



# Human Rights in the Digital Age

## II lecture: Right to private life in the digital age

Visiting prof. dr. Dovile Gailiute-Janusone



MYKOLAS ROMERIS  
UNIVERSITY



**unimc**  
UNIVERSITÀ DI MACERATA

**l'umanesimo che innova**

# Outline

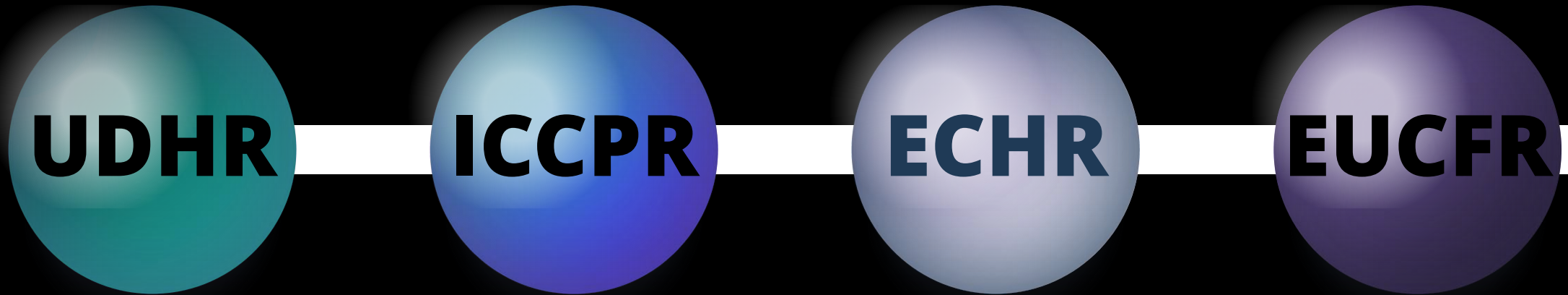
1. Introduction to the right to private life
2. Protection of privacy online
3. Data protection
4. Right to be forgotten
5. Mass surveillance
6. Monitoring at work, right to be disconnected
7. Social networks and privacy
8. Right to private life and Covid-19





# Introduction to the Right to Private Life

# Legal regulation



# Universal Declaration of Human Rights

## *Article 12:*

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

# International Covenant on Civil and Political Rights

## *Article 17*

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

# European Convention on Human Rights

## Article 8

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

# EU Charter of Fundamental Rights

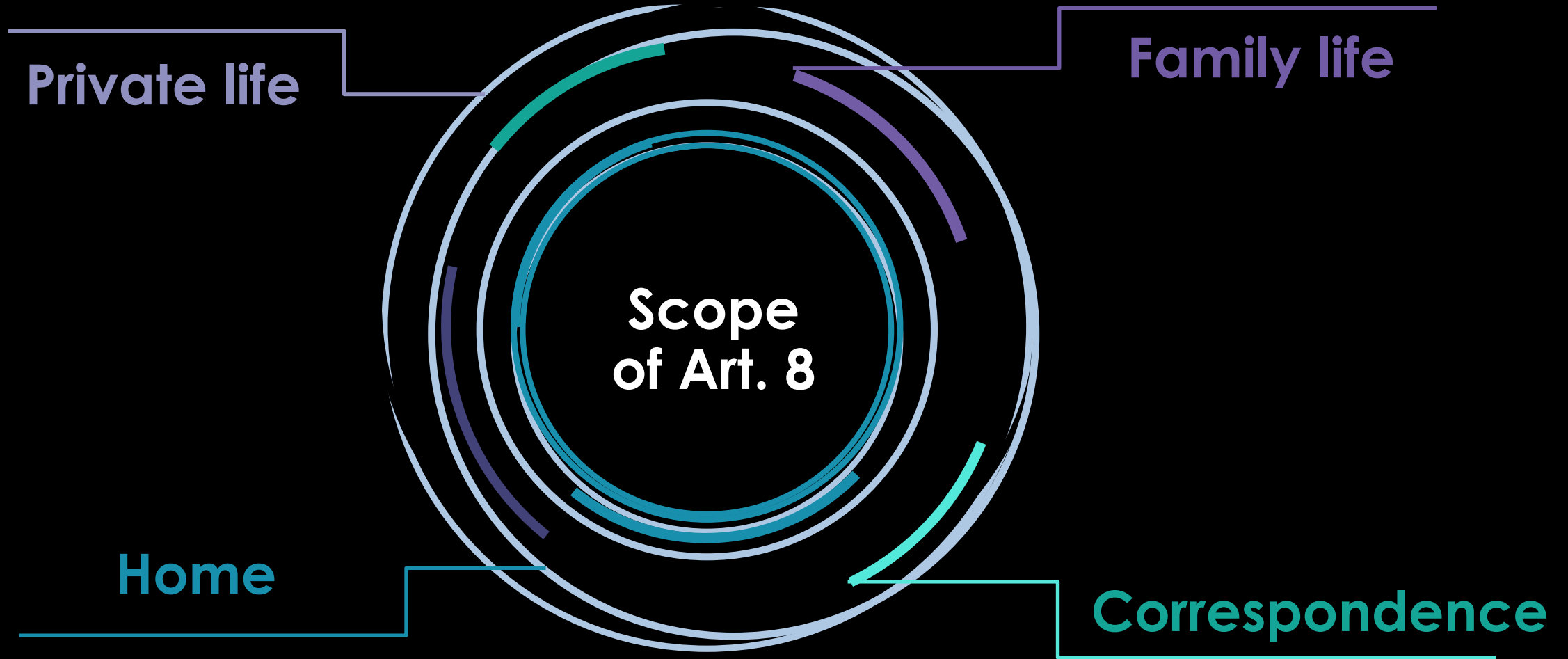
## Article 7

Everyone has the right to respect for his or her private and family life, home and communications

## Article 8

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.





# Content of Article 8

- Article 8 is one of the most open-ended of the Convention rights, covering a growing number of issues and extending to protect a range of interests that do not fit into other Convention categories
- There is no comprehensive definition of Article 8 interests, adapting them to meet changing times

# Content of Article 8

- However, its scope is not limitless.
- In the case of access to a private beach by a person with disabilities, the Court held that the right asserted concerned interpersonal relations of such broad and indeterminate scope that there could be no conceivable direct link between the measures the State was being urged to take in order to make good the omissions of the private bathing establishments and the applicant's private life. Accordingly, Article 8 was not applicable

***Botta v. Italy*, § 35**

# Private life

“The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of “private life”.

However, it would be too restrictive to limit the notion to an “inner circle” in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings”.

***Niemitz v. Germany***



# Limitation Clause



# European Convention on Human Rights

## Article 8

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

# Limitation clause

1

## Legality

**In accordance with the law**

- Prescribed by national law
- Law must be adequately accessible
- Law must be clear and definite

2

## Legitimacy

**Legitime aims**

- national security
- public safety or the economic well being of the country
- prevention of disorder or crime
- protection of health or morals
- protection of the rights and freedoms of others

3

## Proportionality

**Necessary in a democratic society**

- correspond to a pressing social need
- proportional to the legitimate aim pursued
- justified by relevant and sufficient reasons

# In accordance with the law: Case-law

“The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data”

*Shimovolos v. Russia*, § 68

Lawfulness also requires that there be adequate safeguards to ensure that an individual's Article 8 rights are respected.

Applicant's profession may be a factor to consider as it provides an indication as to his or her ability to foresee the legal consequences of his or her actions

*Versini-Campinchi and Crasnianski v. France*, § 55



# Legitimate aims: Case-law

It is for the respondent Government to demonstrate that the interference pursued a legitimate aim

*Mozer v. the Republic of Moldova and Russia* [GC], § 194

The Court has also found both economic well-being and the protection of the rights and freedom of others to be the legitimate aim of large governments projects, such as the expansion of an airport

*Hatton and Others v. the United Kingdom* [GC], § 121

The Court found that the government had provided no legitimate justification for allowing journalists to publish images of a person detained before trial, when there was no public safety reason to do so *Toma v. Romania*, § 92

