CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Regulating AI
The perspective of the French CNIL

Félicien Vallet

IRDT Conference – Regulating AI

8 July 2021

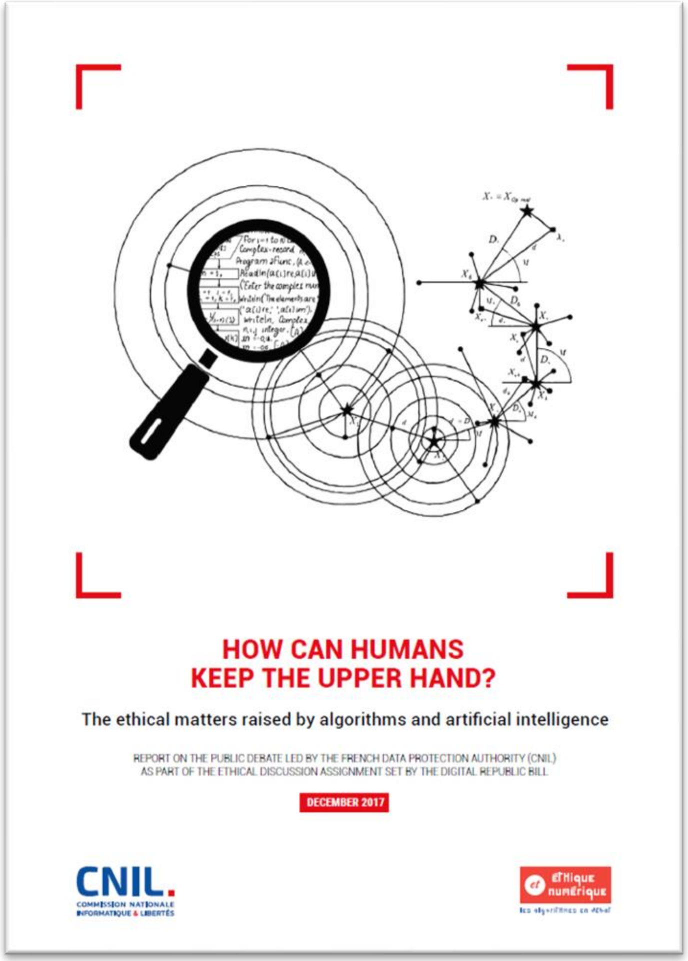
CNIL.

AI, A COMPLEX SUBJECT FOR THE CNIL

Between Top-Down…
and Bottom-Up approaches!

- The CNIL's ethical report (December 2017)
  - A large public debate
    - 3000 people
    - 60 associated events
    - 45 partners (universities, syndicates, professional federations, administrations)
  - Two pilars :
    - Fairness
    - Continued attention and vigilance
  - Six recommandations
  - One among the **many** « ethic of AI » reports
- But for it's everyday regulating job, the CNIL has a deal with **very practical questions**

  → **Puts the GDPR principles in tension!**



HOW CAN HUMANS
KEEP THE UPPER HAND?

The ethical matters raised by algorithms and artificial intelligence

REPORT ON THE PUBLIC DEBATE LED BY THE FRENCH DATA PROTECTION AUTHORITY (CNIL)
AS PART OF THE ETHICAL DISCUSSION ASSIGNMENT SET BY THE DIGITAL REPUBLIC BILL

DECEMBER 2017

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

éthique numérique
les algorithmes en débat

Concrete issue n°1

- **Project DATAJUST :** request submitted to the CNIL concerning the implementation by the French Ministry of Justice of an algorithm responsible for identifying the amounts awarded in compensation for victims' personal injury and with which guidelines for professionals and the general public will be produced.

  - How can we ensure the absence of potentially harmful biases?
  - What measures and practices should be recommended to eliminate or at least reduce this risk?

Concrete issue n°2

- **Startup X1 :** Following a processing audit procedure, the CNIL found out that personal data had been illegally collected and used to train an AI model.
  - What is the legal status of this object?
  - If the deletion of the data can be required, should the AI model also be deleted or not?

Concrete issue n°3

- **Startup X2 :** This company is marketing a tool implementing machine learning methods for the coding of medical procedures ("PMSI coding") in a hospital center Y1.

  - What is the legal status of this object (personal/anonymous data)?
  - Can the startup transfer the model learned in hospital center Y1 to hospital center Y2 and adapt it there?
  - If possible, what measures and practices should be recommended to minimize the risks?

Concrete issue n°4

- **Pharmaceutical laboratory X3:** request for authorization to conduct an observational study on prostate cancer using electronic medical records.
- For this purpose, the processing of the entire active file of patients received in the tested centers, **affected AND non-affected patients** is asked to collect a large number of **"true negatives"** (> 100 million medical records including those of female persons)

  - Refusal of the CNIL for non-compliance with the principle of minimization.
  - Where to place the cursor?

Concrete issue n°5

- **Startup X4:** Request for advice on an automated store theft detection solution. The solution provider would like to access the video surveillance data of its customer to train its system and adapt it.

