Déjeuner-conférence
Société Européenne des Ingénieurs et Industriels
17 juin 2022

Intelligence artificielle et protection de la vie privée : pour une réconciliation du droit et de l'ingénierie

Thierry Léonard
Professeur Université St Louis-Bruxelles
thierry.leonard@usaintlouis.be

Bruno Schröder
Technologue en retraite. Ir 82
bruno_schroder@hotmail.com
Bruno Schroder | LinkedIn

CePri
Centre de droit privé

Pourquoi nous?

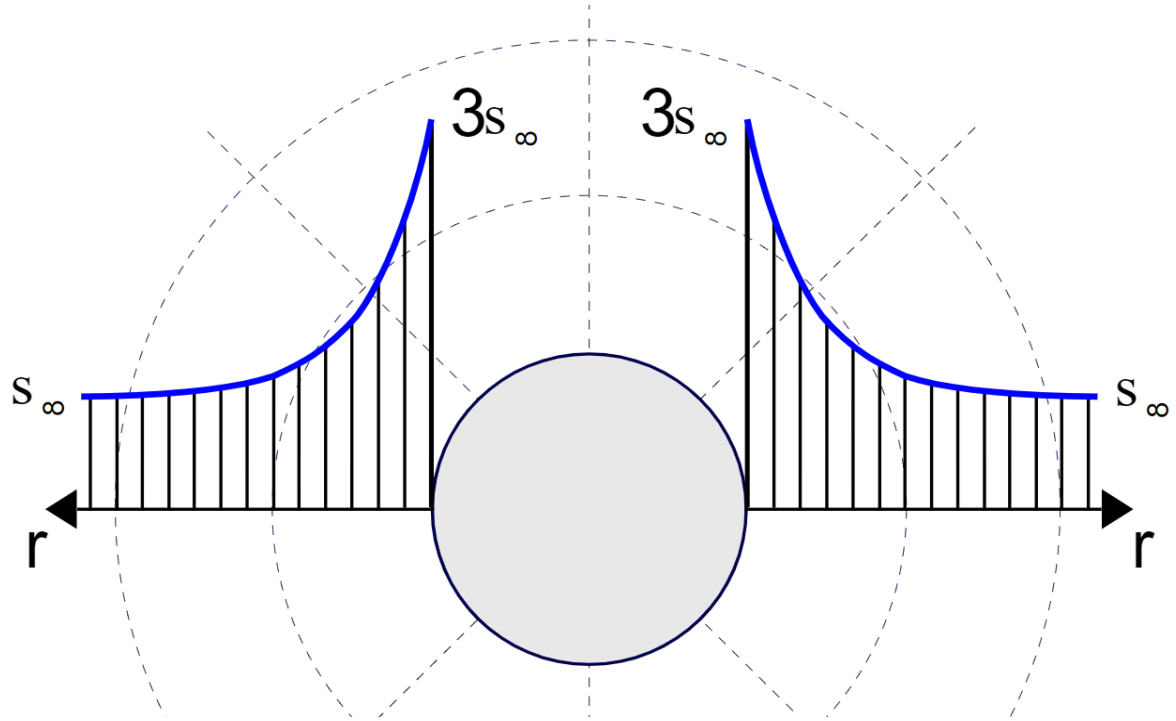
- Plusieurs rencontres en tant qu'orateurs dans des conférences et colloques sur l'IA et la protection des données personnelles
- Une expérience pratique de l'application de la règle à la technologie générant de nombreux « pourquoi ? »
- Une conviction partagée de notre incapacité à traiter le problème avec les seuls outils de notre domaine d'expertise

QUI “CONSTRUIT” LES ÉLÉMENTS OPÉRABLES DE NOTRE SOCIÉTÉ ?

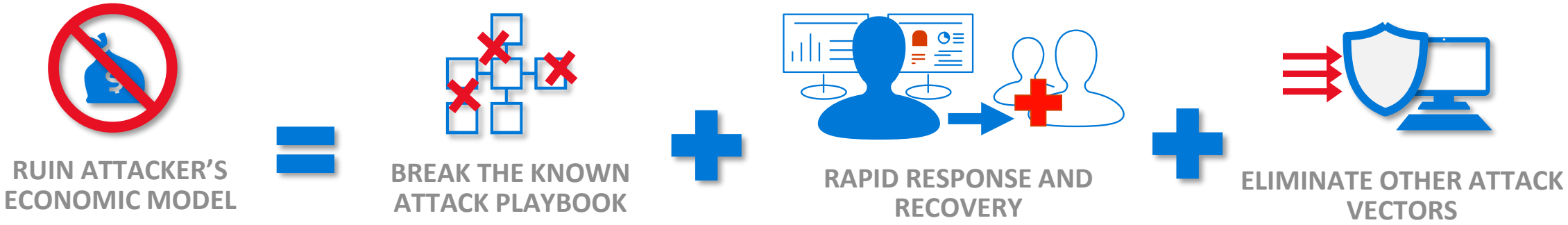
JURISTES ET INGÉNIEURS,
AUX RÔLES ET OUTILS TRÈS DIFFÉRENTS

ET LE POLITIQUE EN GUIDE SOCIÉTAL

LE TRAITEMENT DES TROUS



Stratégie de compensation



Transformer la difficulté de la défense en problématique d'attaque

Stratégie d'éradication

COUNCIL OF EUROPE

COMMITTEE OF MINISTERS

RESOLUTION (73) 22

ON THE PROTECTION OF THE PRIVACY OF INDIVIDUALS VIS-A-VIS ELECTRONIC DATA BANKS IN THE PRIVATE SECTOR

(Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies)