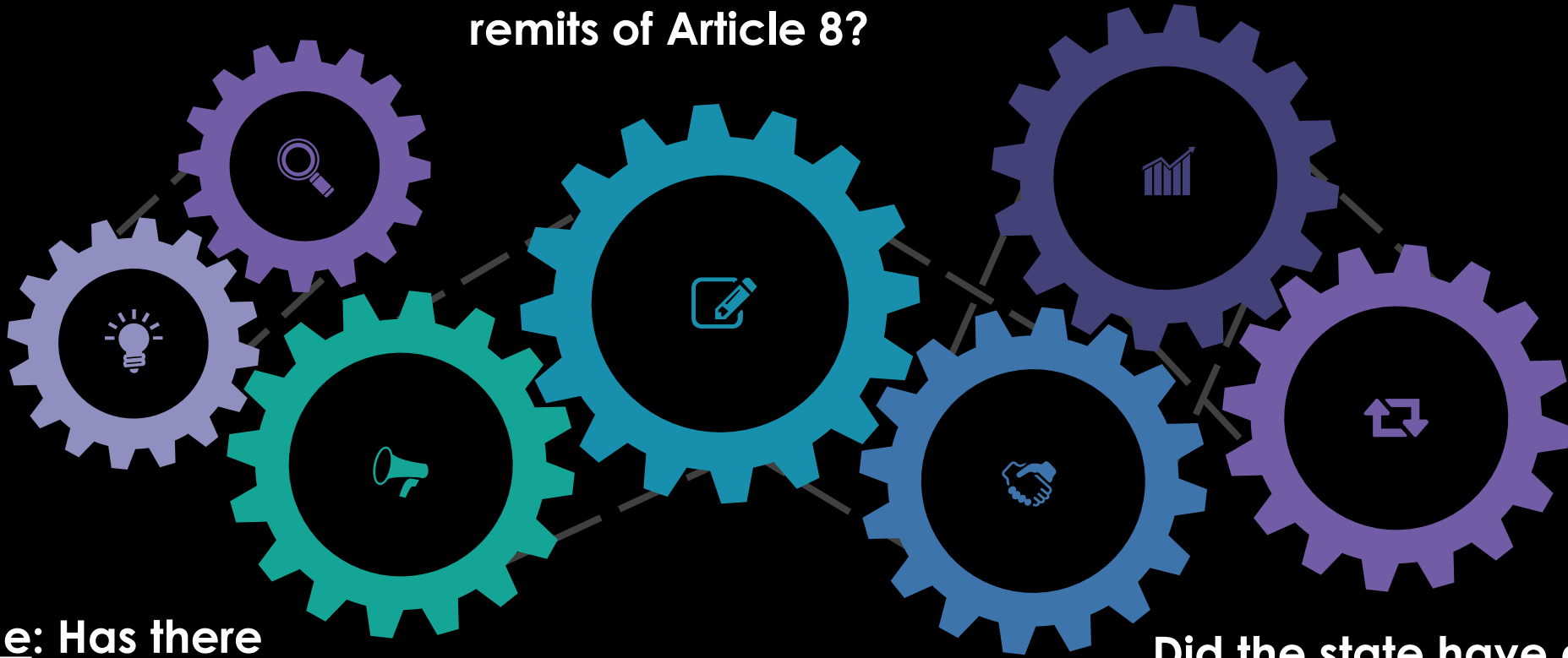
# Fair balance?

Right to private life of individual **v.** Interests of society



# II stage test at the Court

I stage: Does the complaint fall within the remits of Article 8?



II stage: Has there been an interference?

Did interference meet the requirements?

Did the state have a positive obligation to protect the right invoked?

# Privacy online





[https://www.youtube.com/watch?v=UhhYSrUHnao&feature=emb\\_title](https://www.youtube.com/watch?v=UhhYSrUHnao&feature=emb_title)

# Main Issues



Data  
protection

Mass  
surveillance

Video  
surveillance

Monitoring  
at work

Online  
harassment



# Data protection





Opening for signature on 28 January 1981 of Convention 108, the first legally binding international instrument in the field of data protection

Opening for signature of the Additional Protocol on 8 November 2001 in Strasbourg, requiring the parties to set up supervisory authorities exercising their functions in complete independence.



Accession of the first non-European State, Uruguay to Convention 108 and its Additional Protocol.



Convention 108+, adoption of the Amending Protocol CETS No. 223 for the modernisation of Convention 108

55 States Parties to Convention 108



Convention 108+ includes:

- stronger requirements regarding the proportionality and data minimisation principles, as well as the lawfulness of the processing;
- an extension of the types of sensitive data to include genetic and biometric data, trade union membership, and ethnic origin;
- an obligation to declare data breaches;
- greater transparency of data processing and stronger accountability of data controllers.





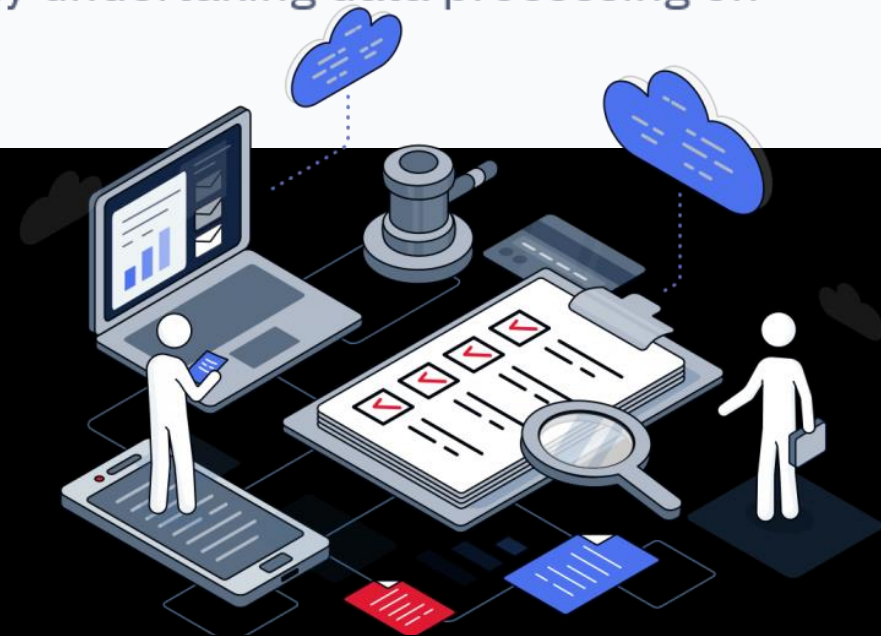
# **General Data Protection Regulation**

## SCOPE

# Who does the GDPR apply to?

All organisations that process personal data and operate within, or sell goods to the EU are impacted by the GDPR. The definition of processing is designed to cover practically every type of data usage and includes collection, storage, retrieval, alteration, storage and destruction.

The GDPR applies to both data 'controllers' and 'processors'. Data controllers determine the purpose and manner in which data is processed. Data processors are any third-party undertaking data processing on behalf of a controller.



# What is personal data?

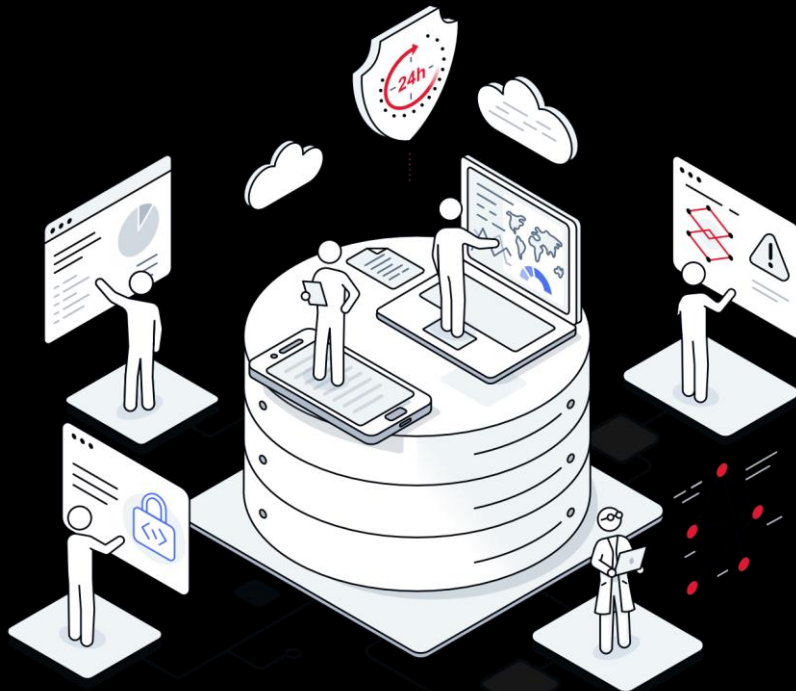
Article 4 of the GDPR defines personal data as ‘any information relating to an identified or identifiable natural person’. For most organisations, this means implementing appropriate measures to protect information relating to employees, customers and partners. The GDPR expands the definition of personal data to include all information that could be used to indirectly identify individuals. Other examples of personal data include:

- ✓ ID numbers
- ✓ IP addresses and cookie IDs
- ✓ HR records
- ✓ Customer contact details
- ✓ Health records
- ✓ Biometrics
- ✓ CVs and employment details
- ✓ CCTV and call recordings



# Personal data shall be...

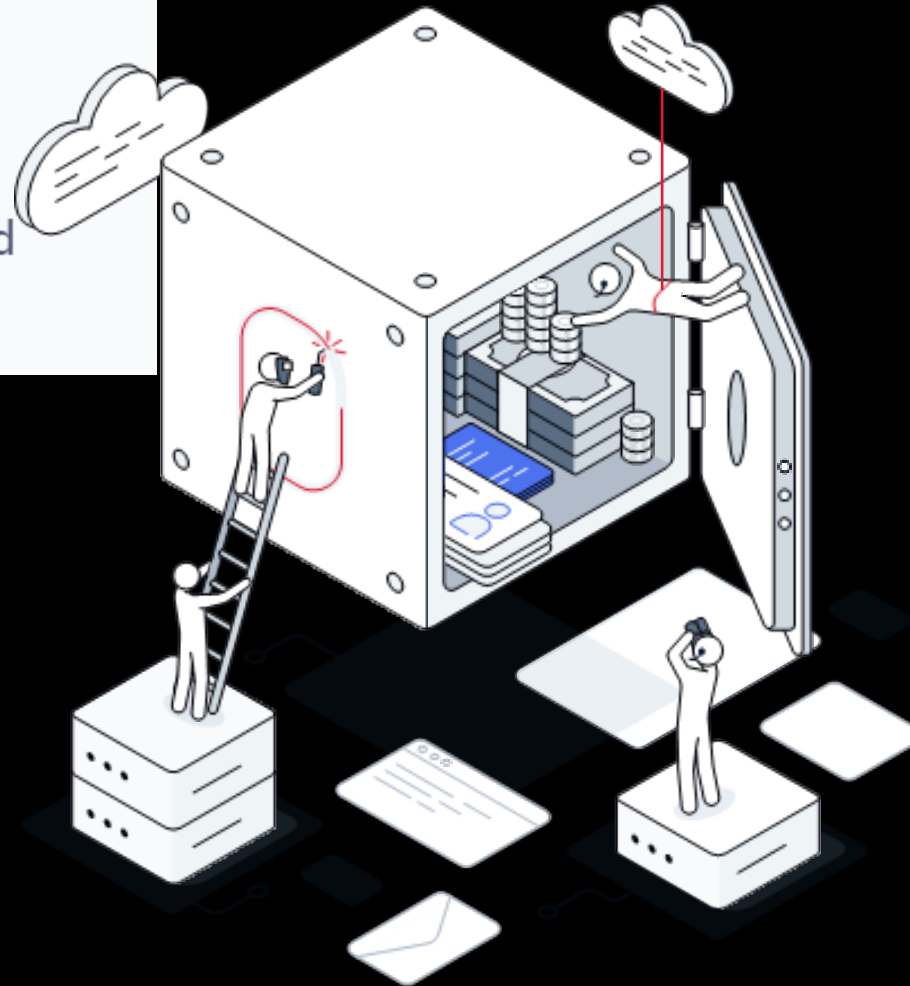
- ✓ Processed lawfully, fairly and in a transparent manner
- ✓ Collected for specified, explicit and legitimate purposes
- ✓ Adequate, relevant and limited to what is necessary
- ✓ Accurate and, where necessary, kept up to date
- ✓ Retained only for as long as necessary
- ✓ Processed in an appropriate manner to maintain security



# The importance of ensuring the security of personal data

In order to ensure ongoing data security, principle six of the GDPR states that personal data should be processed in an appropriate manner.

Protecting personal data against unauthorised processing, accidental loss and destruction forms an integral part of measures all organisations should take.



## ECtHR: S. and Marper v. the United Kingdom [GC]

“The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of **Article 8** [of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence] ... The subsequent use of the stored information has no bearing on that finding ... However, in determining whether the personal information retained by the authorities involves any ... private-life [aspect] ..., the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained ...”

## ECtHR: S. and Marper v. the United Kingdom [GC]

“The protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... [It] must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse ...”



# Tasks



The applicant had been charged with criminal offences but not convicted. Therefore, the applicant asked for his fingerprints and cellular samples to be destroyed, but the police refused. Under the Law, fingerprints and DNA samples taken from a person suspected of a criminal offence may be retained without limit of time, even if the subsequent criminal proceedings end in that person's acquittal or discharge.

**Does such Law violate Article 8 of the Convention?**

The applicant was sentenced to terms of imprisonment for rape of 15 years old minors by a person in a position of authority. The applicant was included in the national sex offender database on account of his conviction and on the basis of the law. Data on this database will be saved for 30 years.

**Does the inclusion of the applicant in the sex offender database violate Article 8?**

***S. and Marper v. the United Kingdom*** , 30562/04; Judgment  
4.12.2008 [GC]

The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests

**Violation of Article 8**

***Bouchacourt v. France* (no 5335/06); *Gardel v. France* (no 16428/05); *M.B. v. France* (no 22115/06)**

The Court took the view that the length of the data conservation – 30 years maximum – was not disproportionate in relation to the aim pursued – prevention of crime – by the retention of the information. Moreover, the consultation of such data by the court, police and administrative authorities, was subject to a duty of confidentiality and was restricted to precisely determined circumstances

**No violation of Article 8**



**RIGHT**  
TO BE FORGOTTEN  
ONLINE



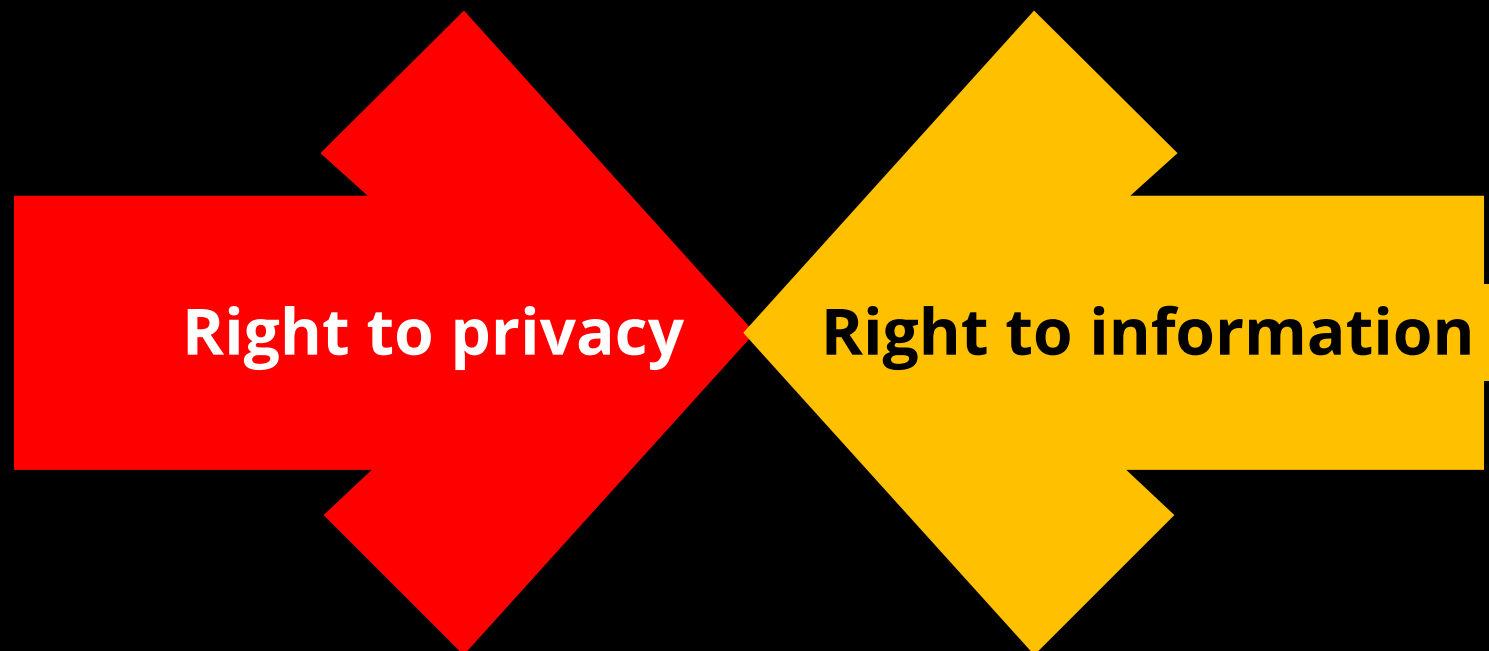
# Right to be forgotten

The right to be forgotten is a new and developing area of Internet privacy rights that refers to the right an individual has to have information about him or her removed from the Internet, even when that information is factually correct

The right is primarily grounded in notions of privacy and data protection but also relates to intellectual property, reputation, and right of publicity

Critics contend that the right to be forgotten stands in conflict with freedom of expression and can lead to revisionist history

# Conflict of interests



## "Google case" (C-131/12) ruling of 13 May 2014 of the EUCJ

Spanish citizen complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant.



