Evolution of the notion of privacy through history: from Aristotle to GDPR

Estelle Pawlowski-Cherrier

Cyber in Berry 2 – 16 July 2024

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

Outline

Privacy protection: definitions and issues

Evolution of the notion of privacy: some (hi)story

The informational dimension of privacy and some metrics

Privacy as a fundamental right: Privacy by Design principle and the GDPR

My personal data

- Estelle Pawlowski: estelle.pawlowski@ensicaen.fr
- Associate professor at ENSICAEN
- Teaching : Cybersecurity - Risk management - Privacy protection – Biometrics

- Research : GREYC Laboratory, SAFE Team
- Topics : biometric authentication, cybersecurity, usability, privacy protection, community detection in social graphs

- Data Protection Officer

Privacy protection: definition and issues

- Misunderstanding the history of privacy can lead to **unfounded fears**
- There are debates about privacy in **society**, in **politics** and in the **scientific communities**

- Two approaches:
  - Protection of the user's identity
    ⇨ protection of the link between data corresponding to an individual and his/her identity
  - Protection of user data (informational privacy)
    ⇨ the identity is known by the attacker
    ⇨ privacy ≈ confidentiality

⇨Privacy = a concept that depends on the time and context

The handbook of privacy studies, An Interdisciplinary Introduction. Bart van der Sloot, Aviva de Groot (eds), 2018

Privacy protection: definition and issues

What is clear:

Personal data = any information relating to an **identified** or **identifiable** individual.

An **identifiable person** is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA…)
GDPR, Art. 4, 2018

Privacy protection: definition and issues

What is less clear:

« When people want privacy, they don't want to hide away their information from everyone ; instead, they want to share it selectively and make sure that it isn't used in harmful ways.
Privacy isn't all-or-nothing – it's about modulating boundaries and controlling data flow »

The Myth of the Privacy Paradox, D. J. Solove, 2021

Privacy protection: definition and issues

What is the difference between personal data and privacy ?

Economic theory considers personal data to be specific goods, intangible resources whose exploitation affects privacy.

The definition of **personal data** is based on **technical** and **legal grounds**

≠

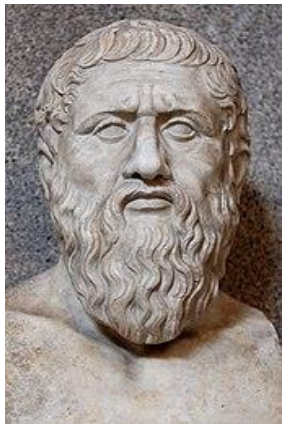
Privacy is rather a **variable-geometry concept** that depends in particular on how it is represented by the individuals themselves.

⇨ historical evolution

Evolution of the notion of privacy: some (hi)story

Before 1500

- Aristotle (384-322 BC): distinction between
  - private domestic sphere of the family (= *oikos*)
  - political activities (= *polis*)
- Hannah Arendt (1906-1975): this split separated the world of women and children (*oikos*) from that of men (*polis*)
- People identified themselves as group members ⇨ limited notion of individuality



Evolution of the notion of privacy: some (hi)story

1500-1800: from the Renaissance to the French Revolution

- Negative notion for Shakespeare: linked to solitude, political conspiracies…
- Late XVth century: England = birthplace of privacy
- Locke (1632-1704)
  ⇨ legitimate aim of individuals to protect their privacy, liberty and property

Evolution of the notion of privacy: some (hi)story

« The history of privacy is bounded; privacy, as an inspiration, didn't really exist before the rise of individualism, and the emergence of a middle class »

J. Lepore, 2007

1500-1800: from the Renaissance to the French Revolution

- A middle class is emerging (around 1500-1600): merchants, scientists/scholars, clergy
  - New sense of autonomy, new self-awareness
  - Time to take up intellectual labour
  - Liberty to choose one's own living space
- Invention of the printing press (≈ 1450)

Privacy = personal autonomy + individuality

Evolution of the notion of privacy: some (hi)story

1800-1900:

- Period of urbanization, development of communications and formation of states
- Changes in the society:
  - Significant growth of the society
  - Need for control
  - New technologies: postal mail, telegraph, telephone, photography, etc.
  - Increasing levels of education: reading, writing, exchanging letters
  - Modern journalism: tabloid press
  - Liberalism: freedom of opinion, new laws to protect individual rights