REALITY IS FREQUENTLY INACCURATE

Douglas Adams (1952 – 2001)

Francis Fukuyama: How to Save Democracy From Technology | Foreign Affairs

The political harms posed by the platforms are more serious than the economic ones

Big Tech poses unique threats to a well-functioning democracy

Opinion | Facebook and the Surveillance Society: The Other Coup - The New York Times

Data: une coexistence difficile

- Des approches divergentes:
  - Technologie: plus de données pour plus de traitements
  - Protection: minimisation des données et traitements limités
- Les fondamentaux de la protection des données ignorent l'évolution technologique
  - Les principes de 1973 and 1981sont toujours au cœur du RGPD
  - Les concepts de base de l'IA, comme le phasage de sa construction, sont ignorés
  - Le contrôle porte sur la collecte des données plutôt que sur l'abus des corrélations
- Les principes actuels sont inefficaces face à l'évolution géo-technologique
  - Modeling as a service (modélisation automatique)
  - Darwinisme régulatoire induit par le compétition géo-économique

Evolution législative de la protection des données personnelles

COUNCIL OF EUROPE

COMMITTEE OF MINISTERS

RESOLUTION (73) 22

ON THE PROTECTION OF THE PRIVACY OF INDIVIDUALS VIS-A-VIS ELECTRONIC DATA BANKS IN THE PRIVATE SECTOR

(Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies)

ANNEX

The following principles apply to personal information stored in electronic data banks in the private sector.

For the purposes of this resolution, the term "personal information" means information relating to individuals (physical persons), and the term "electronic data bank" means any electronic data processing system which is used to handle personal information and to disseminate such information.

1.

The information stored should be accurate and should be kept up to date.

In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2.

The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3.

The information should not be obtained by fraudulent or unfair means.

4.

Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

5.

Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6.

As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7.

Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

8.

Precautions should be taken against any abuse or misuse of information.

Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirections of information, whether intentional or not.

9.

Access to the information stored should be confined to persons who have a valid reason to know it.

The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10.

Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.

— 74 —

Evolution législative de la protection des données personnelles

- Principes de base de la protection analogues depuis 1973 : RGPD/GDPR : dernière évolution d'une approche identique depuis 50 ans.

- Protection centrée sur l'individu dans ses rapports avec une organisation déterminée → il doit conserver le contrôle de "ses" données (transparence du traitement et droits de correction)

Evolution législative (suite)

- Résolution du Conseil de l'Europe (1973) → Convention du Conseil de l'Europe (1981) → Directives de l'UE (1995 et 1999) → Règlement RGPD/GDPR (2016)

- Construction du marché unique de la donnée (2020) : libération de la donnée pour permettre le développement de l'IA européenne (x USA et Chine) MAIS dans le respect des libertés individuelles

Des problèmes fondamentaux non techniques

- Alors que la loi est basée sur l'individu et le recours individuel, comment introduire le sens du groupe?
- Comment analyser et prévenir le risque pour la démocratie?

- **Francis Fukuyama: How to Save Democracy From Technology | Foreign Affairs**
- *The political harms posed by the platforms are more serious than the economic ones*
- *Big Tech poses unique threats to a well-functioning democracy*
- **Opinion | Facebook and the Surveillance Society: The Other Coup - The New York Times**

COMMENT ABORDER LA COMPLEXITÉ MULTIDISCIPLINAIRE ?

1970: James Martin: “The computerized society”

1973: Council of Europe: “Protection of Privacy of Individuals vis a vis Electronic Data Bases in Private Sector” Resolution 73 (22) → access rights, purpose limitation, erasure of obsolete data, anonymization

1994: Philip Agre: https://pages.gseis.ucla.edu/faculty/agre/ → mass data collection and privacy, AI and ethics

1997: Carl Sagan: “The Demon-Haunted World: Science as a Candle in the Dark”

> “*I have a foreboding of an America in my children's or grandchildren's time … when awesome technological powers are in the hands of a very few*, and *no one representing the public interest can even grasp the issues*; … *unable to distinguish between what feels good and what's true, we slide, almost without noticing, back into superstition and darkness…* “

EXEMPLE:

PRIVACY BY DESIGN (ART 25 RGPD)