# "Google case": CJEU position

On the territoriality of EU rules: Even if the physical server of a company processing data is located outside Europe, EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State which promotes the selling of advertising space offered by the search engine

On the applicability of EU data protection rules to a search engine: Search engines are controllers of personal data. Google can therefore not escape its responsibilities before European law when handling personal data by saying it is a search engine. EU data protection law applies and so does the right to be forgotten

On the “Right to be Forgotten”: Individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing. **BUT: right to be forgotten is not absolute and case-by-case assessment is needed**

# Right to be forgotten

GDPR has explicitly recognized the right to be forgotten, both with respect to its territorial scope and its material scope.

More in particular, the burden of proof has now been reversed, which makes the right to be forgotten more effective and meaningful for individuals. As a result, the controller now has to prove that the data cannot be erased because it is still relevant.

# Material scope – Article 17 of the Regulation

Pursuant to Article 17 of the Regulation, the individual who wishes to have certain data erased can now request this erasure in certain situations.

Article 17 of the Regulation includes an obligation for a controller, who has made the personal data public and who is required to erase this personal data, to take "reasonable steps" to inform controllers which are processing the personal data that the data subject has requested the erasure of any links to his personal data.

## The grounds of the right to request delisting under Art. 17(1) of GDPR

The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed

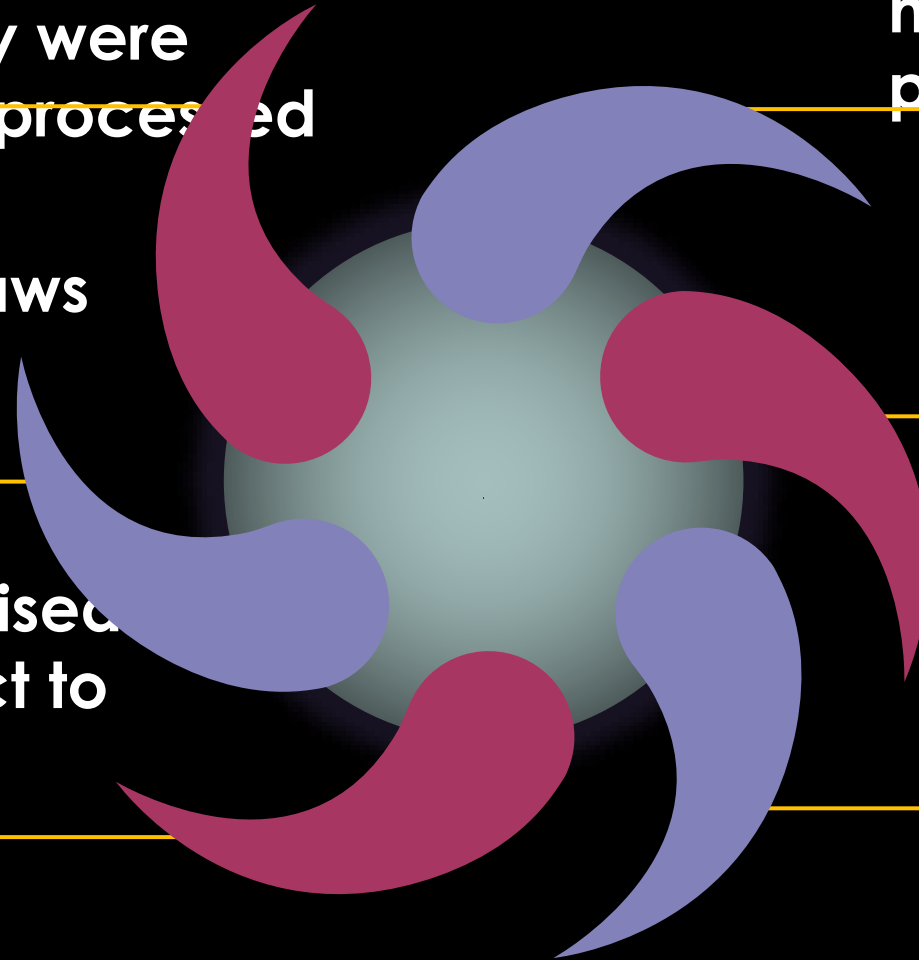
The personal data have been unlawfully processed

The data subject withdraws consent on which the processing is based

The erasure is compliant with a legal obligation

The data subject exercised his or her Right to object to processing of his or her personal data

The personal data have been collected in relation to the offer of information society services to a minor





# Exceptions to the right to request delisting (Art. 17(3) of GDPR)

Right of  
freedom of  
expression and  
information

Legal claims

Compliance  
with a legal  
obligation

Official  
authority of the  
controller

Public interest

# CJEU: Case C-507/17 *Google Inc v. CNIL* (24/09/2019)

Case concerns the territorial scope of European data protection law and extraterritorial application of the right to be forgotten

Google delisted results only in relation to EU domains, such as Google.de or Google.fr, not domains outside of the EU such as Google.com. CNIL requested that Google delist search results subject to a successful request for erasure from all domains worldwide.

CNIL insists that the RTBF can only be effectively enforced if information is genuinely 'deleted' not just on EU domains

Google pinpoints that an obligation to apply the RTBF extraterritorially may compel firms to breach law elsewhere

# CJEU: Case C-507/17 *Google Inc v. CNIL*

EUCJ ruled that the EU's Right to be forgotten does not require Google to delist search results globally, thus keeping the results available to be seen by users around the world.

## ECtHR: Węgrzynowski and Smolczewski v. Poland

The Court has reiterated on numerous occasions that freedom of expression constitutes one of the essential foundations of a democratic society and in that context the safeguards guaranteed to the press are particularly important. The Court has also observed that the most careful of scrutiny under Article 10 is required where measures or sanctions imposed on the press are capable of discouraging the participation of the press in debates on matters of legitimate public concern. Furthermore, particularly strong reasons must be provided for any measure limiting access to information which the public has the right to receive.

**No violation of Article 8**



## ECtHR: *M.L. and W.W. v. Germany*

In 1993 the applicants were convicted of the murder of a well-known actor and sentenced to life imprisonment. In 2007, with the date of their release from prison approaching, they brought proceedings against several media organisations, requesting that they anonymise archive documents which were accessible on their Internet sites and dated from the time of the trial (an article, a file and the transcription of an audio report).

## ECtHR: *M.L. and W.W. v. Germany*

Balancing of the competing interests could result in different outcomes, depending on whether the deletion request was made against the entity which had originally published the information, or against a search engine.

For the reasons set out below, the Court concluded that the refusal to grant the applicants' request had not been in breach of the German State's positive obligations to protect the applicants' private lives. In view (i) of the national authorities' margin of appreciation in such matters when weighing up divergent interests, (ii) of the importance of maintaining the availability of reports whose lawfulness had not been contested when they were initially published, and (iii) of the applicants' conduct vis-à-vis the press.

**No violation of Article 8**

## ECtHR: *Biancardi v. Italy* (77419/16)

The applicant, editor-in-chief of an online newspaper, published an article about a fight, followed by a stabbing, which had taken place in a restaurant, and the related criminal proceedings. One of the accused and the restaurant requested that the article be removed from the Internet. The applicant initially refused to do so, but eventually, eight months later, de-indexed the article in an effort to settle the case they had brought before the domestic courts. The latter, however, found the applicant liable for not having de-indexed it for an excessive period of time despite the plaintiffs' formal request, thus allowing anyone to access information related to the criminal proceedings in issue by simply typing into the search engine the names of the restaurant or of the accused

## ECtHR: *Biancardi v. Italy* (77419/16)

Two main features characterised the present case: (1) the period for which the online article had remained on the Internet and the impact thereof on the right of the private individual in question to have his reputation respected; (2) the nature of the data subject in question, a private individual not acting within a public context as a political or public figure. Indeed, anyone, well-known or not, could be the subject of an Internet search, and his or her rights could be impaired by continued Internet access to his or her personal data. The Court noted that not only Internet search engine providers could be obliged to de-index material but also administrators of newspaper or journalistic archives accessible through the Internet. It also agreed with the domestic courts' rulings that the prolonged and easy access to information on the criminal proceedings concerning the restaurant owner had breached his right to reputation.