« The right to privacy » (Warren et Brandeis, 1890)

Evolution of the notion of privacy: some (hi)story

2 interpretations

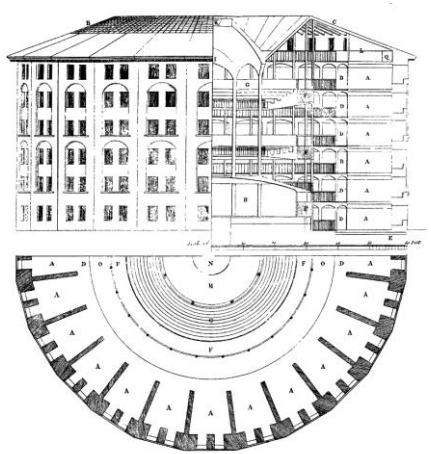
Surveillance state, all-seeing, all-knowing

- Privacy threatened
- J. Bentham's panopticon (prison architecture with a guard in a central tower)
- Disciplinary society

Privacy = the ideal and aspiration of every citizen

Important role of the Revolutions around 1800

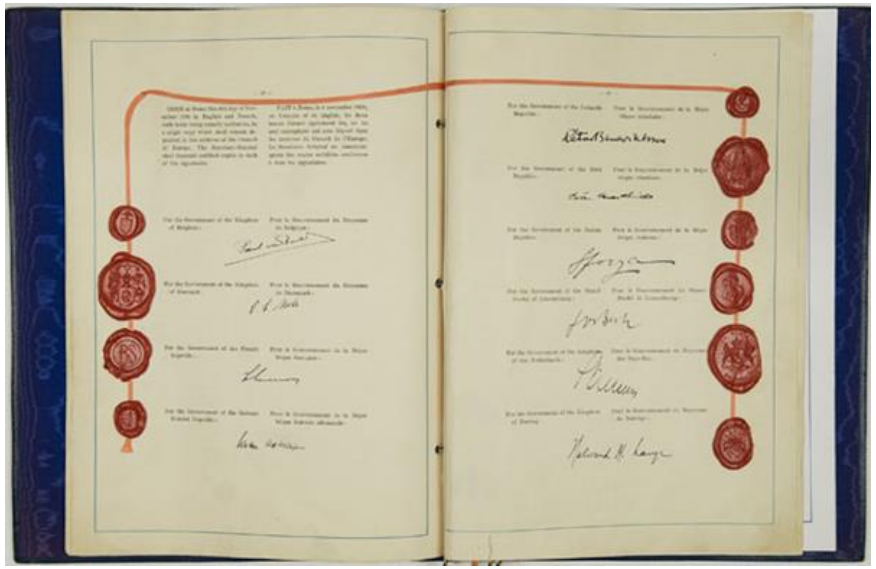
- In America: Bill of Rights
- In France: Declaration of the Rights of Man and the Citizen



Evolution of the notion of privacy: some (hi)story

1900-1970 :

- Privacy ⇨ a more fundamental and intellectual desire/expectation
- Reactions to the 2 World Wars and the end of colonialism
- 1948: Universal Declaration of Human Rights
  = proclamation of rights, only a declarative value
- European Convention on Human Rights
  = international treaty signed in 1950
- European Court of Human Rights, set up in 1959



Evolution of the notion of privacy: some (hi)story

1900-1970 :

- Welfare state (positive or negative notion)
- Women's and children's rights
- Organization and control of housing
- Surveillance files, census services
- Cold War
- Refs:
  - The Origins of Totalitarianism, Hannah Arendt (1951)
  - 1984, George Orwell (1949): police and totalitarian regime, surveillance society, reduced freedoms

Evolution of the notion of privacy: some (hi)story

1970-today: privacy in the age of the PC

New debates on data collection and privacy concerns

- 1978: French Data Protection Act

- 1981: European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

  ⇨ extends the protection of citizens and their fundamental freedoms (right to privacy)

- 1995: Directive 95/46/EC on the protection of personal data

Evolution of the notion of privacy: some (hi)story

1970-today: privacy in the age of the PC

2 well-known whistleblowers:

- 2007: Wikileaks (Julian Assange)
  « privacy for the weak and transparency for the powerful »
- 2013: Edward Snowden reveals what the American and British secret services have collected under the cover of the fight against terrorism

And finally:

2018 : General Data Protection Regulation

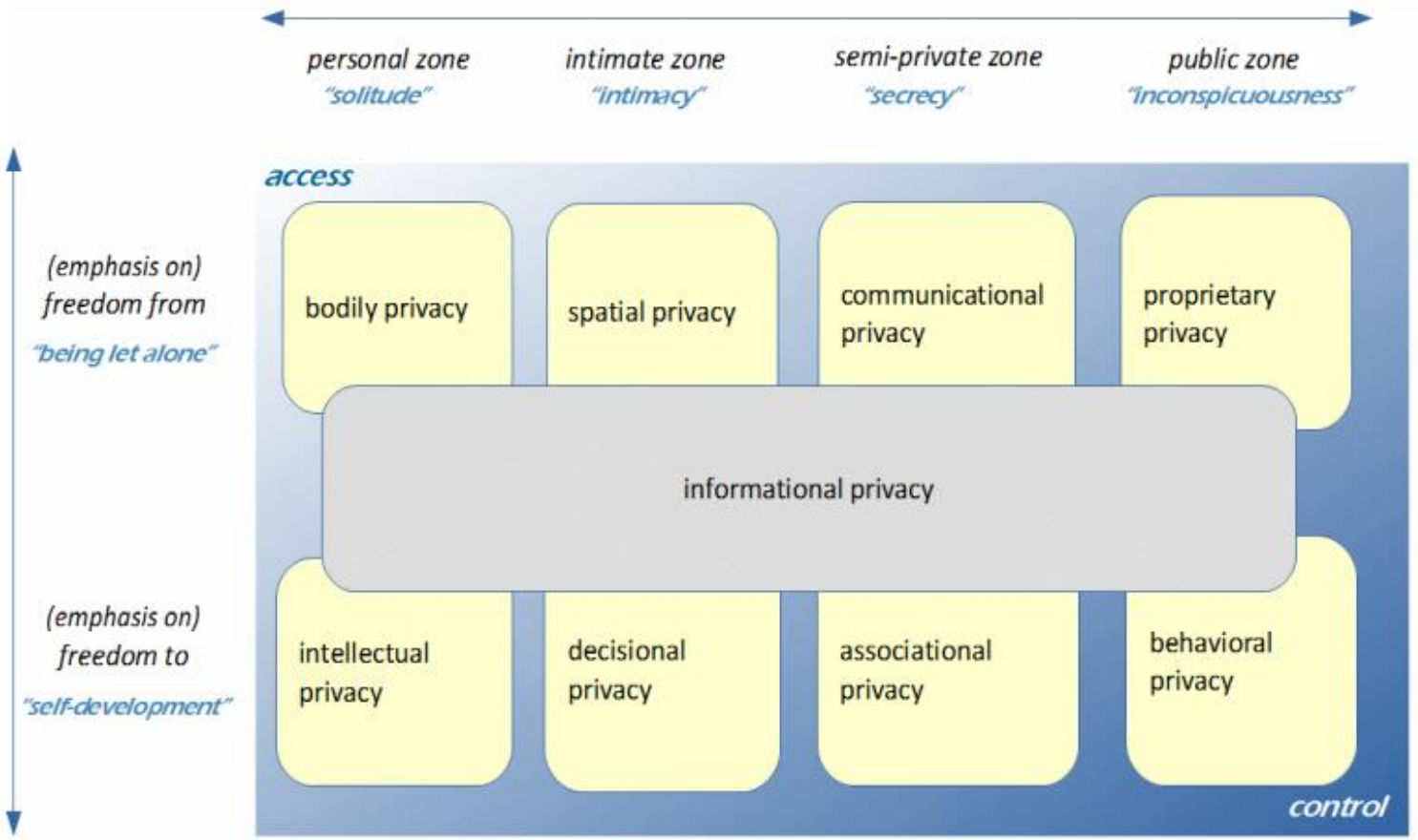
⇨ **privacy = information privacy**

Privacy protection: the informational dimension of privacy

Primary ideal types of privacy

Negative freedom

Positive freedom



A Typology of Privacy, Koops et al., University of Pennsylvania Journal of International Law,2017

