibility to do a quick check of our privacy settings.



Privatsphäre-Check

Wir zeigen dir deine Privatsphäre-Optionen und helfen dir dabei, die richtige Auswahl für dein Konto zu treffen.

Bei welchem Thema sollen wir anfangen?

- Wer sehen kann, was du postest
- So kannst du dein Konto schützen – Vor einer Woche
- So können andere dich auf Facebook finden
- Deine Dateneinstellungen auf Facebook – Vor einer Woche
- Deine Werbepräferenzen auf Facebook

Weitere Privatsphäre-Einstellungen findest du auf Facebook in den Einstellungen.

The Facebook privacy check - https://www.facebook.com/privacy/checkup

The privacy check can be found at:.
https://www.facebook.com/privacy/checkup
The privacy check offers the following options:

- "Who can see what you post": Normally the name, place of residence, studies or work are public so that other people can search for us. Other data, such as mobile phone number or date of birth, should be private.
- "How to protect your account": These are the options to change the password, or to decide how Facebook should notify us when someone logs into our account from a location unknown to Facebook.
- "So others can find you on Facebook": Here we can limit the group of people who can send us friend requests. And even if our mobile phone number or email are not visible, we can set here whether other people can search for us using this data.
- "Your data settings on Facebook": Apps and websites that we have used to log in with our Facebook account are displayed here. Corresponding connections can also be removed here. In addition, automatic face recognition can be activated and deactivated here, with which we can allow Facebook to recognise us in photos and videos.
- "Your advertising preferences on Facebook": Here we can define which profile information advertisers can use to reach us. We can also define who can see our actions on ads.

A complete list of all setting options can be found in the account settings:
https://www.facebook.com/settings

We recommend that you take your time and work through all the menu items. Among other things, you will find the following important setting options:

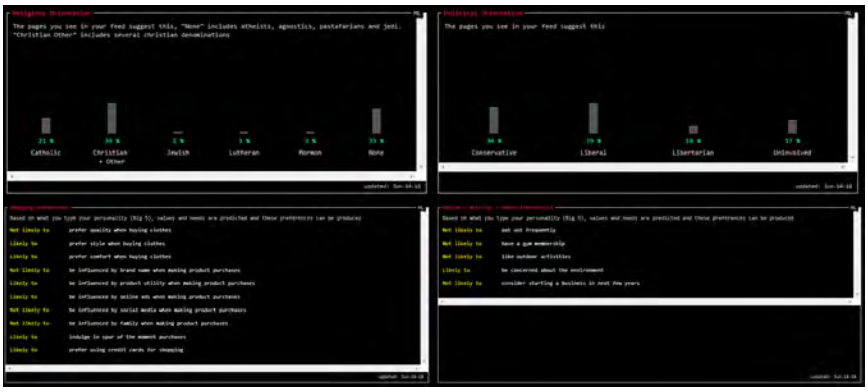
- Who should have access to my account after my death?
- Who is allowed to write messages on my pinboard? Who is allowed to tag me? And do I want to share posts on which I am tagged first? All this can be found in the profile and tagging settings (https://www.facebook.com/settings?tab=timeline)

And if you want to see what data Facebook has collected, you can do so in the "Access your information" section. (https://www.facebook.com/your_information/). There you will find all posts, photos, comments and other information that Facebook has stored about your profile. Very interesting in this context is the section "Advertisements and companies". Here we find information on advertisers with whom we have been linked - be it because we have clicked on an ad of the corresponding company or the companies have shared a list of contact information with Facebook that also contained our data. It's worth taking a look at this list.

2.2.9 Example "Cambridge Analytica": Creation of personal profiles

Cambridge Analytica was an American company that had to file for bankruptcy after it became known that it had used many millions of Facebook accounts and their profile information to create personality profiles and sell them to place election campaign ads. This is considered one of the biggest data breaches ever. Cambridge Analytica used a personality test that, based on just a few questions, can already determine a very accurate picture of a user's interests, especially political interests, and how these in turn can be influenced. These questions were answered by users in the typical style of Facebook surveys in an app. By agreeing to the terms of use, Facebook users also allowed the company to access the friend lists of Facebook profiles. This enabled Cambridge Analytica to create a profile not only of the app's users, but also of similar users who did not use the app at all. In the end, this resulted in a data collection of over eighty million records. As a result, Facebook founder Mark Zuckerberg had to answer questions before the US Congress, and his company's reputation took a noticeable hit.

