

Questions de propriété sur les données et modèles d'apprentissage

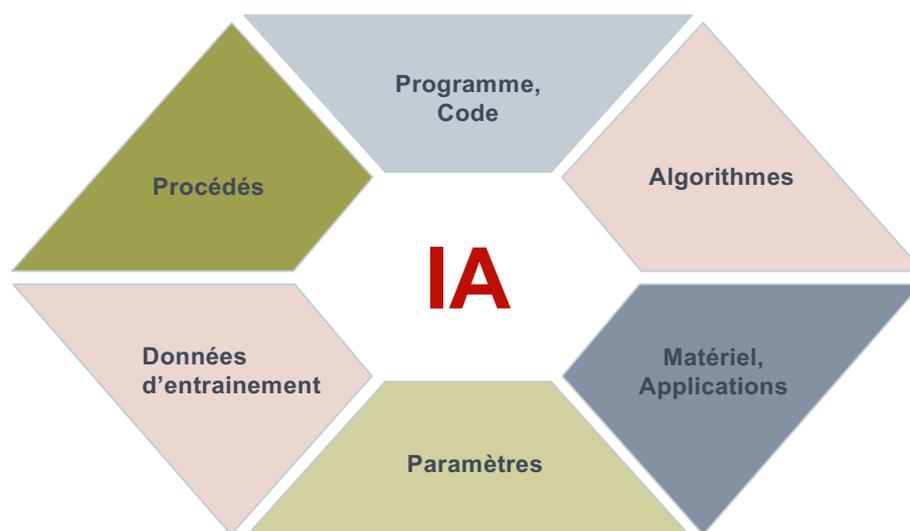
La protection des applications de l'IA par la propriété intellectuelle

Jean-Marc Deltorn

Centre d'Études Internationales de la Propriété Intellectuelle (CEIPI)

jm.deltorn@ceipi.edu

IA : un objet (technique) multifacette



Comment protéger?



Droit d'auteur – programmes - Directive 2009/24/EC

- Les pays de l'UE sont tenus d'accorder la protection du **droit d'auteur aux programmes d'ordinateur**.
- Les programmes devraient être protégés **en tant qu'œuvres littéraires au sens de la convention de Berne** pour la protection des œuvres littéraires et artistiques.
- **La protection prévue par la directive s'applique :**
 - à un programme d'ordinateur qui est original, en ce sens qu'il est la **création intellectuelle propre à son auteur**
 - à toute forme d'**expression** d'un programme d'ordinateur

Droit d'auteur – programmes - Directive 2009/24/EC

Art. 1(2) : La protection prévue par la présente directive s'applique à **toute** forme d'expression d'un programme d'ordinateur.

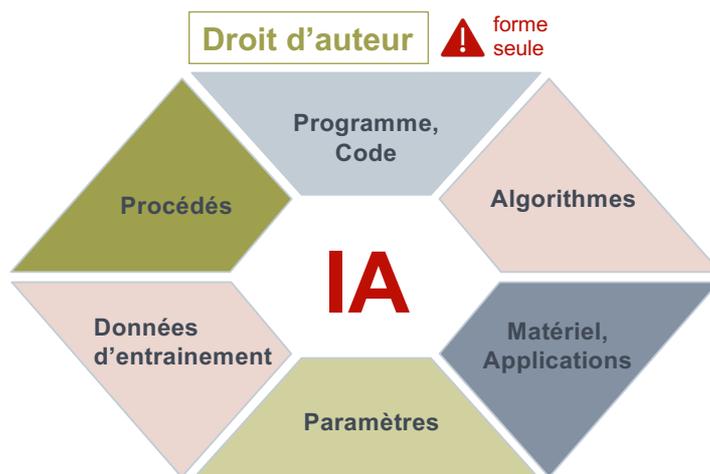
« **Les idées et principes à la base d'un programme d'ordinateur ne sont pas protégés par le droit d'auteur en vertu de la présente directive.** »

→ **Seule l'expression d'un programme est protégée** (code source, code objet, travaux préparatoires de conception).



