# Module 7: Protection of personal data and privacy

**Photo:** Peter Fazekas

# Media and Information Literacy
## AIR - Analyse, Interpret, React


## Authors:
Divina Frau-Meigs, Irma Velez, Pascale Garreau



This publication was created by **Savoir*Devenir** and **IREX Europe** as part of the IN EDU project - "INclusive communities through Media Literacy & Critical Thinking EDUcation" - 604670-EPP-1-2018-1-IT-EPPKA3-IPI-SOC-IN - cofinanced by the Erasmus+ programme of the European Union.

www.in-eduproject.eu

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

This manual is a key output of the IN EDU Engagement Programme. The IN EDU project partners are: Centre for Peace, Non-Violence and Human Rights; FORMA.Azione; PRIZMA; Sofia Development Association; DZZD "Obuchenie"; and ITET 'Aldo Capitini'.





**To cite this resource:**
Divina Frau-Meigs, Irma Velez, Pascale Garreau, Media and Information Literacy - AIR Analyse, Interpret, React. Savoir*Devenir, Paris 2020.

**Online:**
www.savoirdevenir.net/ressources

# Module 7: Protection of personal data and privacy

The first part of this lesson plan deals with knowledge about privacy and MIL added value.

The second part of this lesson plan, the MILAB, deals with hands-on approach to teaching about privacy.

## A few definitions (see glossary)

- Data
- Big data
- Privacy
- Phishing
- Terms of service
- GDPR
- Consumer awareness

## Outline

### PART I Knowledge building

1. Privacy before
2. Privacy in the digital world
3. Characteristics
4. Opportunities and risks
5. Learning objectives, competences and MIL added value
6. Evaluation
7. Training support materials

### PART II MILAB

1. Stage 1 activities
2. Stage 2 activities
3. Stage 3 activities

**PART I** (4x45min sessions)

## 1. Privacy before digital world (20 min)

Session 1: 45 min

Privacy is a state in which one is not observed or disturbed by other people. Signs, images and symbols that create our identity are all things that we may consider to be private and would not want to be revealed to the public because they are intimate and/or may have implications for one's safety.

It is defined by law in many countries and by the Universal Declaration of Human Rights (1948), whereby protecting personal data has to do with the integrity and safety of the person:

- **article 12 on privacy**
  - "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."

- **article 3 on safety**
  - "Everyone has the right to life, liberty and security of person."

**Teacher tip:**

Young people often do not agree with adults about what should be private and what can be public or shared with friends.

A debate on what students consider "intimate" can be a good way to start.

**References:**


DÉCLARATION UNIVERSELLE
DES Droits DE L'Homme
NATIONS UNIES

To read the whole declaration online :
https://www.un.org/fr/universal-declaration-human-rights/index.html

## 2. Privacy in relation to the digital world (25 min)

### ❖ What's new with privacy and personal data?

Online privacy is based on two types of data, as expressed in recent European General Data Protection Regulation (DGPR, 2018):

