NADI
Namur Digital Institute

AI and Data Protection: some issues.

Council of Europe – Seminar for African DPA – 5th of November 2020

Yves Poullet, Professor Universities of Namur and Lille (UClille), Member of the Royal Academy of Belgium and of the Belgian DAP, co-chaiman of the Namur Digital Institute (NADI)

The « red wire »

- From the technology to its success
- Some risks linked with AI applications
- Issues and Data Protection solutions: Convention 108+ facing AI.

AI – the context

The AI phenomenon - A definition;

'artificial intelligence' means a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals.

1. Embedded in hardware devices (sometimes humanoids) – the robots (smart speakers, automated car, chatbots,…)
2. Collecting and processing data: two complementary technologies:
    - The nano phenomenon – the digital ubiquity: Internet of Things (e.g. the RFID, the 'self quantified', the body's implants) 4800 connections each day in 2025
    - The *big data* »: in 30 years, from a capacity of kilo (1000) operations /sec.) to Tera (1000 billions of operations/sec.) - The Moore, Kryder and Nielsen Law: towards an infinite capacity of storage of processing and transmission
3. Simulating human intelligence: from causation (If… then) to pure statistical not necessarily explainable aggregation – the possibility to decide and to predict.
4. With a certain degree of autonomy: From supervised system to non supervised system - From « *machine learning* » to '*deep learning*' – the relative opacity of the AI systems

AI and its applications

- AI and its triple virtue for our Governments, administration, companies AND citizens (e.g. SPOTIFY) – about three paradigmatic examples.
  - Public Security: Use of facial recognition systems by LEA; prediction of burglaries; …
  - Companies' marketing Optimisation – Profiling « *Know your customer* » - « *it will become very difficult for people to see or consume something that has not in some sense been tailored for them.* » (Google CEO) – adaptative pricing – nudges - …
  - Recruiting people – « Objectivitation » of the decision : '*Data do not lie*' – affective computing

The risks linked to the AI applications

- As regards the functioning of AI systems:
  - Reductionism and decontextualisation
  - Errors and biases in programming
  - Opaque functioning
  - Evolutive systems
- As regards the AI applications
  - The continuous spying and global surveillance
  - The ability to predict (the risks of manipulation (the *nudges and the* stigmatisation)).
  - The discrimination: adaptative pricing and exclusion phenomenon
  - The increasing sensitivity of the applications (Health, public security, education, …)
  - The individuals'normalization : the anticipatory conformism.
- As regards the AI actors :
  - The number of actors involved in the building up of a AI system
  - The still increasing desequilibrium of informational powers between certain DC and DS (the GAFAM)

Risks’typology – a first attempt

- As regards ethical values like dignity, autonomy and social Justice
- As regards the dimension of the risks:
  - Risks to the individual
  - Collective risks: the emerging notion of ‘group privacy’ – the risks to the democracy (*Cambridge Analytica*) or to social and legal rules (one-to-one insurance and AI) –

Warning : DP legislation and DPA are in principle not competent to face the collective challenges caused by AI. Need for an enlargment of their competences.

The DP legislations facing the AI challenges – some uncertainties…

Definitions:

- Art. 2 a - The notion of personal data (vs. anonymous data) still available – e.g. the data generated by an autonomous car?
- Art. 6. - The notion of sensitive data- from a definition by nature to a definition by the end-purpose of the processing (e.g. the Cambridge Analytica Case) – the need to include biometric and genetic data.
- The numerous actors in the supply-chain of an AI system:

  1. Beyond Data Controllers and Data Processors ? –

  2. The recent guidelines of the EDPB towards a joint liability between platforms and companies using their services.

The DP legislations facing the AI challenges – some uncertainties…

The D.P. principles (art. 5):

- Need for definite and limited end-purposes (Art. 5.1.) ?
- Data minimization and proportionate duration in contradiction with the AI essence (art. 5.4. c) ?
- Consent (Art. 5.2.) – from panacea to the '*privacy bug*' – The need to have choices between different levels of profiling (e.g. Spotify)
- Loyalty and transparency Principles (Art. 5.4 a)) and the need to reinforce the information to be given to the D.S. (e.g. in case of profiling: the categories of data, their origin, the processing model used, the impact of the decision or draft decision, the beneficiairies, …
- The Security Principle (Art. 7): fear of hackers and bias.

The DP legislations facing the AI challenges – some uncertainties …

- The principle of non submission to a decision taken solely (?) on the basis of an automated system with 'significant' impact to the DS (art. 9.1.a)): the need for explainability and the right to have recourse before a person competent to modify the decision.
- The '*privacy by design*' principle. (art. 10. 2 et 3)
- The obligation to proceed to a '*Privacy Risk Assesment*' (art. 10.2), especially in case of high risk systems (art. 10.4). The problem of the AI systems auditability. Towards an external, continuous, multistakeholders and multidisciplinary systematic assessment?

NADI
Namur Digital Institute

- Questions ?????
- Thanks for your attention and if you want to pursue the dialog… do not hesitate,

Yves.poullet@unamur.be