Les fonctionnalités (y compris les algorithmes) **ne sont pas protégées.**

IA : différentes facettes – différentes protections



IA : quelle(s) protection(s) ?

- Droit d'auteur ?
 - Ne protège pas les fonctionnalités / algorithmes
- Droit sui generis sur les bases de données ?

Droit "sui generis" BDD - Directive 96/9/EC

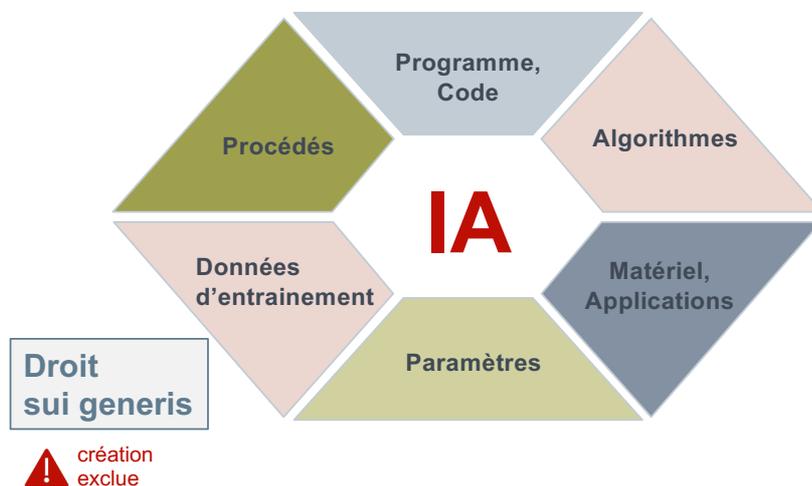
Art. 7 : Le contenu est protégé si « l'obtention, la vérification ou la présentation de ce contenu attestent un **investissement substantiel** du point de vue qualitatif ou quantitatif. »



CJUE (2004) : Le contenu des bases de données pour lequel l'investissement résulte de la **création de données** plutôt que de leur obtention **est exclu de la protection.**

British Horseracing Board Ltd and Others v. William Hill Organization Ltd, CJUE C-203/02, 9 Nov. 2004 ; *Fixtures Marketing Ltd v. Oy Veikkaus Ab*, CJUE C-45/02 ; *Fixtures Marketing Ltd v. Organismos prognostikon agonon podosfairou AE*, CJUE C-444/02 ; *Fixtures Marketing Ltd. v. Svenska Spel AB*, CJUE C-338/02

IA : différentes facettes – différentes protections



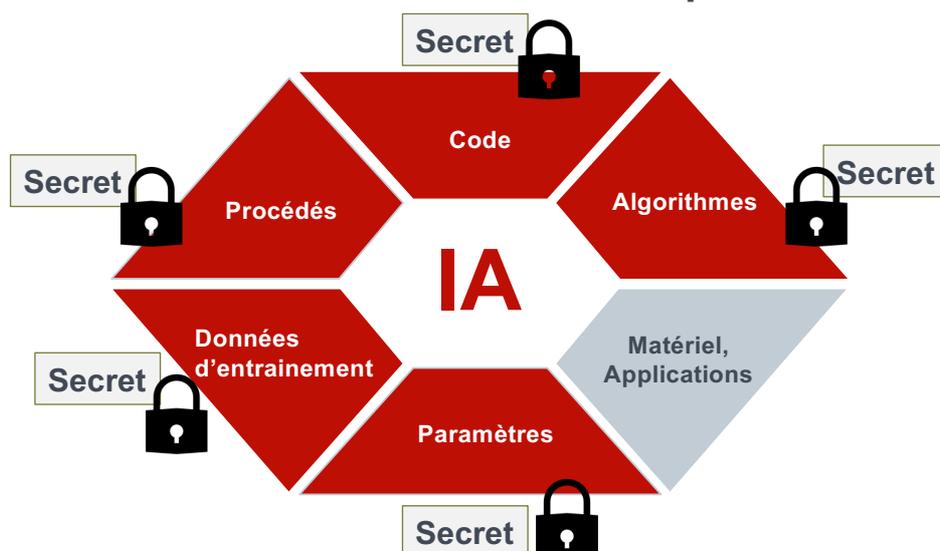
Comment protéger?