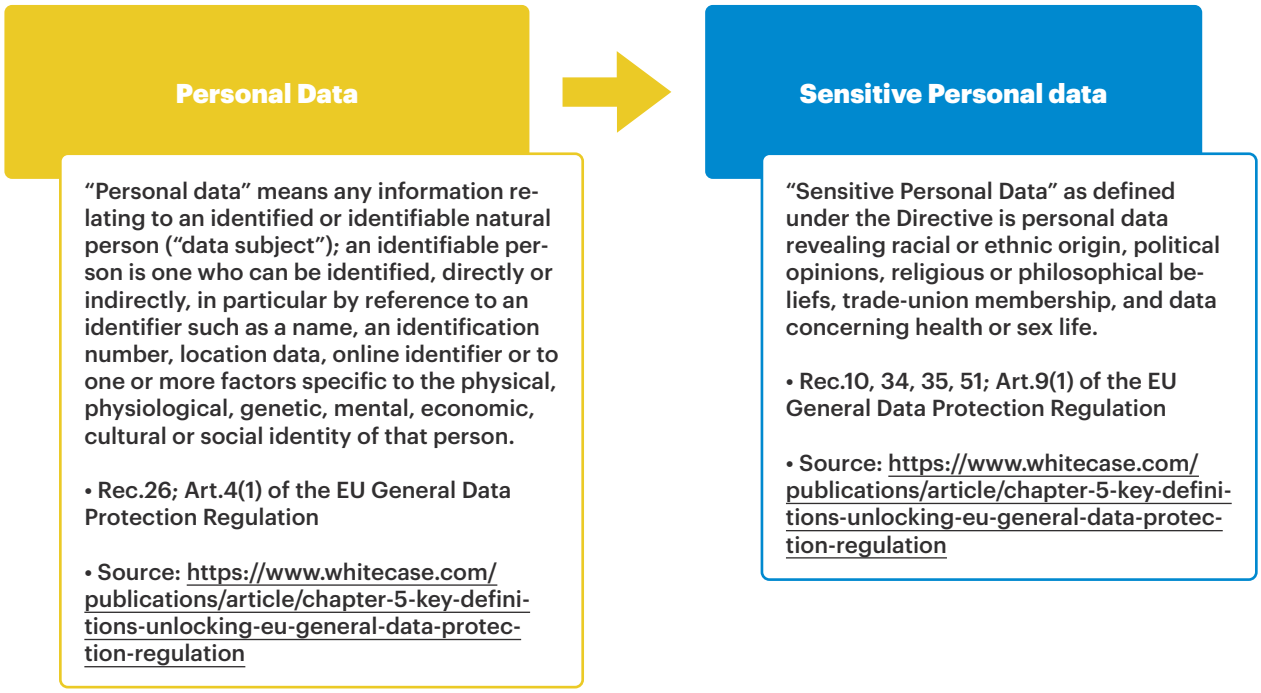



**Figure 1. Personal data vs sensitive personal data**
Source: CNIL/Savoir*Devenir

### ❖ Navigation and online activities leave digital footprints!

The internet and its networks are an infrastructure of services available via a provider that requires your data (IP address, package, ...) for stocking, surfing, streaming, networking... These services are also connected to other devices (e.g. laptop cameras, microphones) and collect data about your navigation. Your navigation leaves footprints: history, temporary internet files, geolocation, messages ...

Two types of data are collected online that may reveal elements of your privacy:

- data deliberately **provided by yourself** (civil status, public records address, text and images publications, likes, votes...)
- data generated and **gathered without your knowing it when you surf** (cookies, navigation histories, ...)

This data is gathered, analysed and used by algorithms for various purposes, mainly commercial. Profiling, prediction and nudging techniques need your data to better target you!

In the United States, even before the digital era, collecting and using personal data is ruled by commercial laws, and aggregation of data from different databases by third parties is thus permitted. In Europe, especially since the GDPR, such actions cannot be taken without the consent of citizens.

## 3. Characteristics of privacy (25 min)

Session 2: 45 min

❖ **Discussion:** what are the characteristics of privacy according to you?

- ✓ Controlling digital footprint
- ✓ Managing of digital footprint and e-reputation and e-presence
- ✓ Uploading content and publishing while making sure to keep boundaries between privacy/intimacy, public/private spheres
- ✓ Sharing contract (private and public conversations, comments, collaboration with others) Buying and selling online and issues with phishing and identity theft

**Teacher tip:**

Have students explore your national data protection centre website and the services it offers.
https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Summary

- ➤ An invasion of one's privacy rights may lead to undue surveillance and stressful situations
- ➤ Regulation online is relatively recent and varies considerably between the European Union, the USA and other regions in the world. This can lead to difficulties in a cross-border space like the internet.

**Teacher tip:**

Make sure you ask students if they have ever been surprised by spam or intrusive advertising after visiting a website. Ask them how they felt and what they should have done.

❖ Formats and examples of privacy and protection in relation to consumer awareness competences (20 min)

- ➤ Terms of service
- ➤ GDPR
  https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679
- ➤ Cookies (Mouchards)
- ➤ Geolocalisation

## 4. Opportunities and risks of privacy and data?

Session 3: 45 min

❖ **Discussion:** (15 min)