1. COMPTE TENU DE L'ÉTAT DES CONNAISSANCES, DES COÛTS DE MISE EN ŒUVRE ET DE LA NATURE, DE LA PORTÉE, DU CONTEXTE ET DES FINALITÉS DU TRAITEMENT AINSI QUE DES RISQUES, DONT LE DEGRÉ DE PROBABILITÉ ET DE GRAVITÉ VARIE, QUE PRÉSENTE LE TRAITEMENT POUR LES DROITS ET LIBERTÉS DES PERSONNES PHYSIQUES, LE RESPONSABLE DU TRAITEMENT MET EN ŒUVRE, TANT AU MOMENT DE LA DÉTERMINATION DES MOYENS DU TRAITEMENT QU'AU MOMENT DU TRAITEMENT LUI-MÊME, DES MESURES TECHNIQUES ET ORGANISATIONNELLES APPROPRIÉES, TELLES QUE LA PSEUDONYMISATION, QUI SONT DESTINÉES À METTRE EN ŒUVRE LES PRINCIPES RELATIFS À LA PROTECTION DES DONNÉES, PAR EXEMPLE LA MINIMISATION DES DONNÉES, DE FAÇON EFFECTIVE ET À ASSORTIR LE TRAITEMENT DES GARANTIES NÉCESSAIRES AFIN DE RÉPONDRE AUX EXIGENCES DU PRÉSENT RÈGLEMENT ET DE PROTÉGER LES DROITS DE LA PERSONNE CONCERNÉE.

Quand la règle de loi doit être intégrée dans la technologie, ni le juriste ni l'ingénieur ne peuvent seuls en valider l'implémentation.

Question of methods

(1) Confrontation des principes de protection des données à la réalité de l'élaboration d'une IA

- l**e pourquoi de la règle, le comment de la technologie**

(2) Au travers des trois étapes du processus de vie de l'IA :

- **la collecte des données** : transparente et limitée selon la nature des données dans le système actuel → transparence moindre (ou différente) et limitée selon les finalités d'utilisation d'exploitation

- l'**analyse et l'élaboration des algorithmes** : aucune protection actuelle → protection à l'égard des processus d'auto-apprentissage, du non respect des finalités exclues, de la loyauté de l'utilisation de modèles, pertinence des corrélations à l'égard des finalités etc.

- **exploitation de l'IA : protection des données à caractère personnel complète, nouvelle protection des personnes concernées par l'algorithme** → risques de discrimination et de non adéquation de l' application à la personne + risques sociétaux

Questions of methods

Les principes revisités sont :

1) Donnée (plus seulement la donnée personnelle)
2) Principe de finalité
3) Principe de transparence
4) Données sensibles (qui deviennent des finalités sensibles)
5) Droits individuels (+ droits collectifs)
6) Sécurité et confidentialité
7) Flux transfrontières de données
8) Institutions de contrôle

Un exemple: le principe de transparence

	Phase 1: Collecte	Phase 2: Analyse/Modélisation	Phase 3: Utilisation/exploitation
4. Transparence	(1) Système centralisé d'identification/tracking des AI (BDIA) (concepteur + type de données + finalité générique+ description du processus d'élaboration de l'algorithme ; data sheets) (fourniture de la clé de pseudonymisation); (2) balance entre informations publique/techniques non confidentielles + informations confidentielles/techniques uniquement accessible aux autorités (secret des affaires ; IP…) (3) information standard et simple pour la personne (4) Information par le Responsable de traitement initial de l'identification des AI qui collectent des données au départ de ses traitements	Documentation sur le processus d'analyse et de mise au point de l'algorithme ainsi que sur ses finalités potentielles non exclues (nlles corrélations) + conservation des corrélations assumées comme pertinentes màj de l'enregistrement auprès de l'autorité si modifications ; (accessible aux autorités de régulation et de protection ; pas aux personnes durant la conception) ; Documentation quant aux mesures de sécurité et d'accès	(1) Information de l'identifiant IA utilisé et de la possibilité d'accès à la documentation du processus d'analyse par l'utilisateur de l'IA ; (2) information et doc sur la pertinence de l'utilisation du modèle IA dans son utilisation spécifique (3) information quant au degré d'incertitude (Inadéquation) du modèle quant à la personne concernée (4) information RGPD

Notre matrice analytique

- L’ingénieur définit les colonnes
- Le juriste définit les lignes
- Explication/réflexion/proposition cellule par cellule
- Comment compenser/améliorer la protection ?

EN GUISE DE CONCLUSION

En guise de conclusion

- Le processus autant que le résultat
- Une dialectique indispensable en amont de la création des règles

→ Notre discussion remet la règle en question et force à modifier les fondements de la protection qu'elle est censée mettre en œuvre

→ Elle permet seule d'éviter le blocage et l'incompréhension dans la collaboration au moment de la création et l'utilisation de la technologie

MERCI POUR VOTRE ATTENTION

Q&A