Privacy protection: the informational dimension of privacy

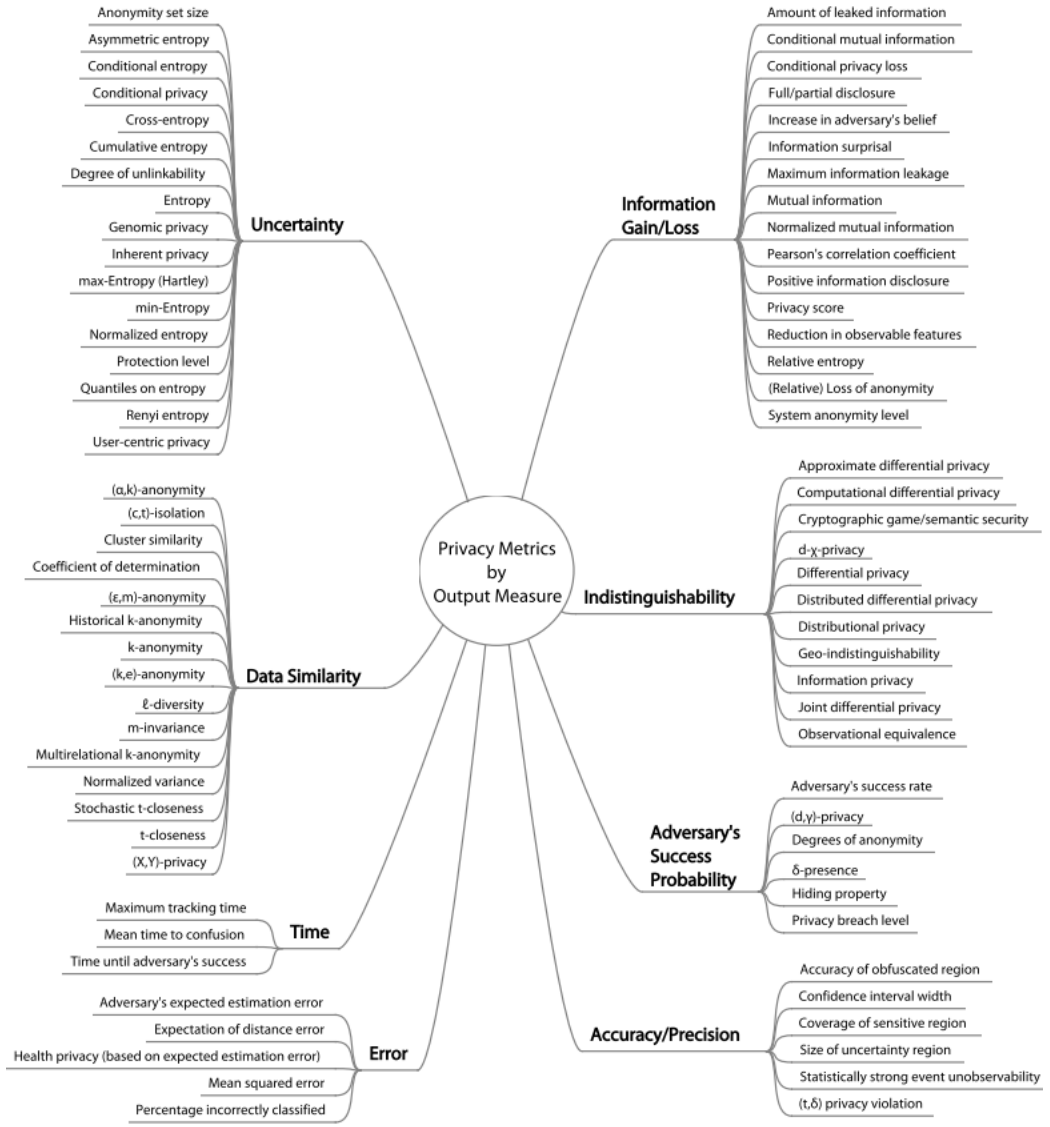
Metrics can be classified into 4 categories:

- **Adversary models** (adversary capabilities)
- **Data sources** (public data, observable data, etc.)
- The **inputs** (a wide range of information can be used to compute a metric)
- The **outputs** (8 variations dealing with confidentiality)

Privacy protection: the informational dimension of privacy

A taxonomy of the existing metrics

I. WAGNER et D. ECKHOFF. « Technical Privacy Metrics: A Systematic Survey ». ACM Computing Surveys (2018).



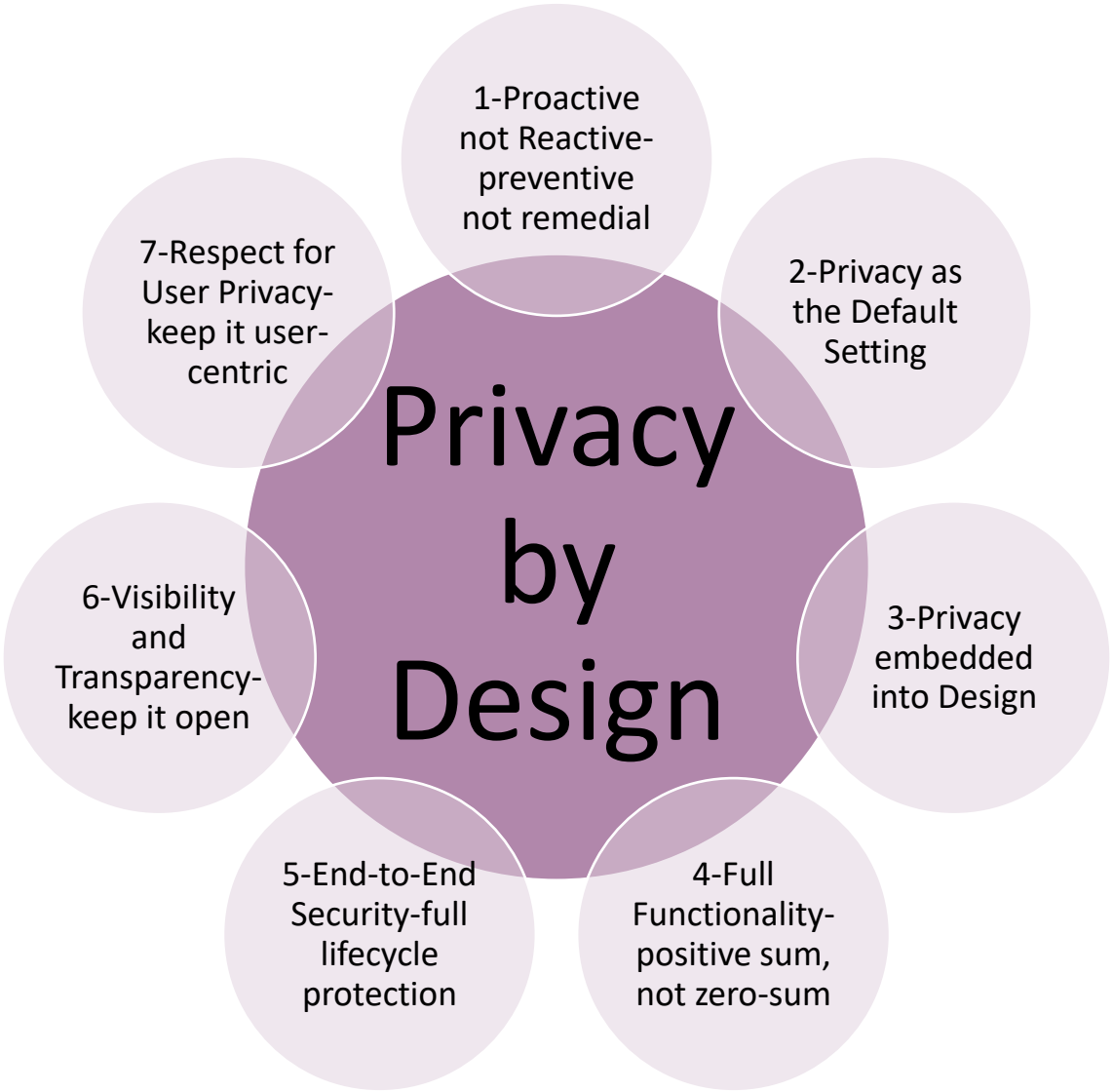
Privacy by Design

- Privacy by design (PbD) = framework first drawn up in Canada in the 1990s
- Originator = Dr. Ann Cavoukian (Privacy Commissioner of Ontario)
- Aim = to address the common issue of developers applying privacy fixes after a project is completed
- Content = the Privacy by Design framework prevents privacy-invasive events *before they happen*