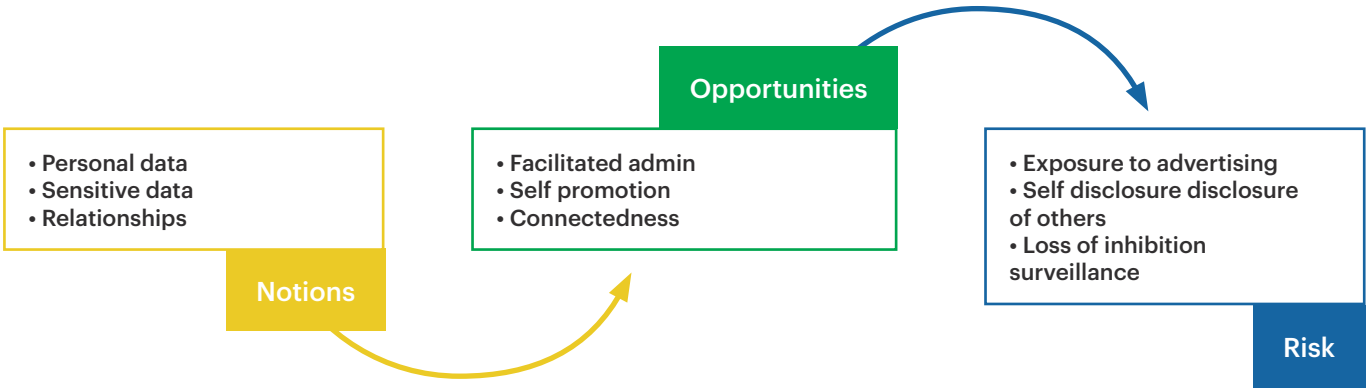
You have heard the saying "if it's free then you are the product" attributed to Andrew Lewis.

What does it means about data mining and privacy risks?


**Teacher tip:**
You may want to check US physics teacher's response on this quote (in the References box below) to understand it as the result of an historical phenomena.

**References:**
Michael Treanor, former Chemistry / Physics Teacher (1997-2017)
Answered Jun 23, 2018.
https://www.quora.com/Who-originally-suggested-that-if-youre-not-paying-for-the-product-you-are-the-product

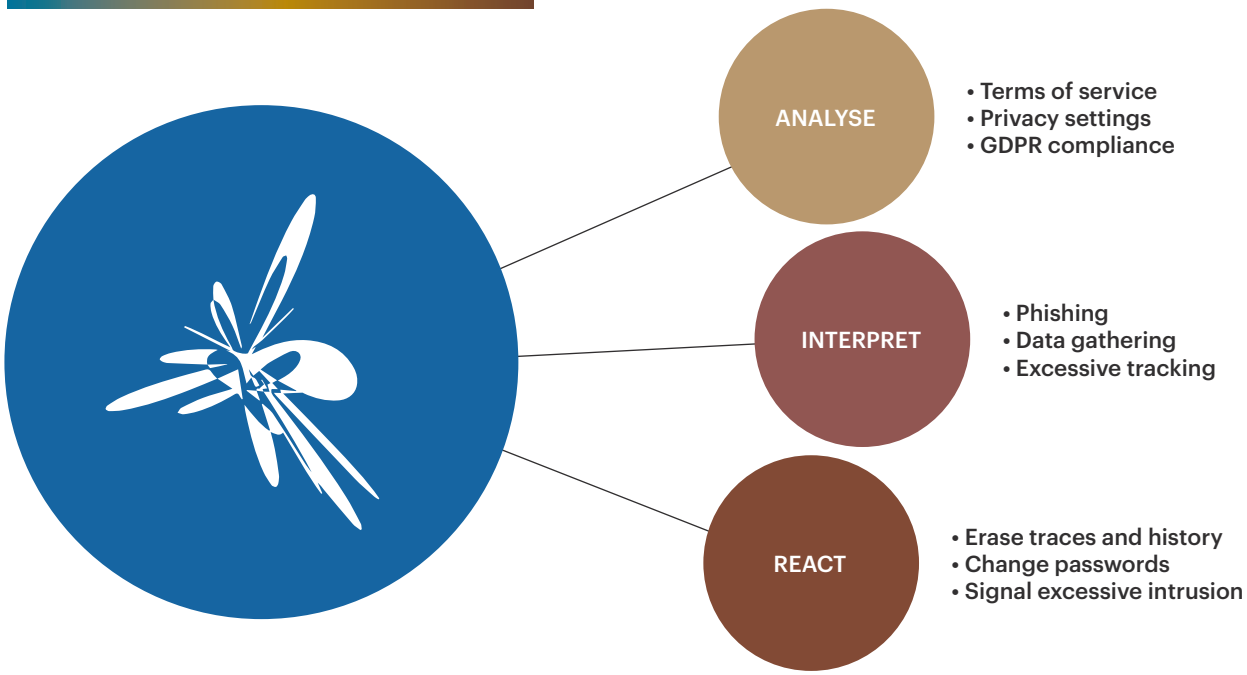
❖ Opportunities and risks (15 min)