- **Droit d'auteur ?**
→ Ne protège pas les fonctionnalités / algorithmes
- **Droit sui generis sur les bases de données ?**
→ Les investissements liés à la création de données sont exclus
- **Secret d'affaires ?**

Secret d'affaires - Directive (UE) 2016/943

- La **directive** a participé à **harmoniser** les règles applicables au sein des Etats membres.
- Un « **secret d'affaires** » doit répondre à **quatre conditions cumulatives**
 - (1) Information (Art. 2 (1))
 - (2) Secret (Art. 2 (1)(a))
 - (3) Valeur commerciale du fait du secret (Art. 2 (1)(b))
 - (4) Mesures pour conserver le secret (Art. 2 (1)(c))

IA : différentes facettes – différentes protections



Secrets d'affaires et ingénierie inverse

Article 3(1)(b) : l'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information et qui n'est pas liée par une obligation juridiquement valide de limiter l'obtention du secret d'affaires.

Raison 16 : L'ingénierie inverse d'un produit obtenu de façon licite devrait être considérée comme un moyen licite d'obtenir des informations, sauf dispositions contractuelles contraires.

Published as a conference paper at ICLR 2018

TOWARDS REVERSE-ENGINEERING BLACK-BOX NEURAL NETWORKS

Seong Joon Oh, Max Augustin, Bernt Schiele, Mario Fritz
Max-Planck Institute for Informatics, Saarland Informatics Campus, Saarbrücken, Germany
{joon,maxaug,schiele,mfritz}@mpi-inf.mpg.de

"Internal information about the model, such as **the architecture, optimisation procedure, or training data**, is not disclosed explicitly as it might contain proprietary information or make the system more vulnerable. **This work shows that such attributes of neural networks can be exposed from a sequence of queries.**"



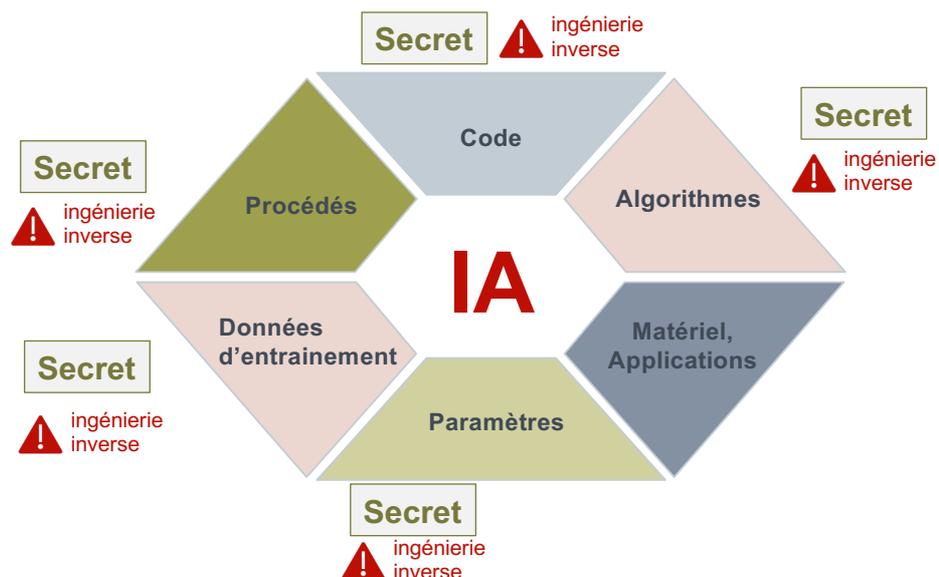
Ingénierie inverse et IA ?...