⇨ 7 foundational principles

Source: Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. Ann Cavoukian, 2009

Privacy by Design



Privacy by Design

1. Proactive not Reactive; Preventive not Remedial

- PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to **prevent** them from occurring

2. Privacy as the Default

- Privacy by Design seeks to deliver the **maximum degree of privacy** by ensuring that personal data are automatically protected in any given IT system or business practice.
- This implies purpose specification, collection limitation, data minimization and use, retention, disclosure limitation

3. Privacy Embedded into Design

- Privacy by Design is embedded into the design and architecture of IT systems and business practices, without diminishing functionality

Privacy by Design

4. Full Functionality – Positive-Sum, not Zero-Sum

- Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

5. End-to-End Security – Lifecycle Protection

- Applied security standards must assure the **confidentiality**, **integrity** and **availability** of personal data throughout its lifecycle including methods of secure destruction, appropriate encryption, or strong access control and logging methods.

6. Visibility and Transparency

- All component parts and operations remain visible and transparent, to both users and providers. Remember, **trust but verify**!

7. Respect for User Privacy

- Keep it user-centric! Respect for User Privacy implies: consent, accuracy, access, compliance

GDPR: important notions

- **Data processing**:
  Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything !
- **Data controller:**
  The person who decides why and how personal data will be processed
- **Data subject:**
  The person whose data is processed
- **Data Protection Officer:**
  Their basic tasks involve understanding the GDPR and how it applies to the organization, advising people in the organization about their responsibilities, conducting data protection trainings, conducting audits and monitoring GDPR compliance, and serving as a liaison with regulators.

https://gdpr.eu/what-is-gdpr/

GDPR: important notions

Legal bases:

- Contract
- Legitimate interest
- Consent: the data subject has given his or her explicit consent to the processing.
- Legal obligation: the processing is imposed by regulatory texts.
- Public-interest mission: the processing is necessary for the performance of a task carried out in the public interest.
- Protect of vital interests: in very specific cases, it may be used as a legal basis, for example when processing is necessary to monitor the spread of epidemics or in cases of humanitarian emergency.

GDPR: data protection principles (1/2)

1. **Lawfulness, fairness and transparency —** Processing must be lawful, fair, and transparent to the data subject.

2. **Purpose limitation —** You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

3. **Data minimization —** You should collect and process only as much data as absolutely necessary for the purposes specified.

GDPR: data protection principles (2/2)