In general, we as users should be very careful when we encounter surveys on advertising-financed websites and portals. For example, the "five-factor model", which is a model of personality psychology, describes that the factors "open-mindedness", "perfectionism", "sociability", "empathy" and "lability" can already create a fairly accurate personality picture. The model is also known as the "OCEAN model" and was the basis for the personality test developed by Cambridge Analytica. Visitors to websites should keep this in mind the next time they are asked on a portal what their opinion is on a topic. An answer is quickly given here, and just as quickly, for example, the personal level of empathy is classified.



The pages you see in your feed suggest this, "None" includes atheists, agnostics, pastafarians and jedi.
"Christian Other" includes several christian denominations

The pages you see in your feed suggest this

```
Based on what you type your personality (Big 5), values and needs are predicted and these preferences can be produced
Not likely to     prefer quality when buying clothes
Likely to         prefer style when buying clothes
Likely to         prefer comfort when buying clothes
Not likely to     be influenced by brand name when making product purchases
Likely to         be influenced by product utility when making product purchases
Likely to         be influenced by online ads when making product purchases
Not likely to     be influenced by social media when making product purchases
Not likely to     be influenced by family when making product purchases
Likely to         indulge in spur of the moment purchases
Likely to         prefer using credit cards for shopping
```

```
Based on what you type your personality (Big 5), values and needs are predicted and these preferences can be produced
Not likely to     eat out frequently
Not likely to     have a gym membership
Not likely to     like outdoor activities
Likely to         be concerned about the environment
Not likely to     consider starting a business in next few years
```

Simulation of Cambridge Analytica data processing: an assumption is made about your religion, personality, mood, activity and political orientation.

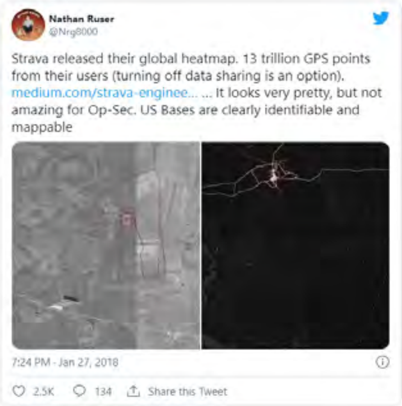
2.2.10 Example "Strava"; risks with public data

Strava is a social network used by runners, cyclists and other sportspeople. Via an app, sporting activities can be recorded and shared with others. The distances covered are saved via GPS with distance, time and other details. The app can be used in combination with other fitness devices such as Fitbit or Jawbone to check one's own performance and compare it with other users.

In January 2018, Strava published a so-called "heatmap". The idea was to display the routes recorded in Strava anonymously on a map. Data from activities recorded between 2015 and September 2017 served as the basis. According to its own information, this was over one billion activities, covering 27 billion kilometres of distances run, jogged or swum.

By overlaying the individual activities, routes that were run more often were shown brighter than less popular routes. Thus, the heat map gave an insight into the most popular routes in the world. So far so good...

Unfortunately, this venture led to a security risk for US forces stationed in Syria and Iraq. The Strava service is also very popular with members of the US military. This led to popular running routes around US military bases becoming visible and thus, especially in sparsely populated regions, the footprints of the bases. Even if the location of military bases is generally known, the heat map shows which of the bases is most used and which routes the soldiers take.



Nathan Ruser
@Nrg8000

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee... ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

7:24 PM - Jan 27, 2018

Detailed report of the BCC: https://www.bbc.com/news/technology-42853072
Original Twitter-Post: https://twitter.com/Nrg8000/status/957318498102865920

This shows that information can be made public even without malicious intent, or how harmless information (anonymised Strava routes) can suddenly be used to draw conclusions about other information (location of military bases and supply routes).

