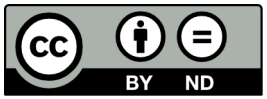
université de BORDEAUX

Personal data law

François Pellegrini
Professor, University of Bordeaux
francois.pellegrini@u-bordeaux.fr



Identity (1)

- Each person has, in the physical world, one or more appearances:
  - Professional
  - Friendly
  - Associative
  - etc.
- Identity is the way an entity is connected to its appearances

Identity (2)

- Perceived through many facets:
  - What we say about ourselves
    - Information provided when registering on a site
  - What we show of ourselves
    - Our actions
  - What can be known of ourselves
    - Traces that we leave

Digital identity

- Digital identity is the link created by digital technologies between a person and her/his various digital appearances
- Question of traces and anonymity
  - Anonymity is (still) possible in the physical world
    - Paying in cash, etc.
  - Can anonymity exist in the digital world?
    - Keepers of centralized digital accounts (or public distributed ledgers) are informed of all transactions
    - Research and practical implementations of cyber-currencies

Personal data and control (1)

- The collection of personal data is a very old activity
  - Concomitant with the invention of the administration
    - Tax collection
  - Concomitant with the invention of writing!
- The use of these data for population control is also old
  - Revenues, heredity and castes, religion, etc.

Personal data and control (2)

- The danger of mass collection of personal data appeared with the automation of their processing
  - Registration and numbering of “sensitive” populations
    - Criminal record (and other files)
    - Worker's logbook
    - Identity card for nomadic and indigenous populations
  - Use of data processing machinery for post-processing (e.g. punchcards)
    - Case of the Netherlands in the 1940s

Personal data and control (3)

- The power of digital tools has further increased the ability to control populations
  - “Cross-matching” across multiple files, rather than mere sorting from a unique file

Personal data and control (4)

- Fear of excessive intrusion by States into the privacy of individuals
  - At the time, only States had the capacity to collect masses of data
- Subsequent shift of the threat to the private sector
- Strong comeback of the States, which require access to private data silos, more or less secretly
  - In the end, it is the States that kill people

Data protection laws (1)

- Creation of specific laws
  - In Sweden, “Credit Information Act” of 1973
  - In France, “Informatics & Freedom” bill of 1978
  - Convention n° 108 of the Council of Europe, 1981
  - Directive 95/46/EC
    - Required a transposition bill in each Member State
  - Regulation EU 2016/679 “General Data Protection Regulation” (GDPR)
    - Uniform application
    - Entered into force on 25 May 2018

Data protection laws (2)

- Article 1 of French “Informatics & Freedom” bill:

  Informatics must be at the service of every citizen. Its development must take place within the framework of international cooperation. It must not interfere with human identity, human rights, privacy, or individual or public liberties.

  Everyone has the right to decide and control the uses that are made of personal data concerning him, under the conditions set by this law.

- Emergence of the constitutional principle of “informational self-determination”

Data protection laws (3)

- Establishment of Data Protection Authorities (DPAs) independent from the executive power and administrations
  - Original legal model of “Independent Administrative Authorities”
    - Can not belong to other powers by virtue of the separation of powers
    - Have to be
  - E.g.: the French CNIL
    - Commissioners & staff

Personal data (1)

- Only relates to natural persons
- Originally defined as “nominative information”
  - Directly associated with the name of the individual
- Extension of its scope to “indirectly nominative” information
  - Registration numbers, phone numbers, etc.
- Extension to “data with personal character” (“personal data”, for short)
  - All that is, directly or indirectly, attached to natural persons
    - Biometrics, behavioral traces (meta-data), etc.

Personal data (2)

- No uniform right on data
  - The legal categories depend on the types of data involved:
    - Works of the mind
    - Commercial data
    - Secrets
    - Personal data
    - Etc.
- No property on data
  - Immaterial, non-rival, goods
  - Data cannot be “stolen”
    - Various incriminations for unlawful copying

Personal data (3)

- Two legal conceptions of personal data compete at the world level
  - In Europe, personal data are attached to the person and their control is inalienable
    - Central role of consent in GDPR and e-Privacy regulations
  - In the United States, data is considered as a good whose control is said to be transferable
    - “Proprietary” vision
    - No data protection law
      - Regulation by the FCC, on economic ground
    - Example of the resale of navigation data by ISPs

Missions of DPAs

- Authorization
  - Prior audit of data processing projects
  - Development of doctrines relating to different types of processing
  - Development of simplified standards and unique authorizations
- Checking
  - E.g.: CNIL can perform online checks since 2014
- Sanction
  - Administrative court specialized in personal data
- Advising

Compliance criteria

- Lawfulness
  - Purpose
    - Precise, explicit, legitimate
  - Categories of data
- Data controller
- Recipient of processed data
- Retention period
- Security measures
- Exercise of data subjects' rights
  - Information, rectification, opposition, etc.