« With the proposed black-box attack approach, an adversary can **use deep learning [...] to build a functionally equivalent machine learning classifier** without knowing the type, structure or underlying parameters of the original classifier. »

Shi, Sagduyu & Grushin, *How to steal a machine learning classifier with deep learning*, IEEE, 2017

→ Le recours au seul secret peut être risqué !...

IA : différentes facettes – différentes protections



Comment protéger?

- **Droit d'auteur ?**
 - Ne protège pas les fonctionnalités / algorithmes
- **Droit sui generis sur les bases de données ?**
 - Les investissements liés à la création de données sont exclus
- **Secret d'affaires ?**
 - Ne protège pas contre l'ingénierie inverse
- **Brevets ?**
 - Protège les fonctionnalités techniques
 - Soumis aux conditions de brevetabilité

Un impact mesurable sur les demandes de brevets

Figure 3.1. AI patent families and scientific publications by earliest publication year
AI patent families grew by an average of 28 percent and scientific publications by 5.6 percent annually between 2012 and 2017

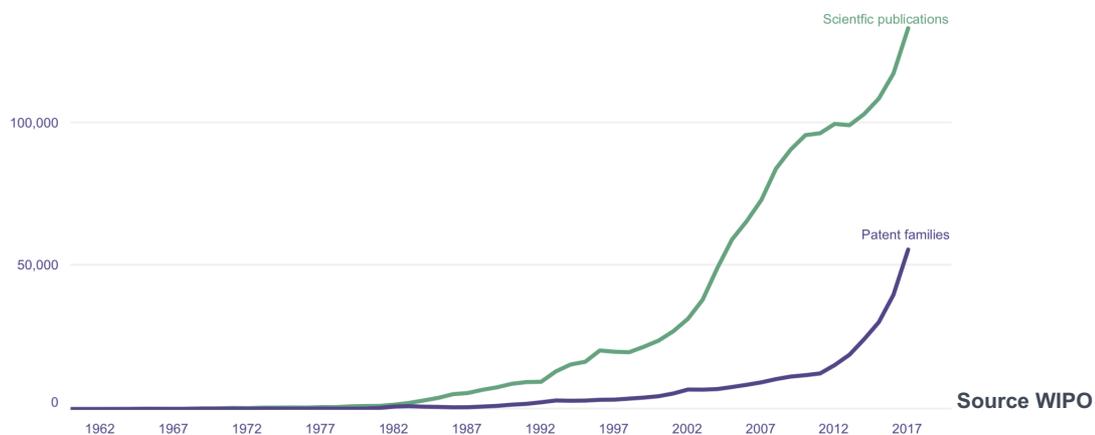
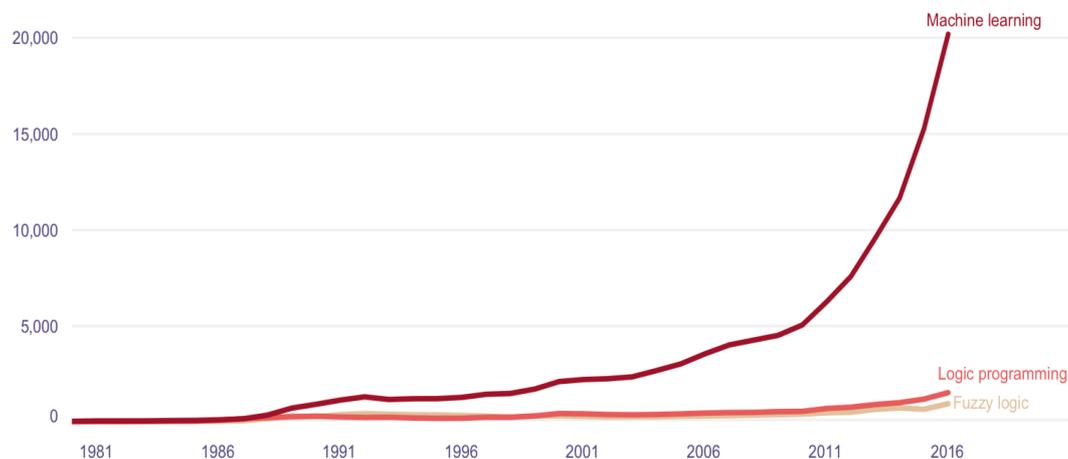