**No violation of Article 10**

# Right to be forgotten: national case-law

**Dutch surgeon wins landmark 'right to be forgotten' case:** surgeon had “an interest in not indicating that every time someone enters their full name in Google’s search engine, (almost) immediately the mention of her name appears on the ‘blacklist of doctors’, and this importance adds more weight than the public’s interest in finding this information in this way”.

**Google victory in German top court :** former managing director of a charity had demanded Google remove links to certain news articles that appeared in searches of his name. The articles from 2011 reported that the charity was in financial trouble and that the manager had called in sick. He later argued in court that information on his personal health issues should not be divulged to the public years later. The court ruled that whether links to critical articles have to be removed from the search list always depends on a comprehensive consideration of fundamental rights in the individual case.

Google

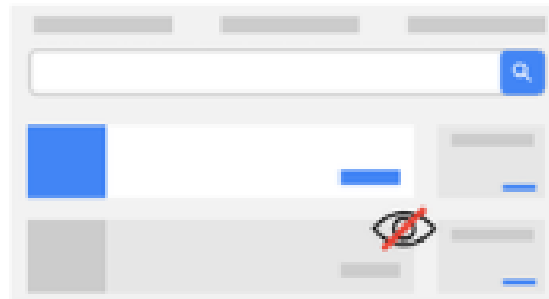


# Google Transparency Report



**4.9 M**

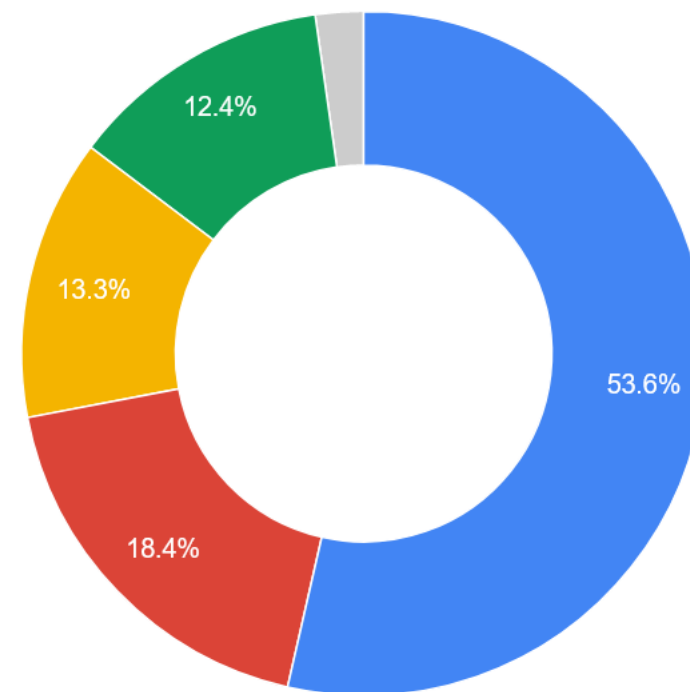
URLs requested to be  
delisted



**48,8%**

URLs delisted

Categories of websites hosting content requested for delisting



Miscellaneous News Directory Social media Other

<https://transparencyreport.google.com/eu-privacy/overview>



## Who makes requests?



Private  
Individual

89%



Other

11%



Minor

40%



Corporate  
Entity

21%



Gov. Official /  
Politician

21%



Non-Gov.  
Public Figure

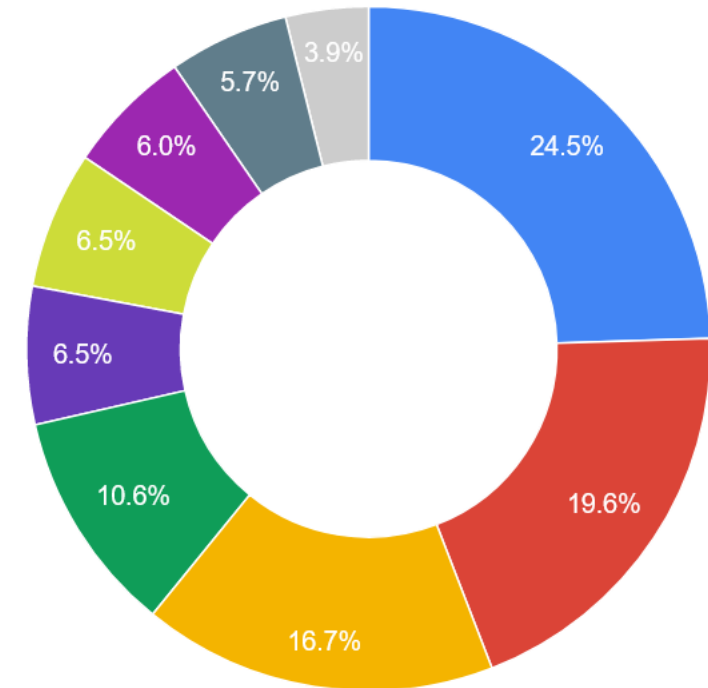
14%



Other

4%

## Categories of content requested for delisting



- Insufficient information
- Name not found
- Professional information
- Miscellaneous
- Crime
- Self authored
- Personal information
- Professional wrongdoing
- Other

# Google transparency report

<https://transparencyreport.google.com/eu-privacy/overview>

# Mass surveillance



# Klass and Others v. Germany (6 September 1978 (judgment))

Five German lawyers complained in particular about legislation in Germany empowering the authorities to monitor their correspondence and telephone communications without obliging the authorities to inform them subsequently of the measures taken against them.

The European Court of Human Rights held that there had been **no violation of Article 8** of the European Convention on Human Rights, finding that the German legislature was justified to consider the interference resulting from the contested legislation with the exercise of the right guaranteed by Article 8 as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime.



# Roman Zakharov v. Russia [GC] (4 December 2015)

This case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court held that there had been a **violation of Article 8** of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications.

# Big Brother Watch and Others v. the United Kingdom

The applicants, a number of companies, charities, organisations and individuals challenged three types of surveillance conducted by the Britain's intelligence agency:

- bulk interception of communications (**violation of Art. 8**). Shortcomings in the legislation meant that the bulk interception regime had been incapable of keeping the “interference” with citizens’ private life rights to what had been “necessary in a democratic society”
- the receipt of intercept material from foreign governments and intelligence agencies (**no violation of Art. 8**). Sufficient safeguards had been in place to protect against abuse and to ensure that UK authorities had not used requests for intercept material from foreign intelligence partners as a means of circumventing their duties under domestic law and the Convention.
- the obtaining of communications data from service providers (**violation of Art. 8**). Operation of the regime had not been “in accordance with the law”

# Surveillance of telecommunications in a criminal context

Since it represents a serious interference with the right to respect for correspondence, it must be based on a “law” that is particularly precise (**Huvig v. France**, § 32) and must form part of a legislative framework affording sufficient legal certainty

A person who has been subjected to telephone tapping must have access to “effective scrutiny” to be able to challenge the measures in question (**Marchiani v. France** (dec.)).

Furthermore, the State must ensure effective protection of the data thus obtained and of the right of persons whose purely private conversations have been intercepted by the law-enforcement authorities (**Craxi v. Italy** (no. 2))



# Surveillance of telecommunications in a criminal context

With regard to secret anti-terrorist surveillance operations, adequate and effective guarantees against abuses of the State's strategic monitoring powers should exist (***Weber and Saravia v. Germany***)

# LEGAL BASIS FOR AUTHORISING PHONE INTERCEPTIONS

There has to be a legal basis for the interception of communications  
this legal basis has to be publicly accessible it has to specify:

the nature of offences that give rise to an interception order

the category of persons liable to have their phone tapped

a limit on the duration of phone tapping

the procedure to be followed for examining, using and storing the data obtained

precautions to be taken when communicating the data to other parties

the circumstance under which the recordings or tapes may or must be erased

precautions have to be taken to protect privileged communication between attorney and client

# Monitoring at work



# Copland v. the United Kingdom, 3 April 2007

Copland was employed by the College, a State-administered body. At the deputy principal's request, her telephone, internet and e-mail use were monitored in order to ascertain whether she was making excessive personal use of them.

The parties disputed the nature and duration of the monitoring. The government claimed Copland's telephone use was monitored only by analysing College telephone bills, while Copland claimed her incoming calls were also monitored, and that the length, volume and telephone numbers were logged. The government claimed that Copland's telephone calls and e-mails were monitored for a few months, while Copland claimed that her calls were monitored for at least 18 months, and her e-mails for at least six months.

At the time, the College did not have a policy on monitoring employees' communications.