Lawfulness

- Conditions for lawfulness:
  - Consent
  - Performance of a contract (or prior steps with consent)
  - Compliance with a legal obligation of the controller
  - Protect vital interest of the data subject or other
  - Task carried out in the public interest
  - Legitimate interest of the controller (except when opposing to above)

Sensitive data (1)

- General prohibition of the processing of "sensitive data"
  - "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" (Art. 9.1 GDPR)

Sensitive data (2)

- Exceptions to this general interdiction
  - “Paragraph 1 shall not apply if one of the following applies:” (Art. 9.2 GDPR)
- Exclusive list of legitimate purposes:
  - Explicit consent of the person
  - Protecting the vital interest of the person when s/he is not able to provide consent
  - Health matters (medical diagnosis, public health)
  - Etc.

Data subjects rights

- Information about data subject's rights and ways to exercise them
- Opposition
- Restriction
- Access
- Rectification and erasure (right to oblivion)
- Portability of data
- Automated individual decision-making

The GDPR

- Main provisions of the GDPR:
  - Harmonized framework at EU level
    - European Data Protection Board (EDPB)
    - Extra-territorial application
  - Change from an authorization regime to a repressive regime (ex-post controls)
  - Reinforced consent
  - Automated processing for individual decisions
  - Right to portability of personal data
  - Promotion of privacy by design
  - Notification of DPAs in case of leaks
  - Data protection officer

Right to oblivion

- Based on the rights of correction and opposition recognized to the data subjects
- Right to request dereference in search engines
  - “Costeja” judgment of the CJEU of 13 May 2014
  - Deleting the link between the person's name and the indexed resources
  - “Inappropriate” link because information has become inaccurate
    - Conflicts with the right of information of the public
    - Need to implement mechanisms to reach balance

Anonymization and re-identification (1)

- Data anonymization is a critical topic in the digital age
  - Feeding of Big Data algorithms
  - "*Open data*"
  - Respect for the privacy of citizens
    - Need not to be able to re-identify
- Difference between pseudonymization and anonymization
  - Peudonymized data are still personal data
  - Anonymized data fall out of data protection laws

Anonymization and re-identification (2)

- Reidentification is an old problem
  - French law of 7 June 1951 “On Obligation, Coordination and Secrecy in Statistics”
  - Creation of the “Committee on Statistical Secret”
    - E.g., use of “binning” techniques
- Recent experiments on the re-identification of masses of data by correlation
  - Only four measure points needed!
  - Significant dilution does not significantly increase the number of measurement points required

Privacy by design (1)

- Taking into account the protection of personal data and privacy from the early design stages of the systems and devices
- Additional comfort for controllers as to their compliance with data protection laws

Privacy by design (2)

- Seven principles
  - Proactive instead of reactive measures
  - Implicit protection of privacy
  - Protection from the design of systems and practices
  - Integral functionality with positive, not zero, sum
  - End-to-end security throughout data retention
  - Guarantee of visibility and transparency
  - Respect of the users

The case of biometric data (1)

- Biometric data are extremely sensitive
  - Not revocable because intimately associated with the persons
- Two main uses:
  - Authentication: being able to ensure that a person is the right one
  - Identification: finding a person in a database from her/his tracks

The case of biometric data (2)

- Issue of device architecture
  - Centralized architectures allow both
  - Decentralized architectures only allow for authentication
- Issue of the extension of the purposes of the files
  - “Judicial requisitions” in ID biometric files
  - “Parental search” in genetic police files

Biometry war

- Offensive actions of some states to collect biometric data stocks for the entire world population
  - Backdoors in biometric collection tools of allied intelligence services (CIA/ExpressLane)
  - Massive collection of documents from the Internet (NSA/PRISM et NSA/MUSCULAR)
    - Allowed the identification of “Satoshi Nakamoto” by stylometry (biometrics of the writing style)
  - “Donations” to some States of biometric border control equipment

From interoperability to portability (1)

- The search for interoperability is a difficult process to implement
  - Delays and technical skills required
  - High cost borne by the new entrant
  - Possible malicious behavior of the author of the initial software
- It is economically more relevant to base the obligation to export the data on the author of the original software
  - Intrinsic knowledge of the data format

From interoperability to portability (2)

- Creation of a right to data portability
- Two sources:
  - Article 20 of GDPR
    - Only concerns personal data
  - Article 48 of French bill “République numérique”
    - Must integrate the Consumer code
    - Also relates to non-personal data
    - Not yet in force

From interoperability to portability (3)

- Obligation on the data controller to allow the export of the data of the person
  - In a machine-readable format
    - An open format in the case of the LRN
  - Possibly directly handed over to a competitor
    - Portability of services beyond portability of mere data

From interoperability to portability (4)

- The right to portability, like that of interoperability, contributes to the implementation of the principle of "informational self-determination"
  - Defined as "the ability of the individual to decide on the communication and use of his or her personal data"
  - Proclaimed as a principle of constitutional rank in Germany in 1983
- Digital analogue of freedom of association

Automated decision-making (1)

- Former French "I&F" bill:
  - No one can be the object of a legally binding automated decision-making processing
  - A human being had to review the decision
- Article 22 of the GDPR:
  - "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"
  - Allows for purely automated decision-making except when the data subject requests not to be so

Automated decision-making (2)

- Data subjects' rights with respect to processing
  - Auditability, as administrative documents, of software used in the public sector
  - Opposed to the fact that many of the algorithms being used are kept secret by software vendors
    - They should not, at least at the abstract level
  - Right of explanation of the principles of the processing in an intelligible manner
    - Relationships with third parties
    - Should be extended to the private sector as well