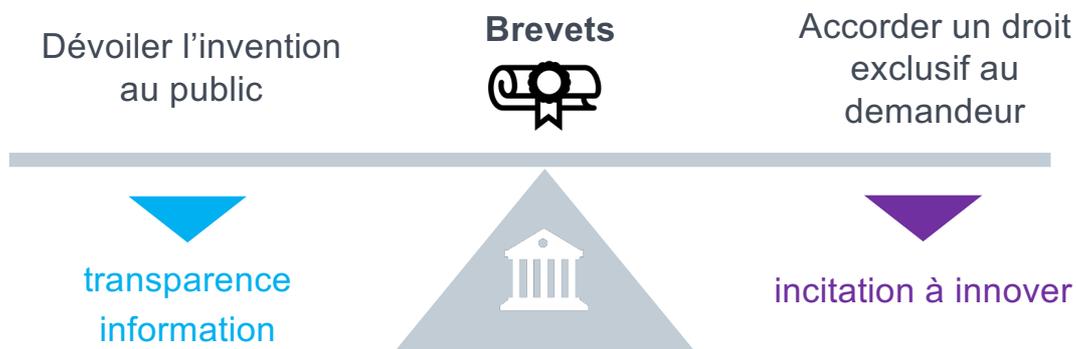
Figure 3.4. Patent families for top AI techniques by earliest priority year
Machine learning grew by an average of 26 percent annually between 2011 and 2016



Note: A patent may refer to more than one category

Source WIPO

Brevets et IA : respecter l'équilibre



Les conditions de brevetabilité

Les brevets sont délivrés pour des **inventions** dans tous les domaines techniques

Pour être brevetable, une **invention** doit:

- être **nouvelle**
- être **inventive**
- être **applicable dans l'industrie**

- **L'IA peut-elle être considérée comme une « invention » ?**

Exclusions au sens de l'Art. 52(2) CBE

- Découvertes
- Théories scientifiques
- **Méthodes mathématiques**
- Programmes d'ordinateur
- Créations esthétiques
- Méthodes dans le domaine des affaires
- Méthodes dans le domaine des jeux
- Activités intellectuelles
- Présentations d'information

Exclus uniquement si
revendiqués
"en tant que tels"

Caractéristiques techniques et mesure de l'inventivité

caractéristiques
« techniques »

évident ?

état de l'art
le plus proche

caractéristiques
« non techniques »

si non évident → 

IA et contribution au caractère technique

Les étapes algorithmiques/IA contribuent au caractère technique de l'invention si elles remplissent l'une ou l'autre de deux conditions (« dimensions »)

- En étant adaptées à une **implémentation technique spécifique**
- Par leur **application à un domaine technique**

(Directives OEB section G-II 3.3)

1^{re} dimension : implémentation technique spécifique



Suffisant :

si l'architecture algorithmique est motivée par des considérations techniques **liées au fonctionnement interne spécifique de l'ordinateur (ou de l'implémentation matérielle)**

Insuffisants :

- Une **implémentation technique générique** ("vanilla" ANN, SVM, GA, etc.)
- La **simple programmation** (coder un ANN, SVM, en C++, Python,...)
- Le simple fait que **l'algorithme (en tant que tel) soit plus efficace**

2^{de} dimension : une finalité technique



Suffisant

si l'étape participe à la solution d'un **problème technique concret**

→ **Pb** : Comment définir le champ des "finalités techniques"?