# Copland v. the United Kingdom, 3 April 2007

- telephone calls from business premises are prima facie covered by the notions of “private life” and “correspondence”. It followed logically that e-mails sent from work should be similarly protected, as should information derived from the monitoring of personal internet usage.
- Applicant had been given no warning that her calls would be liable to monitoring and therefore had a reasonable expectation as to the privacy of calls made from her work telephone.
- collection and storage of personal information relating to the applicant’s use of the telephone, e-mail and internet, without her knowledge, had amounted to an interference with her right to respect for her private life and correspondence.
- in the absence of any domestic law regulating monitoring at the material time, the interference was not “in accordance with the law”.

**Violation of Article 8**

# Bărbulescu v. Romania

Mr Barbulescu's employers asked him to create a Yahoo Messenger account for responding to client enquiries and informed him that these communications would be monitored. The records showed that he had used the Internet for personal purposes, contrary to internal regulations. The employer's regulations explicitly prohibited all personal use of company facilities, including computers and Internet access. The employer had accessed the Yahoo Messenger account in the belief that it had contained professional messages.

Mr Barbulescu maintained in writing that he had only used the account for professional purposes. The employer produced a transcript of his communications on Yahoo Messenger and it was not disputed that some messages contained sensitive personal data.

Mr Barbulescu's employment was terminated for breach of the company's internal regulations which specified that computers were not to be used for personal purposes. Mr Barbulescu challenged his employer's decision on the basis that it was null and void since, by accessing his communications, his employer had violated his right to correspondence.

# Bărbulescu v. Romania, 12 January 2016

In its Chamber judgment the European Court of Human Rights held, by six votes to one, that there had been **no violation of Article 8** of the Convention, finding that the domestic courts had struck a fair balance between Mr Bărbulescu's right to respect for his private life and correspondence under Article 8 and the interests of his employer. The Court noted, in particular, that Mr Bărbulescu's private life and correspondence had been engaged. However, his employer's monitoring of his communications had been reasonable in the context of disciplinary proceedings.



# Bărbulescu v. Romania, 5 September 2017 [GC]

The Grand Chamber held, by eleven votes to six, that there had been a **violation of Article 8** of the Convention, finding that the Romanian authorities had not adequately protected the applicant's right to respect for his private life and correspondence. They had consequently failed to strike a fair balance between the interests at stake. In particular, the national courts had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; nor had they had regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or the degree of intrusion into his private life and correspondence. In addition, the national courts had failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge.

# Libert v. France, 22 February 2018

This case concerned the dismissal of an SNCF (French national railway company) employee after the seizure of his work computer had revealed the storage of pornographic files and forged certificates drawn up for third persons. The applicant complained in particular that his employer had opened, in his absence, personal files stored on the hard drive of his work computer.

The Court held that there had been **no violation of Article 8** of the Convention, finding that in the present case the French authorities had not overstepped the margin of appreciation available to them. French law foresaw that all files created by employees on a work computer were to be considered as being of professional nature, unless identified as personal

# ***López Ribalda and Others v. Spain [GC], 17 October 2019***

The applicants worked as cashiers and sales assistants in a supermarket. The supermarket had been sustaining economic losses. In order to investigate these losses, the employer of the applicants decided to install surveillance cameras. Some of the cameras were in plain sight while others were hidden. The applicants were notified of the presence of the cameras that were visible, but not about those that were hidden. The applicants were dismissed when video footage showed that they had been stealing items.

# ***López Ribalda and Others v. Spain [GC]***, 17 October 2019

Chamber of the Court held, by six votes to one, that there had been a **violation of Article 8**. In the Court's view, the video-surveillance carried out by the employer, which had taken place over a prolonged period of time, had not complied with the requirements stipulated in the relevant legislation. Moreover, the domestic courts had failed to strike a fair balance between the applicants' right to respect for their private life and their employer's interest in the protection of its property rights

# ***López Ribalda and Others v. Spain [GC]***, 17 October 2019

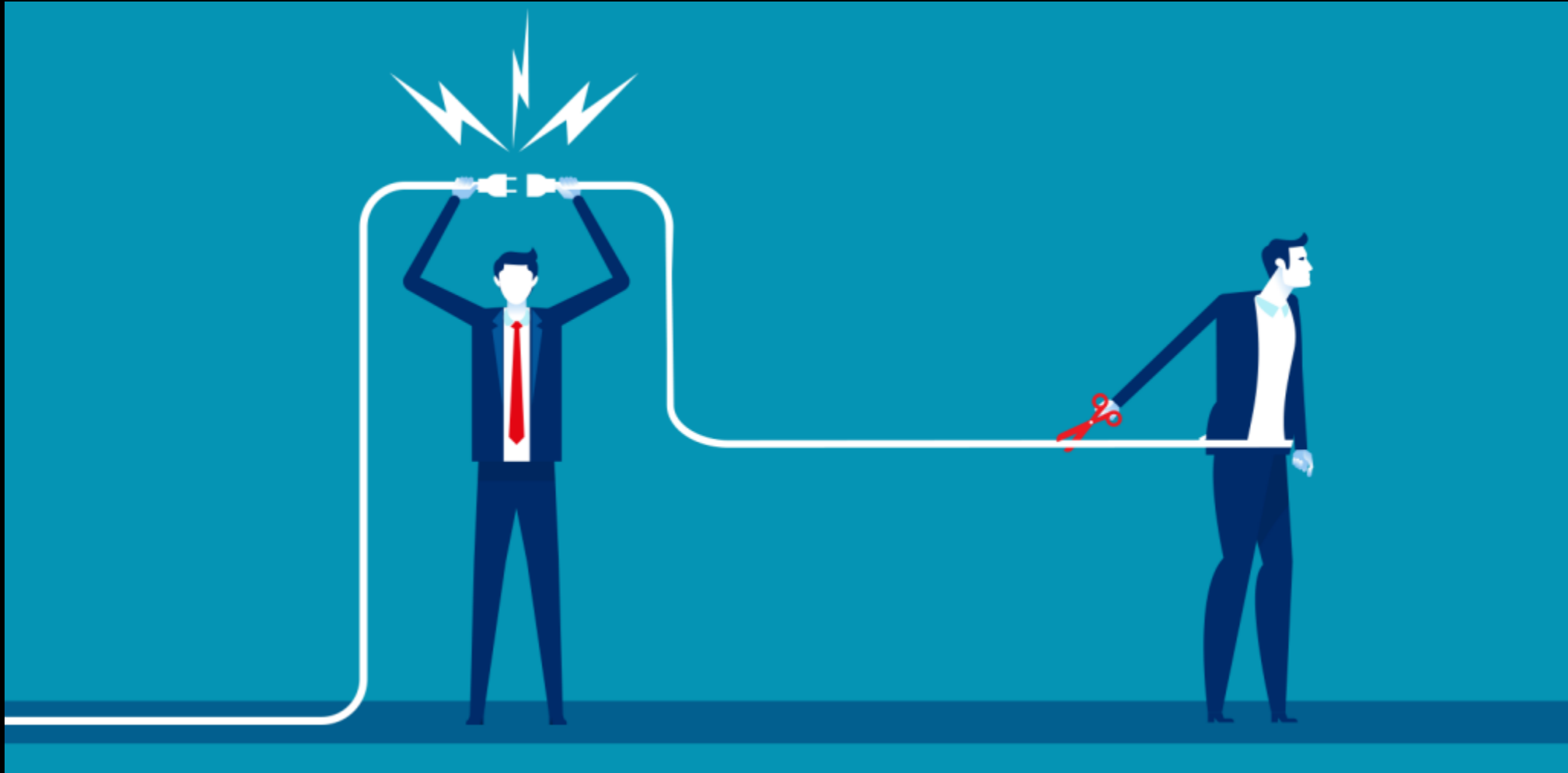
- installation of the video-surveillance had been justified by legitimate reasons, namely the suspicion that thefts had been committed. The courts had then examined the extent of the monitoring and the degree of intrusion into the applicants' privacy, finding that the measure had been limited as regards the areas and staff being monitored and that its duration had not exceeded what was necessary in order to confirm the suspicions of theft.
- The length of the monitoring (ten days) had not appeared excessive in itself. Only the supermarket manager, the company's legal representative and the union representative had viewed the recordings obtained through the impugned video-surveillance before the applicants themselves had been informed.
- The consequences of the impugned monitoring for the applicants had been significant. However, the video-surveillance and recordings had not been used by the employer for any purposes other than to trace those responsible for the recorded losses of goods and to take disciplinary measures against them
- Having regard to the significant safeguards provided by the Spanish legal framework, including the remedies that the applicants had failed to use, and the weight of the considerations justifying the video-surveillance, as taken into account by the domestic courts, the national authorities had not failed to fulfil their positive obligations under Article 8 such as to overstep their margin of appreciation.