Strava offers the option in the privacy settings to explicitly reject data collection for the heatmap - even for activities that are not marked as private. But who could have predicted in advance such a side effect of a nice idea like a heatmap for popular sports routes. .

3. My data, my rights

3.1. Who owns our data?

There is no doubt that our personal data belongs to us first. And we have the right to determine how this data is used and published. But does all my data really belong to me personally? We always assume that all information about me belongs to me. But is that true? What about my phone number or my email address? Are these really mine or do they remain the property of the provider who only provides me with these identifiers and only grants me rights of use? Do the usage data that I leave behind, for example, during internet research, belong to me personally or to the provider who collects them? This question is not easy to answer. The problem: According to current law, ownership can only exist in physical objects, and data unfortunately do not count as intellectual property either.

On the other hand, data is a valuable commodity. The business models of many large internet companies are based on offers that are financed by the users' data. Thus, the question of a possible "ownership of data" is quite justified. Who owns our data and who is allowed to use it?

For personal data that can be clearly attributed to a person, the answer may still be quite simple: This data may only be processed on a legal basis. At the very least, we have a right to know which provider has stored which of our information and what it is used for. This right was enshrined in the European General Data Protection Regulation (GDPR).

My data, my rights		
He/she knows his/her rights in relation to his/her personal data and can exercise these rights.		
Knowledge	**Skills**	**Competences**
He/She • knows the basic principles of the European General Data Protection Regulation (GDPR) • knows its own rights arising from the GDPR. • knows the limits of the GDPR and the risks of data processing outside the EU	He/She is able to • to make use of his or her rights granted by the GDPR..	He/She is able to • determine the data protection risks of using a particular provider.

But what if our data is anonymised? Such data has considerable economic value. They are the basis for a wide variety of economic sectors and are even traded. And even if there should be a clear regulation in the future regarding the ownership of data, the question arises how such "data ownership" can be implemented and proven in practice.

Anyone who buys a DVD from a retailer can use it for as long as the life of the data carrier allows. But anyone who buys a digital copy via Amazon, for example, can only stream the film in combination with their Amazon account. And only for as long as Amazon stocks the film in its library. Several lawsuits have already been filed in the USA in this regard.

3.2 The European General Data Protection Regulation (GDPR)

3.2.1. Introduction

The right to protect one's own personal data is already enshrined in the EU Charter of Fundamental Rights. In May 2018, the European General Data Protection Regulation (GDPR) also entered into force. The aim of the regulation is to protect the "fundamental rights and freedoms of natural persons", in particular their right to the protection of personal data (GDPR Art.1). It contains rules and regulations for the processing of personal data. Among other things, it obliges companies and public bodies to inform data subjects about the intended processing of data at the time of data collection.

What data is affected by the GDPR?

According to the GDPR, personal data is any information that relates directly or indirectly to a person. In addition to our name, our login or our email address, this also includes information such as customer numbers, online identifiers, location data and the like. Ultimately, this means all data that in any way allows conclusions to be drawn about our person. (GDPR Art. 4 lit.1)

Companies and public bodies may only store and process this data under certain conditions. For example, personal data may only be collected for a specific, unambiguous and legitimate purpose and may only be used for this purpose. Companies are also obliged to collect only the data that is really needed for the corresponding purpose (keyword "data minimisation"). (GDPR Art. 5 lit.1)

Of course, with an online mail-order business I still have to give my name and complete address, because the company has to be able to send me the ordered goods. When subscribing to a newsletter, on the other hand, only the email address may be mandatory, because only this is really needed for sending the newsletter.

The provider must also delete my personal data as soon as the actual purpose is no longer given. However, this does not mean that my data will be deleted immediately. State laws often take effect here. In Germany, companies have to keep billing data for up to 10 years, in Spain for 5 years. So just because I delete my account with my online mail-order company, certain ones remain stored because the company is legally obliged to do so.

3.2.2 Our rights

Duty to provide information when collecting data (Art.13 GDPR)

The GDPR tries to make the processing of our data transparent for users. As soon as a company or a public body wants to store data from us, we must be informed at the time of collection about what specifically happens with this data.

