



18/07/2023

Legal issues in exploiting vulnerabilities

Part 1 - Summary

- The main principles of personal data protection
 - a brief history: why data protection has become so important
 - GDPR (2016)
 - LED (2016)
- A look back at the H2020 Exfiles project (2020-2023)





1. The main principles of personal data protection



Personal data protection: a brief history



- The German (1971) and Swedish (1973) examples
- Council of Europe resolutions of 1973 and 1974
- In France: the Law of January 6, 1978 on data processing, data files and individual liberties
- Council of Europe Convention 108, January 28, 1981
- Directive 95/46/EC
- 2012 : The European Commission proposed a global reform of data protection

-----2013----- : *the snowden case*-----



- **European Regulation 2016/679 of April 27, 2016 (applicable on May 25, 2018).**
- **LED (same day)**

What is personal data processing about?

- **Art. 4 GDPR :**
- ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

That's quite broad...

L. Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

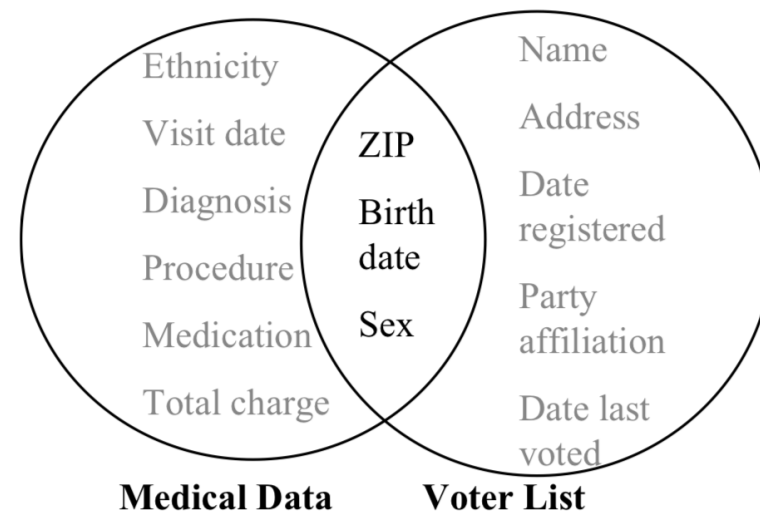


Figure 1 Linking to re-identify data

A more recent example





0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

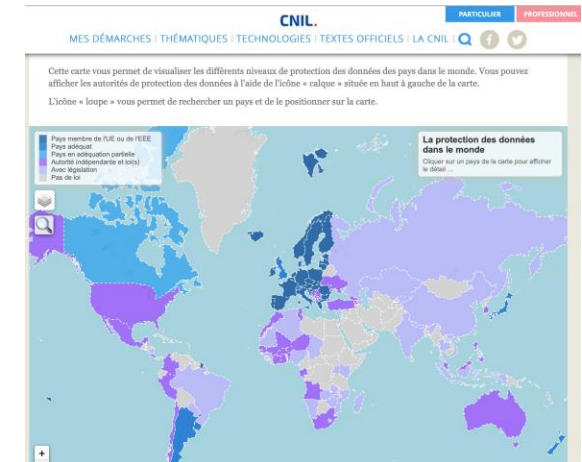
Adopted on 10 April 2014

The opinion elaborates on the robustness of each technique based on three criteria:

- (i) is it still possible to single out an individual,
- (ii) is it still possible to link records relating to an individual, and
- (iii) can information be inferred concerning an individual?

OK, so how is personal data protected according to GDPR?

- Global principles (i.e. lawfulness, fairness and transparency, purpose limitation, data minimisation, storage limitation, etc.)
- Rights of the data subject
- A legal basis (consent, legitimate interest, **processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller**, etc.)
- Privacy by design (record of processing, DPO, PIA, etc.)
- Limited transfers to third countries
- Security of processing



But behind GDPR, there is the « law enforcement directive » (LED)

- Same day (April 27th 2016). A directive, not a regulation
- Applies to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- Excerpt : (4) « The **free flow of personal data between competent authorities** for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, **should be facilitated** while ensuring a high level of protection of personal data ».
- Seems to be a copy/paste of GDPR...