- Risks tend to appear because the internet and social media feels like a "private space" when in reality they are a public space. It opens users as consumers to phishing and theft of personal data; exploitation of data for profiling (political, commercial...); surveillance; abuses such as cyber-bullying and hate speech.
- Opportunities appear due to a sense of connectedness and of shared interests. It opens users as consumers to e-reputation and e-presence options (social media influencers...)

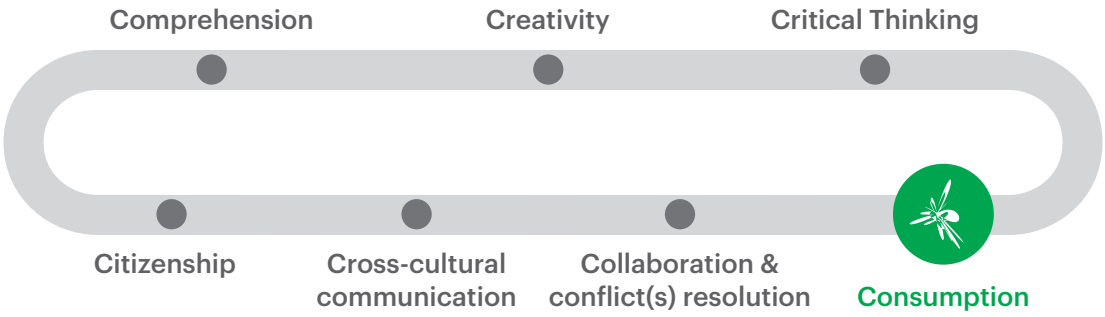
Summary

Building Students' critical thinking: AIR




## 5. Focus on CONSUMPTION/CONSUMER AWARENESS competences (7C) (15 min)

- It allows users to deal with social media and other virtual social spaces as public spaces where online products and services are being sold. Understanding the implications of the commercial reality of online spaces is key to protect users' online privacy.




**See introduction and glossary**
Source: Savoir*Devenir

❖ MIL competences break-down categories/indicators of Consumption/consumer awareness competences

Students should be able to

- Tell the difference between different digital footprints and different types of data
- Understand the way social media collects data
- Use of tools and resources to protect privacy (privacy settings)
- Protect themselves against tracking, excessive use and risks
- Understand what GDPR is and about online rights and responsibilites
- Respect others' privacy online

❖ MIL added Human Right value

✓ Freedom of expression
✓ Privacy

## 6. Evaluation (45 min)

Session 4: 45 min

Show 3 pictures and ask students to rate them for "privacy" (from 0 not safe, to 5 very safe)

## 7. Training support materials
(see additional section to Lesson Plans)

- References to other materials and resources
- Useful links for pedagogical animation
- Glossary
- Useful software for MIL integration in learning outcomes (online resources by country)
  https://docs.google.com/spreadsheets/d/10wxgYEe9O8GiSKo8kTjv8uQqpkOeHJp5_k0ytBcZsdU/edit?usp=sharing

## PART II. MILAB
## (4 x 45 min sessions, according to allotted schedule for MIL)

To go further

MILAB activities are devised according to the three stages (1-beginning, 2-consolidating and 3-deepening). The three stages are indicative: they can be followed as suggested below or used in a 'plug-in', modular approach depending upon the time allotted to MIL and/or the level of outcome desirable.

They involve several pedagogical activities including: workshops, role play, written exercises and games. They explore different media formats such as blogs, videos and web articles in order to build students' critical thinking skills (AIR).