**No violation of Article 8 (Grand Chamber)**

## **Criteria for the assessment of proportionality of video-surveillance measures in the workplace:**

- whether the employee had been notified of the possibility of video-surveillance measures being adopted by the employer and of the implementation of such measures;
- the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy;
- whether the employer had provided legitimate reasons to justify monitoring and the extent thereof;
- whether it would have been possible to set up a monitoring system based on less intrusive methods and measures;
- the consequences of the monitoring for the employee subjected to it;
- whether the employee had been provided with appropriate safeguards, especially where the employer's monitoring operations were of an intrusive nature: such safeguards might take the form, among others, of: the provision of information to the employees concerned or the staff representatives as to the installation and extent of the monitoring; a declaration of such a measure to an independent body; or the possibility of making a complaint.

# Right to disconnect

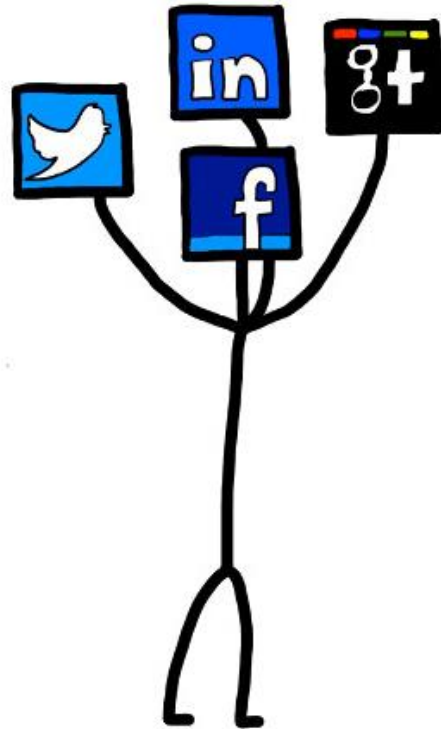


The right to disconnect refers to a worker's right to be able to disengage from work and refrain from engaging in work-related electronic communications, such as emails or other messages, during non-work hours.



# Social networks and privacy

We see  
EVERYTHING





[https://www.youtube.com/watch?v=-e98hxHZiTg&feature=emb\\_title](https://www.youtube.com/watch?v=-e98hxHZiTg&feature=emb_title)

# Threats to Privacy on Social Media

## Data Mining

Personal data is stored and leveraged by companies to better target advertising to their users. Sometimes, companies share users' data with third-party entities, often without users' knowledge or consent

## Phishing Attempts

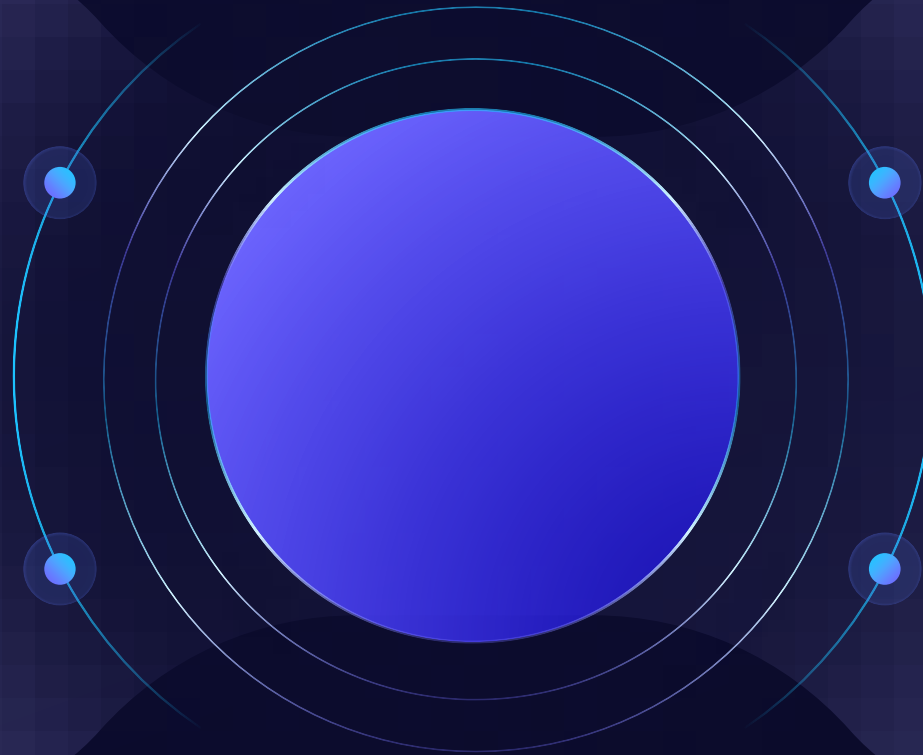
Often in the form of an email, a text message, or a phone call, a phishing attack presents itself as a message from a legitimate organization. These messages trick people into sharing sensitive data, including passwords, banking information, or credit card details. Phishing attacks often pose as social media platforms

## Malware Sharing

Malware (malicious software) is designed to gain access to computers and the data they contain. Once malware has infiltrated a user's computer, it can be used to steal sensitive information, extort money, or profit from forced advertising. Social media platforms are an ideal delivery system for malware distributors

## Botnet Attacks

Social media bots are automated accounts that create posts or automatically follow new people whenever a certain term is mentioned. Bots and botnets are prevalent on social media and are used to steal data, send spam, and launch distributed denial-of-service attacks that help cybercriminals gain access to people's devices and networks





## **CJEU: *Maximilian Schrems v. Facebook Ireland Limited***

Schrems tried to sue Facebook in Austria over its participation in the U.S. National Security Agency's PRISM program, and he tried to sue the company on behalf of 25,000 other Facebook users from around the world.

Judgment: Schrems was able to sue Facebook as a consumer, but he could not bring the claims of all those other people.

# Belgium

Facebook is in violation of Belgium's privacy laws by placing tracking codes, commonly referred to as "cookies," on third-party websites.

Facebook's failure to comply with the court's order will result in a fine of 250,000 Euros a day and could reach up to 100 million Euros.



# France

Facebook has been fined €150,000 by France's privacy watchdog for violating the country's data protection rules.

Facebook has failed to properly inform users of how their personal data is tracked and shared with advertisers, though it stopped short of ordering the company to change its practices.

# Online harassment





## Volodina v. Russia (no. 2)

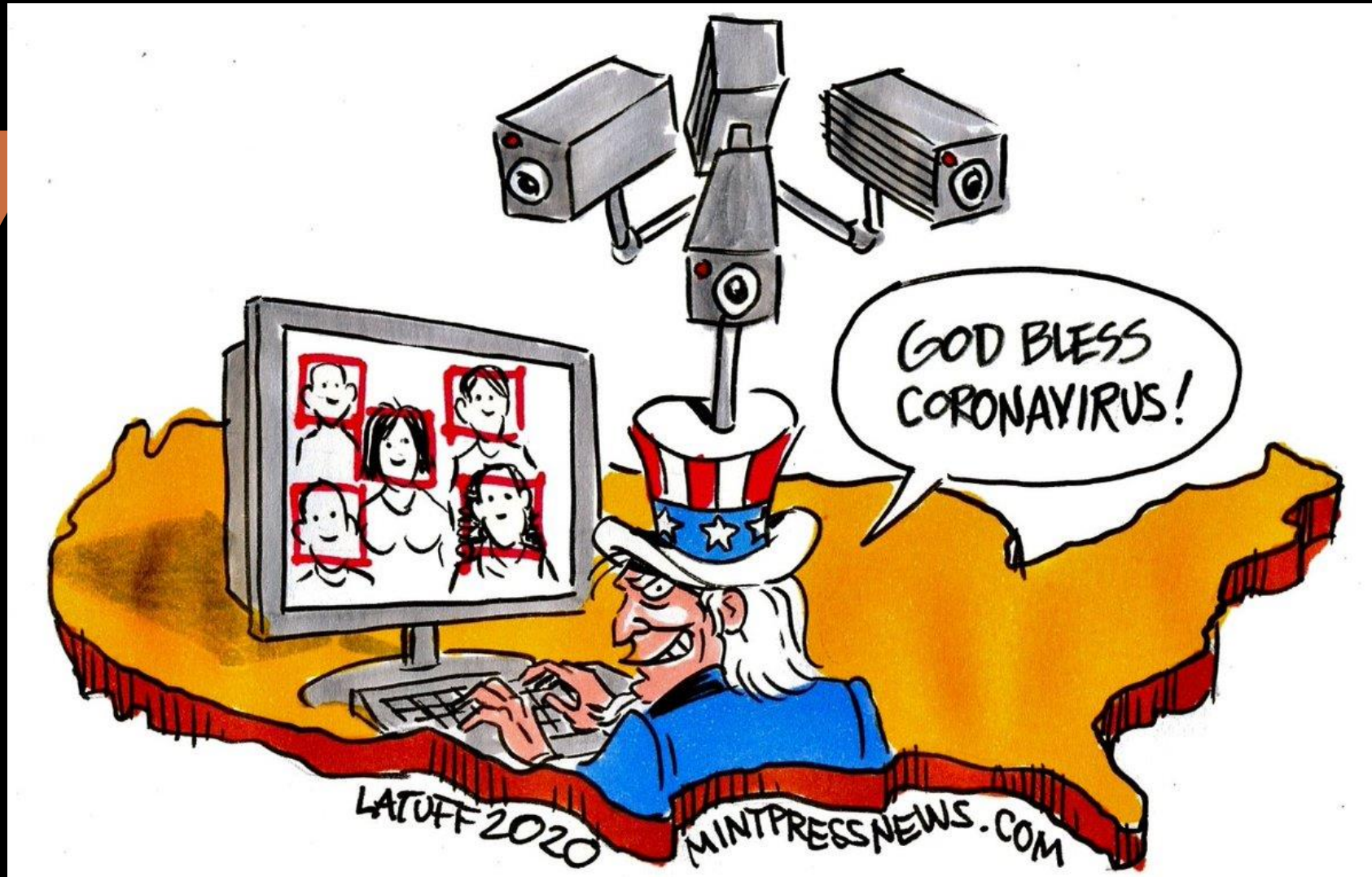
This case concerned the applicant's allegation that the Russian authorities had failed to protect her against repeated acts of cyberharassment. She submitted, in particular, that her former partner had used her name, personal details and intimate photographs to create fake social media profiles, that he had planted a GPS tracker in her handbag, that he had sent her death threats via social media; and that the authorities had failed to effectively investigate these allegations.