Exactly the same key words are used in the definitions. We also find many of the common principles, for example in article 4:

Article 4

Principles relating to processing of personal data

1. Member States shall provide for personal data to be:
 - (a) processed lawfully and fairly;
 - (b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
 - (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
 - (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.
3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.
4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

It is ALMOST a copy / paste of art. 5 RGPD.

ALMOST : for instance the principle of transparency is missing !

Similarly, article 4 states that the data collected must **not be excessive** and must not be limited to what is necessary (RGPD), which is not exactly the same thing...

Same issue regarding the right to access :

Article 15

Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:
 - (a) avoid obstructing official or legal inquiries, investigations or procedures;
 - (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
 - (c) protect public security;
 - (d) protect national security;
 - (e) protect the rights and freedoms of others.

So that's the state of the art...but new challenges are arising

Pegasus Case: "Government Did Not Cooperate" - Supreme Court Cites Report

Pegasus Spyware Case: "We don't want to make any more comments without going through the complete report," Justice Ramana said.

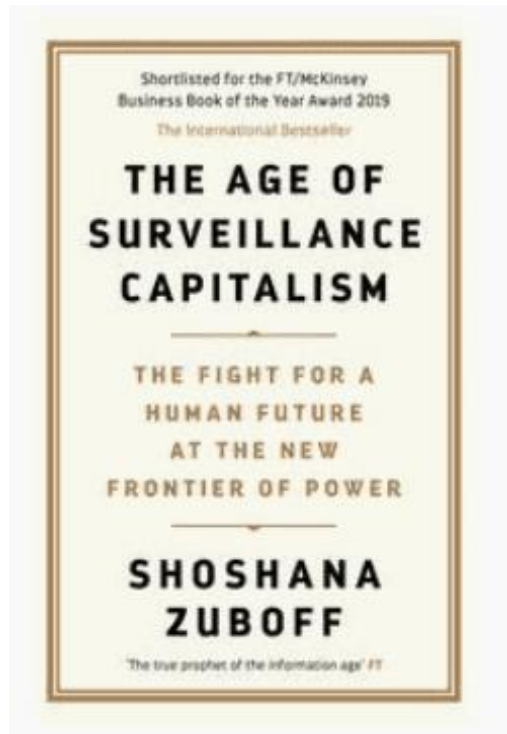
India News | Reported by Arvind Gunasekar, Edited by Akhil Kumar | Updated: August 25, 2022 1

Spotlight EncroChat Turns into a Case for the CJEU

18 November 2022 (updated 1 month, 3 weeks ago)

 **Thomas Wahl**

Published in printed  Issue 3/2022  pp 197 – 198



MIT
Technology
Review

Featured Topics Newsletters Events Podcasts

SIGN IN

SUBSCRIBE

TECH POLICY

Predictive policing is still racist—whatever data it uses

Training algorithms on crime reports from victims rather than arrest data is said to make predictive tools less biased. It doesn't look like it does.

By Will Douglas Heaven

February 5, 2021

Some reactions are already here

POLICY AND LEGISLATION | Publication 15 September 2022

Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and
2. an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.



See also



The EXFILES project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883156

2- A look back at the H2020 Exfiles project (2020-2023)





The EXFILES project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883156



The legal and ethical WP

| # | Title | Lead | Date |
|------|---|--------|---------|
| T2.1 | Fundamental support study on Encryption and Fundamental Rights | ULille | M01-M18 |
| T2.2 | Ethical framework for forensic research | RHUL | M01-M30 |
| T2.3 | Study on the use and conservation of methods by law enforcement | ULille | M18-M24 |
| T2.4 | Draft of Regulatory and Ethical Recommendation and good practices | RHUL | M24-M36 |

Some examples of fundamental rights discussed :

- Protection of personal data
- Respect for private and family life
- Respect for professional secrecy
- Proportionality (balance between fundamental rights)
- Subsidiarity (competences of the EU and the MS)
- Right not to self-incriminate
- Right to a fair trial (rights to evidence and to defence)

Main identified legal discrepancies

- Definition & provision on e-evidence
- Search and seizure regimes
- Legal framework for secrecy of correspondences
- Legal obligation to decrypt
- Legal obligation to cooperate (e.g. for service providers)
- Punishment for illegal use of data as evidence



A lot remains to be done...and this could change the very role of the EU.