***EXPLORING CONSUMPTION/CONSUMER AWARENESS COMPETENCE:***
***contribution to social media via tweet, post, story...***

**STAGE 1 (15-16)**
Understanding privacy and data protection

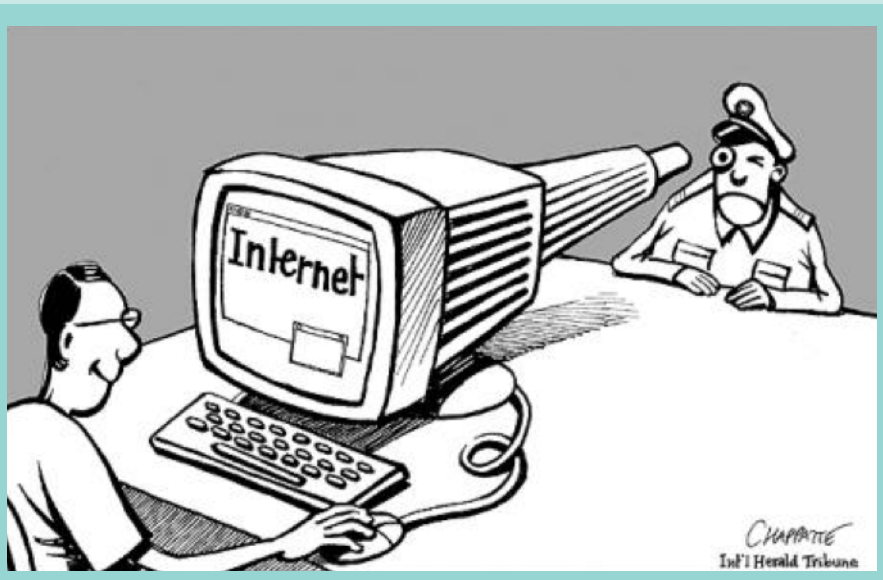



**Figure 2: Digital media provides new access for corporations wanting to track audience data.**
Source: https://wisc.pb.unizin.org/commarts250/chapter/week-15-viewing-labor/

**Teacher tip:**
You may want to introduce the topic by describing a comic visual representation of it, such as this one, try to polarize the ideas of seeing and being seen through the use of the internet.

**Debate on phishing** 2 x 45 min

*Conduct a debate on the practice of phishing:*
*Have the students reflect on online shopping, forms of payment accepted, information about products, https... but also risks of identity theft, having one's account phished, ...*
*Organize class in teams. Leave time for online research.*

**Teacher tip:**
Debate actions such as tracking, hyper-targeting, but also manipulation and propaganda.

## ➤ **Debate on phishing** (continued) 2 x 45 min

*In small groups:*
*Help students set the debate's pros and cons to protect their privacy and prevent phishing, look for both good practices and technical solutions, including encryption.*
*Have them present their arguments with a moderator.*

*Collectively: have them create a safe user checklist with items about scam/phishing prevention such as: odd email requests (about bank accounts...); suspicious subject lines (announcement of prize, award...); contact list fraud (all your contacts receive same message...); attachments by unsolicited senders (they contain viruses...). Have them write the solution in front of each item (erase, trash, block, signal, encrypt...) according to AIR critical thinking skills.*

## ➤ **Evaluation and feedback** 45 min

Observe and name the three companies in the diagram below with the most extensive tracker networks. What does it say about your personal exposure to third parties?

*The most-used cookies on the internet*
Based on a scale of 440 million page sample loaded in the study by Cliqz.