According to the duty to inform, the following questions must be answered:

- Who wants to store and process our data?
- For what purpose should our data be processed?
- What is the legal basis for storing our data?
- Which recipients receive access to our information?
- Is our data transferred to third countries outside the EU?
- How long will our data be stored?
- If the provision of the data is required by law or contract or is necessary for the conclusion of a contract: What would be the consequences for us if we do not provide the data?

In addition, we must be informed of other rights when collecting data, such as the right to information, the right of revocation and the existence of a right of complaint to a supervisory authority.
The GDPR does not impose any restrictions on sectors or use cases. For this reason, we have been increasingly confronted with data protection notices and information on the storage of our data since the introduction of the regulation.

Right to information (Art.15 GDPR)

We have the right to know what data companies have stored from us and for what purpose, and who has access to this data. We can also request this in writing. Companies are obliged to provide us with information about this.

Since responding to these requests involves effort for the companies concerned, it can take several weeks before such a request is answered. Large providers in the digital sector have started to make the relevant information available online.

Right to rectification and erasure (Art. 16 + 17 GDPR)

If information stored about us is incorrect, we naturally have the right to request that the data be corrected. If we move, for example, our address will change.

In addition, the GDPR includes the "right to be forgotten", i.e. the right to have our data deleted. If we request the erasure of our data, the controller is obliged to comply with this request without delay. However, there are some limitations here. First of all, it must be ensured that the purpose for which the data was collected has ceased to exist. In addition, the data controller may, for example, be subject to legal obligations that make it necessary to store the data. So we probably won't be able to simply delete our data everywhere, but we can at least get information about what data is stored for what reason by the respective data controller.

Other rights: :

Right to restriction (Art. 18 GDPR)

If we suspect that the processing of our data is unlawful or disproportionate to the original purpose, we can lodge a complaint and have the processing of our personal data restricted.

Right to data portability (Art. 20)

The European General Data Protection Regulation gives us the right to request the data stored about us in a "structured, commonly used and machine-readable format". The idea behind this is to ensure data portability, i.e. the possibility to transfer personal data directly from one controller to another. This could, for example, make it easier to move from one social network to another. However, this right is weakened by the limitation "as far as technically feasible". But even if seamless data transfer between different services will not be possible in the foreseeable future, the right to data portability at least allows us to receive the data we hold about ourselves in a format that we can further process.

Right of objection (Art. 21)

As already mentioned, any processing of our personal data must always have a legal basis. If we take out an insurance policy, our data must be processed for contractual reasons. We provide information on our tax return due to legal requirements.

However, we often disclose information voluntarily. Then the processing of our data is usually based on consent that we have given to the respective provider. This is particularly the case in the area of direct advertising. Here we have the right to object.

If it is advertising, the provider must accept the objection immediately and stop processing our data. In other cases, we may be asked to explain the reasons why we are now refraining from the original consent to the processing. If the provider does not comply with our request, we still ultimately have the option of filing a complaint with a supervisory authority.

Complaint to the supervisory authority

In each country where the General Data Protection Regulation applies, there are one or more data protection supervisory authorities. In Germany, each federal state even has its own data protection commissioner and supervisory authority. Companies are obliged to report data protection incidents to the supervisory authorities. But even as a private individual, we can turn to the authorities with complaints.

Due to violations of the GDPR, national supervisory authorities can demand high fines. The highest fine to date, amounting to 50 million euros, went to Google (as of the end of 2020). But other companies have also already had to pay high fines: H&M paid €35.2 million and TIM Telecom €27.8 million.

The reasons vary: Google was prosecuted for lack of information and data processing without consumer consent. In H&M's case, it was a technical error that made private information of all the company's employees publicly available. However, the fine was not imposed because of the technical error, but because the publication revealed that H&M was collecting sensitive personal data of its employees. TIM's fine, in turn, was imposed for different reasons: From improperly obtaining consent for data processing to excessive data retention.

But it doesn't only hit the big ones: In Austria, a betting office was fined €5,000 for illegal video surveillance. In Hungary, a company refused to hand over data and was fined 6.5% of its annual turnover.