18/07/2023

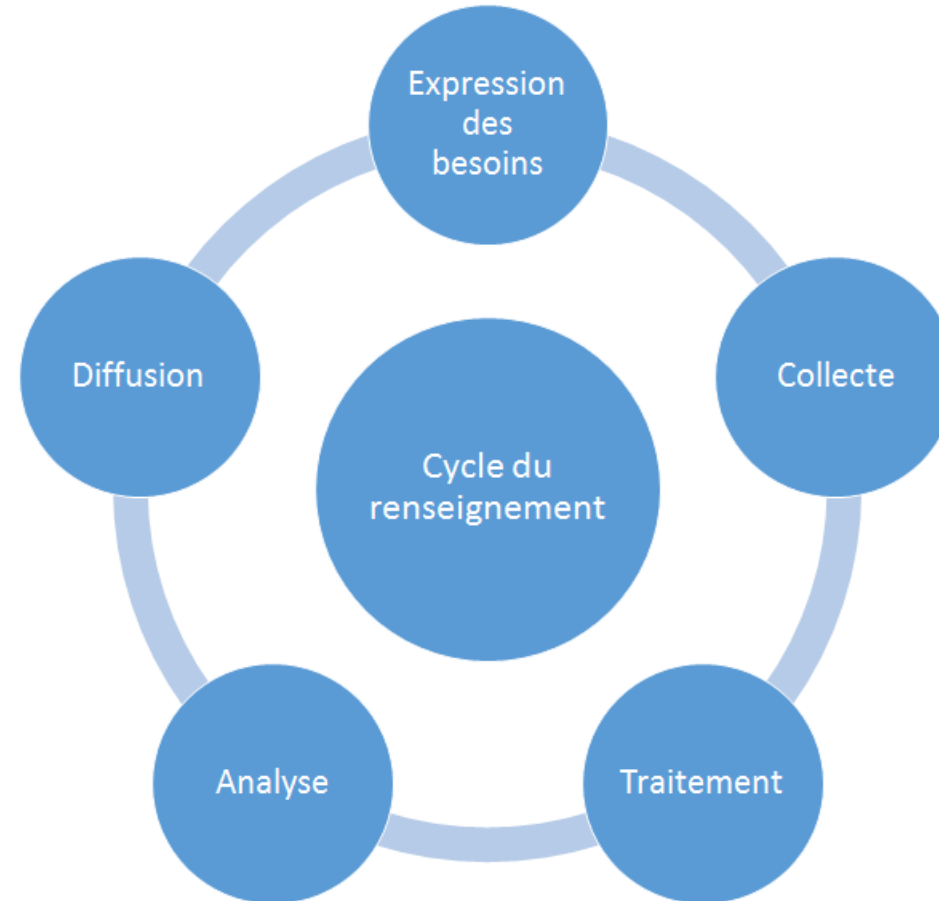
But all this applies
only in the field of
GDPR and LED.
What about
intelligence ?

I. What is intelligence?

Sherman Kent, *Strategic intelligence for American World Policy* (1949)

Intelligence is :

- **An information**
- **An activity :**
 - The research orientation
 - The information's collection
 - The information's processing
 - The analysis
 - The dissemination
- **An organisation**



The legal definition of intelligence



2015 – Intelligence Law

The home security code (CSI) : Intelligence is a public policy that contributes to "*national security strategy and the defence and promotion of the fundamental interests of the Nation*".