  - Is it possible to constitute datasets of learning data from video surveillance cameras?
  - With what safeguards?
  - What methods should be used to "anonymize“/”de-identifiy” video data (blurring, masking of the background, colorimetric post-processing, use of GANs for face substitution)?

CNIL.

THE EDPB/EDPS JOINT OPINION

Timeline

- **21 April :** publication of the proposal for a Regulation by the European Commission (EC)
- **~23 April :** request of a joint EDPB-EDPS opinion
  - Deadline 18 June (8 weeks)
- **01 May – 10 June :** Work by the Technology Expert Subgroup (taskforce of 6 DPAs)
- **18 June :** adoption in plenary session
  - Representants of :
    - 27 EU countries
    - EDPS
    - 3 EFTA EEA States (IS, LI, NO)
  - **Opinion:** https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

edpb
European Data Protection Board

EDPS

EDPB-EDPS

Joint Opinion 5/2021

on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)

18 June 2021

Focus on 4 fundamental points

- The need to draw red lines for future AI uses
- The challenge of the articulation with the GDPR
- The importance of establishing harmonized governance
- The essential support for innovation

1. The need to draw red lines for future AI uses

- Willingness of the EC to clarify prohibited uses in order to build ethical and trusted AI in the EU

- However, **need to broaden the scope** of prohibited AI systems and clarify their definition
  - Prohibited uses are unclear ("real-time", "significant delay")
  - Intrusiveness does not necessarily depend on the purpose ("private" vs "public" security)
  - Exceptions to the prohibition are too vague ("prevention of a threat to the life or physical safety of natural persons"

- **Call for a general ban** on any use of AI for automated recognition of human features in publicly accessible space (face recognition, gait, fingerprints, voice, and other biometric or behavioural signals)

1. The need to draw red lines for future AI uses

- Also, call for the prohibition of:
  - **Biometric systems used to classify individuals** into groups (based on alleged ethnicity, gender, political or sexual orientation, etc.)
  - **AI systems that infer person’s emotions** (except in very specific cases, such as certain health purposes)
  - **All forms of “social scoring”**

- The clarification of the framework, specifying what is permitted and what is prohibited would benefit to **citizens but also professionals**
  - No differences in interpretation depending on the sector or the Member State

- In the case of the CNIL, it is to be put into perspective with several public statements over the last few years :
  - Call for a democratic debate on new video uses (September 2018)
  - Facial recognition: for a debate living up to the challenges (December 2019)
  - Call for vigilance on the use of so-called "smart" cameras and thermal cameras in the context of the COVID-19 epidemic (June 2020)

2. The challenge of the articulation with the GDPR

- Welcome the **risk-based approach** adopted by the EC
- Focus on a limited volume of AI systems said to be "high risk" for fundamental rights
  - ~10% of the totality of AI systems (source DG CNECT)
- In an **overwhelming majority of cases**, high risk AI systems will process personal data
  - **major issue of articulation** with the GDPR and the Law Enforcement Directive
- Classification of an AI system as high risk **does not mean its use is authorized**
  - An AI system could be a CE marked product and not satisfy GDPR
  - **Compliance with the legal obligations must be a precondition** for entry into the European market
- Need for a **systematic third party certification** of high risk AI systems

3. The importance of establishing harmonized governance

- Need to **clarify the governance** of the "European Artificial Intelligence Board" (EAIB)
  - Guarantee its **independence** and **autonomy**
    - Today, a predominant role of the EC
  - **Strengthen** its powers and allow it to exercise **real control**
    - Particularly when for AI systems deployed at the European scale
    - Possibility to propose amendments to Annexes I and III
  - Propose real **cooperation mechanisms**
    - Single point of contact for individuals and companies
    - Designation of the national authority by the EAIB for organisations whose activities cover more than half of the Member States of the EU

3. The importance of establishing harmonized governance

- Data Protection Authorities (DPAs) should be **designated national supervisory authorities** since:
  - DPAs **already regulate AI systems** involving personal data and exchange with solution providers (and will carry on doing so!)
  - DPAs are **competent and experienced regulators**
  - There is a need to provide a **coherent framework** and a clearly **identified interlocutor** for professionals
  - The EC gives **the EDPS the power of competent authority** for AI systems implemented by the European institutions, bodies and agencies
- Of course, acting as national supervisory authorities would require **substantial financial and human resources**

4. The essential support for innovation

- Innovation and design of AI systems in line with European values and principles **is to be encouraged**

- Necessity to combine protection requirements with an advanced understanding of the technological challenges in order to **propose a balanced view of regulation**

- National competent authorities must implement support measures and **in particular "regulatory sandboxes"**
  - Concerns on the reuse of data to allow further processing based on the public interest
  - Question of the responsibility between the national competent authority and the data controller

- In France, **the CNIL already supports innovation** through various actions such as:
  - Thematic workshops and webinars
  - The "personal data sandbox" initiative (February 2021)
  - The CNIL's digital innovation lab (LINC)

CNIL.

THANK YOU FOR YOUR ATTENTION