And it doesn't always have to be fines in the millions: A hospital in Hungary had to pay 90€ because it violated a patient's right to information and unlawfully charged a copying fee.[34] 48€ fine went to the Estonian police because a police officer used the police database for private research (unlawful use).

An overview of the fines imposed by the European supervisory authorities can be found on the following website:
https://www.enforcementtracker.com/

3.2.3 Criticism

The General Data Protection Regulation (GDPR) attempts to strengthen our rights. But there is also criticism of the new regulation. Because it is deliberately vague in many places. Personal data can be processed on the basis of the "legitimate interest" of the respective company, which is difficult to assess in individual cases. Companies are obliged to take "appropriate measures" to protect the data, which among other things take into account the "state of the art". And our requests are to be answered "without disproportionate effort".

These formulations open up room for interpretation. Thus, the General Data Protection Regulation is interpreted very differently in the member states and by the competent data protection authorities.

There is also a widespread perception that the GDPR does not do justice to the complexity of the digitally networked world. In the face of networked applications, systems distributed across national borders through cloud computing, as well as the abundance of data (big data), the practical application of the GDPR appears to be very difficult.

However, the mere existence of the GDPR is already an important step in the field of data protection. How difficult and complex such projects are can be seen in the planned ePrivacy Regulation. The new regulation is to replace the existing ePrivacy Directive and strengthen the privacy of citizens online. Thematically, it mainly deals with topics around direct marketing and the use of cookies. The regulations of the GDPR are to be concretised with the new regulation. Originally, the new ePrivacy Regulation was to come into force together with the GDPR in 2018. However, the EU member states could not agree on a common line. In November 2020, another compromise proposal was rejected.

3.2.4 Problem: Right to erasure and to be forgotten

The GDPR strengthens our rights to our data through the principles of informational self-determination and purpose limitation of data processing. We are allowed to determine which of our data is used, processed and published. And companies are only allowed to store our data as long as it is necessary for the respective purpose. If the purpose ceases to apply, the data must be deleted again. We also have a right to have our data deleted. But to what extent can this right always be enforced in the digital age?

In 2000, the cameraman Matthias Fritsch filmed a muscular, lightly clad man at a techno parade and posted the video on Youtube in 2006. The man shown on the video sued in court against the publication of the video, claiming that he had not consented to its publication. The court found in his favour and Matthias Fritsch had to delete the video from his profile. In the meantime, however, the video achieved a kind of cult status in the Internet community. Due to the man's appearance and stature, the video has already been copied several times under the name "Techno Viking" and re-released in new versions. Although Fritsch deleted the video on his channel, the video can still be accessed today via various portals. The phenomenon shows the problem of the right to deletion in the age of the internet.

Even if we delete all our data on a social network today, we cannot be sure that all cross-references and possible copies are deleted with it. If we delete a picture from our smartphone, the copy that we may have previously sent via a messenger is not automatically deleted as well. Today, our data usually exists simultaneously in different places. A complete deletion can often not be guaranteed one hundred percent.

The Streisand effect

The Streisand effect describes the phenomenon that an attempt to delete an unwelcome piece of information achieves exactly the opposite and it is precisely the request for deletion that attracts public attention.
The name goes back to the singer and actress Barbra Streisand. On the website Pictopia.com, 12,000 aerial photos of the California coast were published. The photos were intended to document the erosion of the Californian coast for the California Coastal Records Project. In one of the pictures, the actress discovered her own house. She demanded the immediate deletion of the photo and sued the website and the photographer for 50 million US dollars in damages. The lawsuit was unsuccessful. But it was Streisand's lawsuit that first established a link between the photo and her property. As a result, the photo went viral on the internet.

n.

3.3 Data protection outside the European Union

Through the GDPR, we have a common regulation on data protection within the European Union. The regulation applies in all member states and thus protects all personal data of EU citizens that is processed within the EU. But what happens when we use services that are not based in the EU? Ultimately, the European General Data Protection Regulation does not apply then either.

The internet as a global village makes national borders disappear. And it is often not recognisable to us which country an individual provider comes from or even in which country our data is stored and processed.

One thing is certain, however: anyone who orders via the internet from a supplier in a non-European country does not enjoy the same consumer rights as with a European supplier.