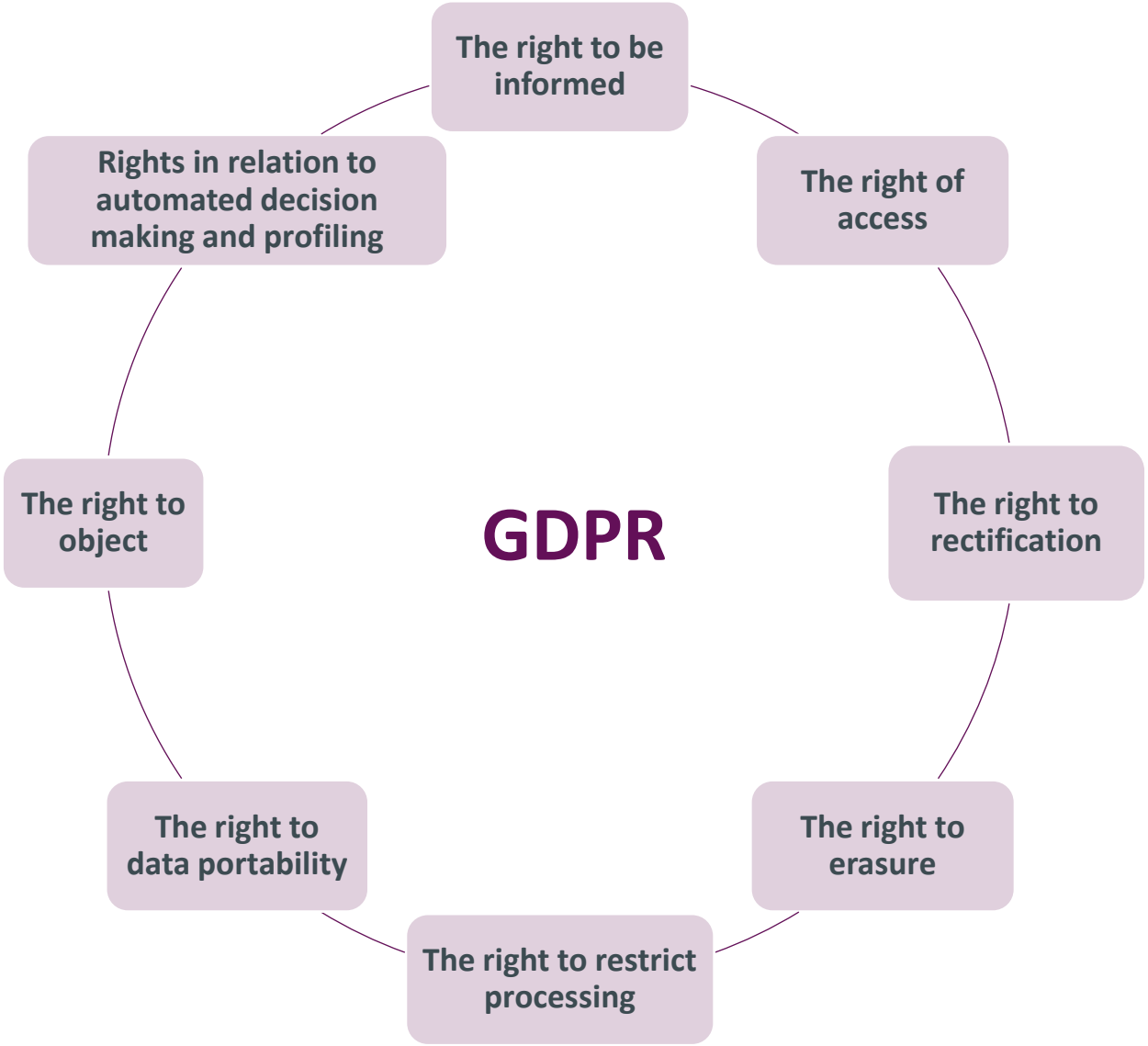
4. **Accuracy —** You must keep personal data accurate and up to date.

5. **Storage limitation —** You may only store personally identifying data for as long as necessary for the specified purpose.

6. **Integrity and confidentiality —** Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).

7. **Accountability —** The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

GDPR: Data subjects' privacy rights



GDPR: how to implement compliance ?

Sheet n°0: Develop in compliance with the GDPR

Sheet n°1: Identify personal data

Sheet n°2: Prepare your development

Sheet n°3: Secure your development environment

Sheet n°4: Manage your source code

Sheet n°5: Make an informed choice of architecture

Sheet n°6: Secure your websites, applications and servers

Sheet n°7: Minimize the data collection

Sheet n°8: Manage user profiles

Sheet n°09: Control your libraries and SDKs

Sheet n°10: Ensure quality of the code and its documentation

Sheet n°11: Test your applications

Sheet n°12: Inform users

Sheet n°13: Prepare for the exercise of people's rights

Sheet n°14: Define a data retention period

Sheet n°15: Take into account the legal basis in the technical implementation

Sheet n°16: Use analytics on your websites and applications

The CNIL publishes a GDPR guide for developers

11 June 2020

Conclusion

- **Privacy** = polysemous notion, can be related to confidentiality
- **Legal context**: GDPR is not sufficient
- **Technological context**: there is still a lot to do !

Raising awareness is vital ! (students, employees, executive committee: everybody !)

How do we stop passively inhabiting data,
and become active citizens of it ?
It's up to all of us to imagine a more just and participatory data democracy.

Jer Thorp, Living in Data, 2021


Thank You !