- Intelligence is define as an **activity**
- For more simplicity, it is preferable to adopt an **organisational view of intelligence**

There are **two main categories of intelligence service**

- Specialised intelligence services (first circle intelligence services)
- Second-circle intelligence services

-  Communauté du renseignement incluant les services spécialisés de renseignement
-  Autres services de renseignement


 **Président de la République**


 **Coordination nationale du renseignement et de la lutte contre le terrorisme (Centre national de contre-terrorisme)**

 **Premier ministre**

Inspection des services de renseignement

ACADÉMIE DU RENSEIGNEMENT

 **Ministère de la Justice**


 **SNRP**


 **Ministère des Armées**


 **DSSE**

 **DRM**

 **DRSD**

 **Ministère de l'Action et des Comptes publics**

 **DNRED**

 **TRACFIN**

 **Ministère de l'Intérieur**

 **DGSI**

 **DRM**

 **Police Nationale**

 **Centre National de Renseignement Antiterroriste**

II. What is the legal framework for intelligence?

Intelligence services contribute to the **protection of national security**. It is for this reason that they have exceptional powers.

Until recently, there was no real legal framework for intelligence services' activities

- Several **condemnation** by the European Court of Human's rights in 1991
- Since then, France **have gradually adopted a legal framework**
 - Only **certain aspects** (access to files, security interceptions, or connection data's requisition)
 - Ex. **law of 10 July 1991**, which established the first legal framework for interception of communication

Intelligence Law of 24 July 2015

- provides a framework for Intelligence services activities
- Strengthens their powers and resources

➔ Not all intelligence activities, **only digital aspects !**

The intelligence services are now authorised to :

- collect **connection data**
- set up beacon systems to **remotely locate car or mobile telephone**
- monitor digital networks **using automated data processing** (algorithms)
- intercept connection data and conversations using **IMSI-catchers**
- **intercept communications** by any means of transmission (wired, wireless or satellite)
- capture images and conversations in a private place
- penetrate **computer systems** and **retrieve data** contained in these systems

1. Data likely to be collected

- **Communications:**

- All kind of communications
- Difficulties in accessing these communication
 - **Encrypted channels** (very sophisticated encryption tools/refuses to cooperate with intelligence services)
 - Services refuses to reveal their targets

- **Connection data:**

- Date generated automatically during a communication of any kind.
- Date **extremely valuable** to the intelligence services, more than the content of communications
- connection data allows *"very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them"*

- **Computer data:**

- Intelligence services can collect **new data**: sounds, images, but also computer data
- The law of October 2017 : it's now possible to collect computer data circulating on WIFI or stored in connected objects
- a **draft law** proposed to create a procedure enabling judges to authorise law enforcement agencies to **remotely activate an electronic devices**, its **camera** and **microphone** to geolocate or eavesdrop on people in certain investigations

2. Ways of collecting personal data

- **IMSI-catcher**

- Fake relay antenna
- Possibility to collect connection data **and** communications
- Difficulties with 5G

- **Algorithms**

- Analysis of **all the metadata** circulating on electronic communications networks, based on **predetermined parameters**
- Identification of « **weak signals** », i.e. *"trends or traces that may be unreadable or undetectable in isolation, but which, when related to a group of people, highlight occurrences that reveal certain behaviour patterns"*.

Safeguards :

- Only for **fight against terrorism**
- Used by services in the **first circle**
- Only **connection data**
- A **procedure** must be followed

The **major innovations** since the law of 2021

- Algorithms are now **permanents**
- They can collect **URLs**
- The date **retention period** had been increase

III. What are the issues surrounding the exploitation of vulnerabilities?

- **absence of a legal framework** specifically dedicated to the issue of vulnerability exploitation
 - a fundamental **distinction** must be made between
 - intelligence techniques
 - the technical means used to capture or intercept the data
 - Only **certain means** are identified in the law (*algorithms, IMSI catchers*)
 - The law is **dependant** on technical developments

What are the issues on the REV project ?

- It is necessary to establish a **specific framework** for the use of vulnerability exploitation as an investigative technique?
- How can we ensure that the **evidence** is fair, but also that it can be explained?
- How ton apply the new **European acts**