But even if we entrust our data to a European provider, this does not mean that the provider does not use other service providers who may have access to our data. Much more important, therefore, is the question of the extent to which a company cooperates with other companies. A German company might have its headquarters in Germany, but the servers with the customer data could be in a data centre in Strasbourg or Amsterdam and looked after by a Scandinavian IT company. Similarly, the company could use certain software solutions, which in turn are provided by providers based in the USA or rely on call centres based in Eastern Europe or Asia. This raises the question of the extent to which the protection of our data can be guaranteed in accordance with the GDPR.

The EU has defined a list of countries that are considered safe third countries. These are countries that the European Commission confirms have an adequate level of data protection. This means that these countries have implemented a comparable or better level of data protection. This currently includes all countries from the European Economic Area (Norway, Iceland and Liechtenstein) as well as explicitly Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

This regulation does not exclude the transfer of personal data to other countries. The only difference is that in this case the data controller must ensure that the data are sufficiently protected at the recipient's end. To simplify this, the EU has developed so-called standard contractual clauses that can be signed by companies in third countries. The corresponding regulations on data protection are then defined there.

For us as end users, it is unfortunately often not clear where our data goes and who ultimately has access to it. Despite all the rules and regulations, the responsibility for which service providers we use and which personal data we make available to them lies with ourselves.

3.4 Special case U.S.

The biggest internet companies are based in the USA. Microsoft, Google, Facebook, Twitter and Co. are all not European companies. As a rule, these companies have a branch in the EU, but data transfer to the USA cannot be ruled out. Therefore, we need appropriate regulations that ensure the protection of EU citizens' data in the USA.

For a long time, there were corresponding agreements between the EU and the USA. First, there was the "Safe Harbor" agreement since 2000, which allowed companies to transfer personal data from an EU country to the USA in accordance with European data protection guidelines. The agreement was declared invalid in 2015.

In order to further guarantee the transfer of data between the EU and the USA, the EU-US Privacy Shield was adopted in 2016. This was declared invalid by the European Court of Justice in 2020.

Both cases stem from a lawsuit filed by Austrian Maximilian Schrems. The core of the lawsuits was the accusation that Facebook's branch in Ireland shares its data with the parent company in the USA. In this way, data of European citizens is transferred to the USA. This fact became explosive in 2013 through the revelations of Edward Snowden (2013). He revealed that US intelligence services have access to servers of US companies such as Facebook and Google. Most recently, the so-called CLOUD Act (Clarifying Lawful Overseas Use of Data Act) was passed in the US in 2018. This law obliges American companies to grant US authorities access to stored data. The judges of the European Court of Justice declared the "Privacy Shield" invalid. In view of the access possibilities of the US authorities, the data protection requirements are not guaranteed.

From a data protection perspective, the transfer of personal data should therefore be viewed critically, even if the current EU standard contractual clauses are still valid from a purely legal perspective. The USA is currently not considered a safe third country.

However, the US state of California shows that there is a lot of movement on this issue. With the California Consumer Privacy Act (CCPA), it has implemented the strictest data protection law in America to date. The model for the new law was the European General Data Protection Regulation.

.

3.5 Conclusion

The digitalised world is increasingly driven by data. It is important that we become aware of the value of our own data. We need to learn to understand when we disclose which data and to be sensitive with our information. With whom do I share my data? For what purpose? Where is it stored? Is the data requested really needed?

It is a fact that our personal data is collected. Often this is done with our consent, even if we cannot always see the implications of this decision. In other cases, information is also collected from us without our explicit consent.

We must also be aware that regulations like the GDPR are only regulations. They may be on paper, but they only protect us to a limited extent in real life. We cannot check whether a company fulfils its duty to inform or complies with applicable laws. All we can do is trust the providers and regulators and remain critical. This applies to the email from our bank, the friend request in the social network as well as to the newly discovered online shop. It is better to check more thoroughly for seriousness and authenticity.

Principles of data minimisation can also be implemented in our everyday lives. When publishing data in blogs, forums, social networks, etc., the principle is that we should not publish anything that we do not really want to make public. Even if an online service offers the possibility to restrict access to published information to a certain group of users, we should always think carefully about what information we put online. Because the internet does not forget.