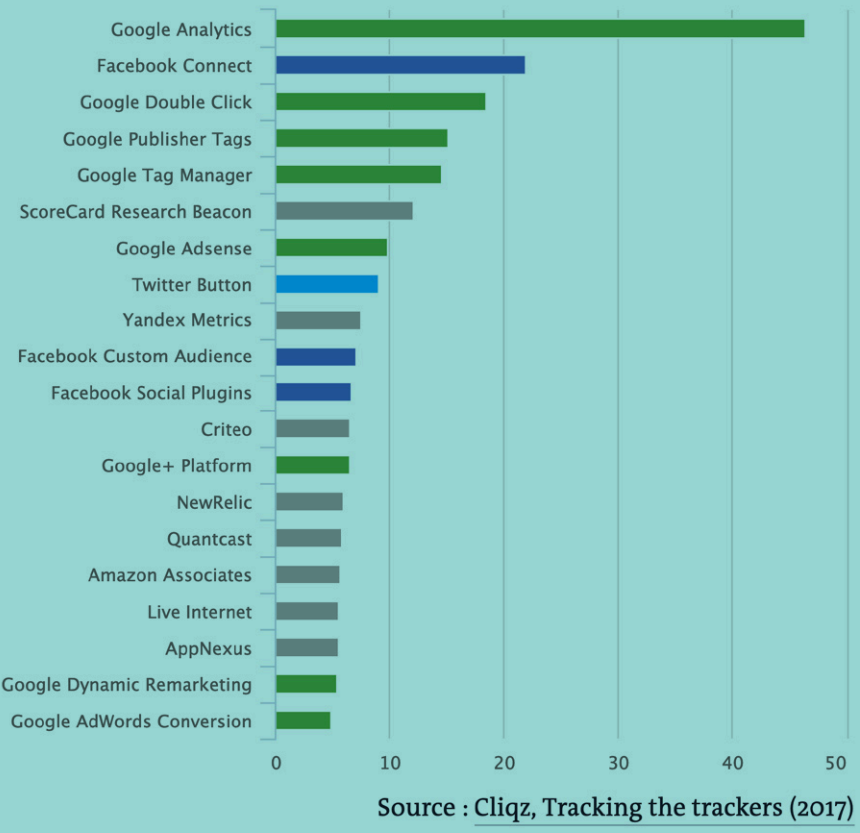



**Figure 3: The most-used cookies on the internet (Les mouchards les plus utilisés sur internet )**
Source: https://www.lemonde.fr/les-decodeurs/article/2018/03/30/cookies-mouchards-comment-vous-etes-suivis-sur-internet_5278722_4355770.html

**STAGE 2 (16-17):**
Mastering privacy online

**Simulation** 2 x 45 min

*Discuss the GDPR with students and their rights and responsibilities and options for redress*
*Link:* https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en
*Have them consider specific rights:*

1. *right to consult,*
2. *right to correct,*
3. *right to suppress personal data,*
4. *right to portability of data,*
5. *right to erasure.*

*Then have them download the template for the right to erasure*
*https://gdpr.eu/right-to-erasure-request-form/*

*Have them consider the reasons for erasure and redress in section 4 of the template. What would they put if they had an issue about how their data are being used (as children, under-age in particular).*

**Teacher tip:**
Ask students to have a debate on the right to erasure vs right to memory? Can one erase one's facts and deeds at will?

**Google search** 45 min

*Look up "Cookies" and their connection to browsing history.*
*Collect information and verify sources on how to disable cookies and how to use browser's extensions that signal and block cookies and advertising.*

**Teacher tip:**
Discuss Ghostery or uBlock Origin as ways to block cookies and adverts.

**Evaluation and feedback** 45 min

*Make the students work in small groups to discuss how to create a good password and explain the rationale behind their choice. They can help themselves with online wiki tools such as:*
https://www.wikihow.com/Create-a-Password-You-Can-Remember

**STAGE 3 (18-19)**
Building a sustainable privacy and personal data protection online

### Online search — 2 x 45 min

*Ask students to look at search engines that do not track and do not facilitate advertising, such as Qwant, DuckDuckGo, Ecosia, Lilo...*
*Have them look for their mission statements, have them identify their economic model (how are they sustainable?).*
*How do these search engines compare with the major commercial search engines, such as Google, Yahoo!...*

### Debate — 45 min

*What do they think of search engine pluralism? Are they ready to migrate to non-tracking online search to protect their privacy? How do they feel about selling their personal data to private companies to make money?*

### Evaluation and feedback — 45 min

Look at the Spanish controversy, one of the first on the Right to Erasure (or right to Be Forgotten) and look at the template for erasure.

> In May 2014, the European Court of Justice ruled against Google in Costeja, a case brought by a Spanish man, Mario Costeja González, who requested the removal of a link to a digitized 1998 article in La Vanguardia newspaper about an auction for his foreclosed home, for a debt that he had subsequently paid. He initially attempted to have the article removed by complaining to the Spanish Agency of data protection, which rejected the claim on the grounds that it was lawful and accurate, but accepted a complaint against Google and asked Google to remove the results. Google sued in the Spanish Audiencia Nacional (National High Court) which referred a series of questions to the European Court of Justice. The court ruled in Costeja that search engines are responsible for the content they point to and thus, Google was required to comply with EU data privacy laws. On its first day of compliance only (May 30, 2014), Google received 12,000 requests to have personal details removed from its search engine.

**Figure 4: González v Google**
Source: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070fr.pdf

*What were his arguments? What were Google's arguments? How was it solved? What do you feel about it?*

**Teacher tip:**
You can refer the students to the template for the right to erasure created since 2018:
https://gdpr.eu/right-to-erasure-request-form/