## Volodina v. Russia (no. 2)

The Court held that the Russian authorities had failed to comply with their obligations under that provision to protect the applicant from severe abuse. It noted, in particular, that, despite having the legal tools available to prosecute the applicant's partner, the authorities had not carried out an effective investigation and had not considered at any point in time what could and should have been done to protect the applicant from recurrent online harassment. Notably a reluctance to open a criminal case and a slow pace of the investigation resulting in the perpetrator's impunity – disclosed a failure to discharge their positive obligations under Article 8 of the Convention

### Violation of Article 8

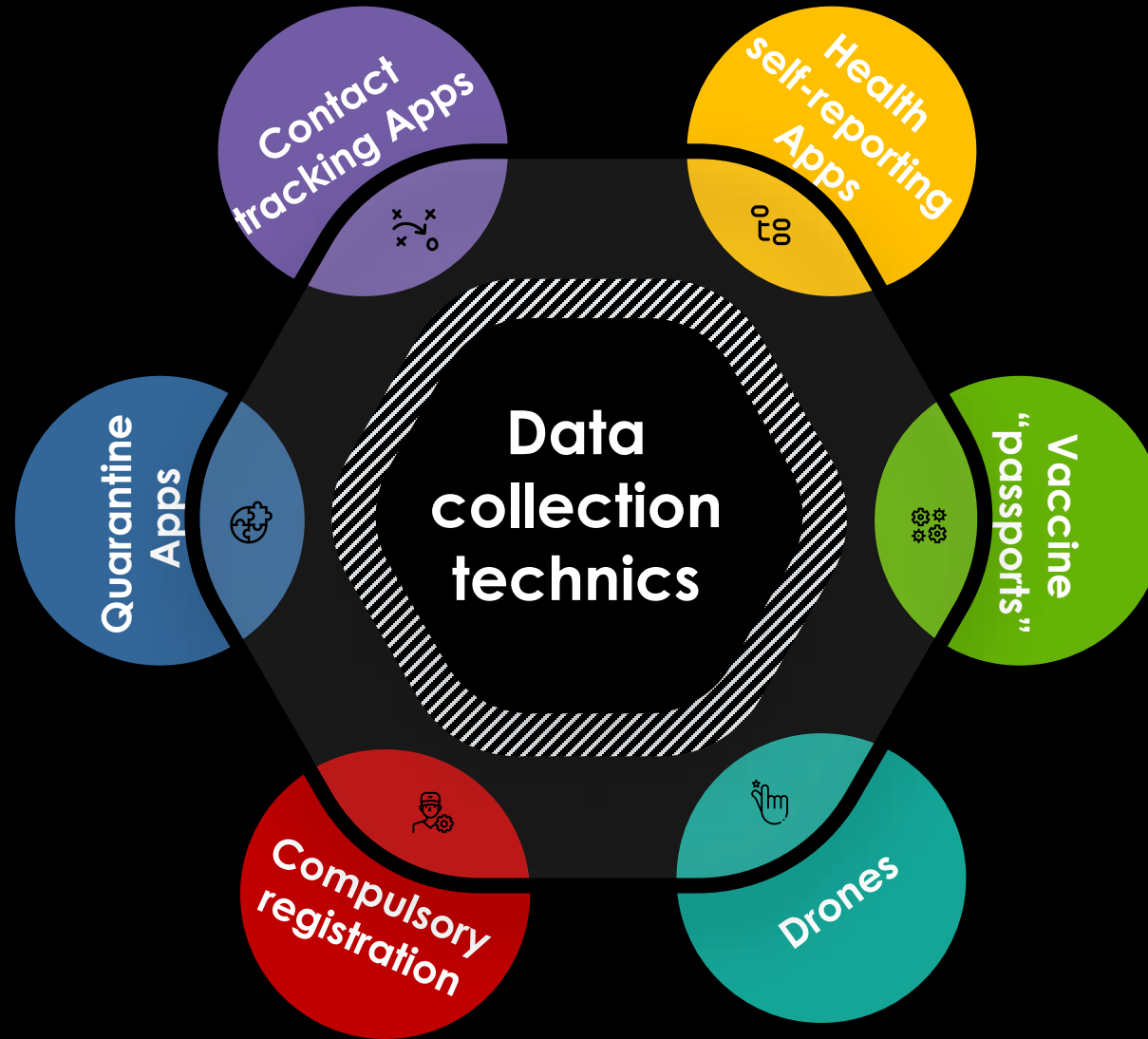
# Right to private life and COVID-19



# Issues

- 1 Data collection (medical, personal data, information about traveling, contacts, etc.)
- 2 Compulsory vaccination
- 3 Visits of family members in social care institutions, hospitals, prisons, etc.





# Risks

```
graph TD; Risks((Risks)) --> A((Collection of sensitive data)); Risks --> B((Data used for other purposes)); Risks --> C((Data accessible to the third parties)); Risks --> D((No legislation and adequate safeguards)); Risks --> E((False information)); Risks --> F((Extension of surveillance in the future)); Risks --> A;
```

**Collection  
of sensitive  
data**


**Extension of  
surveillance  
in the future**

**Data used  
for other  
purposes**

**False  
information**

**Data  
accessible  
to the third  
parties**

**No  
legislation  
and  
adequate  
safeguards**



**Data protection legislation "remains applicable and allows for an efficient response to the pandemic, while at the same time protecting fundamental rights and freedoms."**

*The European Data Protection Board*



## *Vavricka and Others v. The Czech Republic*

The applicants alleged that the various consequences for them of non-compliance with the statutory duty of vaccination (not Covid one) had been incompatible with their right to respect for their private life under Article 8 of the Convention. The judgement presented the submission of the third party interveners- the Government of France emphasised that States should be “able to adopt effective public health policies to combat serious and contagious diseases, as clearly illustrated by the COVID-19 pandemic.” The Court stated that the Czech Republic did not exceed their margin of appreciation and so the impugned measures can be regarded as being “necessary in a democratic society”

**No violation of Article 8**

## Gatsalova v. Russia

The case concerned the Russian authorities' refusal to return the body of the applicant's deceased husband, who had allegedly participated in an attack on law-enforcement authorities and was killed shortly thereafter, and the lack of an effective domestic remedy in that regard. Bodies of 95 presumed terrorists, including the body of Mr Gatsalov, were cremated. The cremations took place following a decision by the authorities not to return the bodies of the deceased to their families

Violation of Article 8



**THANK YOU**  
**QUESTIONS?**

**Contacts: [dgailiute@mruni.eu](mailto:dgailiute@mruni.eu)**