Ultimately, it's like road traffic. Of course, an accident can always happen. But if we behave prudently and exercise caution, we reduce the risk considerably

Endnoten

1 https://de.statista.com/statistik/daten/studie/1010134/umfrage/anzahl-der-von-facebook-entfernten-fake-accounts-weltweit/

2 https://www.security-insider.de/was-ist-ein-digitales-zertifikat-a-688440/

3 https://www.datenschutz.org/biometrische-daten/

4 https://www.mimikama.at/fake-gewinnspiele-auflistung/

5 https://www.pcwelt.de/ratgeber/Datenschutz-So-schuetzen-Sie-Ihre-Privatsphaere-im-Web-57287.html

6 https://www.it-zoom.de/mobile-business/e/das-sind-die-dreistesten-datensammler-15442/
https://whotracks.me/

7 https://de.statista.com/statistik/daten/studie/872986/umfrage/anteil-der-spam-mails-am-gesamten-e-mail-verkehr-weltweit/

8 https://www.polizei.bayern.de/kriminalitaet/internet/betrug/index.html/56975

9 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing.html

10 https://www.internet-beschwerdestelle.de/de/beschwerde/einreichen/e-mail-und-spam.html

11 http://www.argedaten.at/php-generiert/datenschutz_seminare_at_Welche_rechtlichen_Schritte_sind_gegen_Spam_m%C3%B6glich.html

12 https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073

13 https://de.statista.com/infografik/23251/anzahl-neuer-malware-varianten/

14 https://www.heise.de/newsticker/meldung/Vor-20-Jahren-Ein-verliebter-Wurm-umrundet-die-Welt-4713566.html

15 https://praxistipps.chip.de/die-5-gefaehrlichsten-viren-aller-zeiten-und-was-sie-angerichtet-haben_42111

16 https://www.heise.de/security/meldung/Virus-oder-Impfstoff-WiFatch-befaellt-Router-und-schuetzt-vor-Malware-2837158.html

17 https://de.statista.com/statistik/daten/studie/1038985/umfrage/betroffenheit-durch-ransomware-nach-umsatzgroessenklasse-der-unternehmen-in-deutschland/

18 https://www.bundespolizei-virus.de/virenschutz/drive-by-downloads/

19 https://www.avg.com/de/signal/windows-10-privacy-everything-you-need-to-know-to-keep-windows-10-from-spying-on-you

20 https://www.brandeins.de/magazine/brand-eins-wirtschaftsmagazin/2019/unabhaengigkeit/smartphones-legaler-lauschangriff

21 https://www.tagesschau.de/inland/cyberangriffe-bka-101.html

22 https://de.statista.com/statistik/daten/studie/193207/umfrage/finanzielle-schaeden-durch-cyberkriminalitaet-in-deutschland/

23 https://www.zeit.de/datenschutz/malte-spitz-data-retention

24 https://www.welt.de/print/die_welt/wirtschaft/article195830359/Was-sind-meine-Daten-wert.html

25 https://de.statista.com/statistik/daten/studie/458825/umfrage/werbeeinnahmen-von-facebook/

26 https://de.statista.com/statistik/daten/studie/75188/umfrage/werbeumsatz-von-google-seit-2001/

27 https://irights.info/artikel/metadaten-fotos-anbringen-loeschen-bearbeiten/26353

28 https://t3n.de/news/smartphone-spionage-alphonso-897108/

29 https://transparency.facebook.com/community-standards-enforcement

30 https://www.handysektor.de/artikel/berechtigungen-was-wissen-meine-apps-ueber-mich/

31 https://de.statista.com/statistik/daten/studie/801670/umfrage/umsatz-mit-mobilen-apps-nach-segmenten-in-deutschland/.

32 https://www.gameswirtschaft.de/wirtschaft/mobilegames-umsatz-deutschland-2019/-

33 https://direc.ircg.ir/wp-content/uploads/2020/01/SuperData2019YearinReview.pdf

34 https://www.dsgvo-portal.de/dsgvo-bussgeld-gegen-krankenhaus-2019-12-09-HU-223.php