Insuffisants :

- **Application générique** (la mention au "contrôle d'un système technique" ne suffit pas)
- Potentialité seule : il faut que la fonction soit effectivement remplie et qu'elle soit clairement délimitée / justifiée (v. données...)

2^{de} dimension : une finalité technique

Exemples de finalités techniques de l'IA (Directives OEB G-II, 3.3)

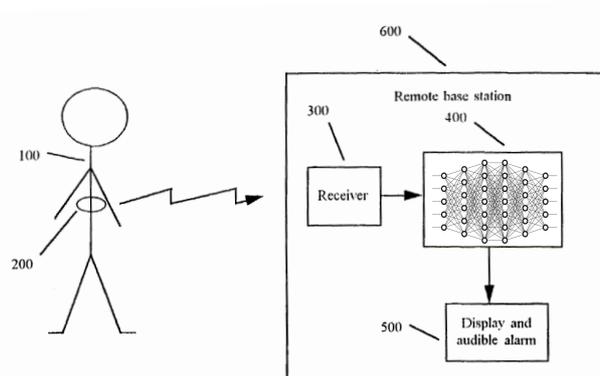
1. Traitement d'image (classification, segmentation)
2. Traitement de la parole (reconnaissance, débruitage)
3. Détection d'erreurs, codage, compression, cryptographie
4. Analyse médicale
- ...
- ... Véhicules autonomes, contrôle industriel, robotique



Non techniques : « linguistique » (spam, ranking), méthodes d'affaire, etc.

Exemple d'application technique : T 598/07

Utilisation d'un réseau de neurones dans un moniteur cardiaque pour limiter les fausses alertes



Finalité technique
→ l'algorithme **peut contribuer**
au caractère inventif

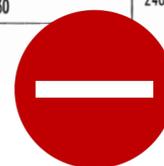
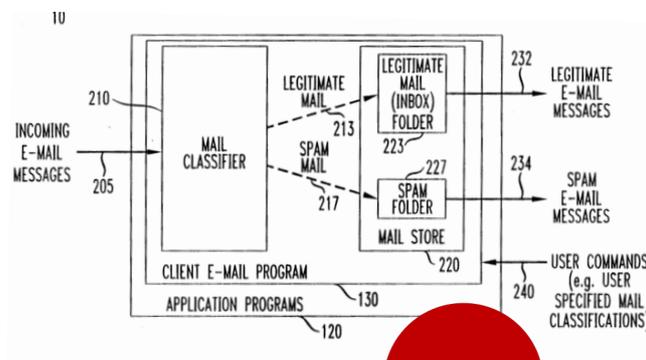
L'utilisation de l'algorithme dans un tel contexte doit alors être comparée à l'art antérieur : la solution peut être "évidente" ou "non évidente" → **analyse au cas par cas**

Exemple d'application non technique : T 0022/12

SVM pour la classification de "spam"

Les considérations "linguistiques" constituent une finalité "non technique"

→ L'application d'un algorithme à une finalité non technique **ne peut contribuer au caractère inventif**

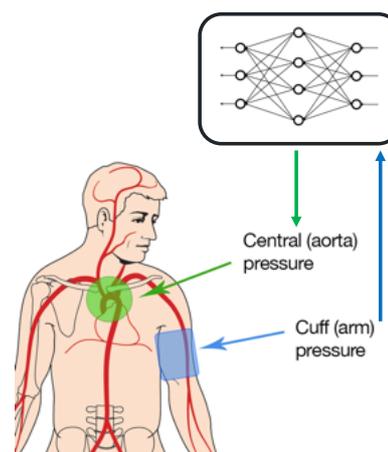


T 161/18 (Äquivalenter Aortendruck/ARC SEIBERSDORF) du 12.5.2020

Claim 8: Device for determining the cardiac output from the peripheral arterial blood pressure signal, comprising a measuring device for detecting the blood pressure signal, a computing unit for transforming the measured blood pressure signal into the equivalent aortic pressure (...)

characterized in that:

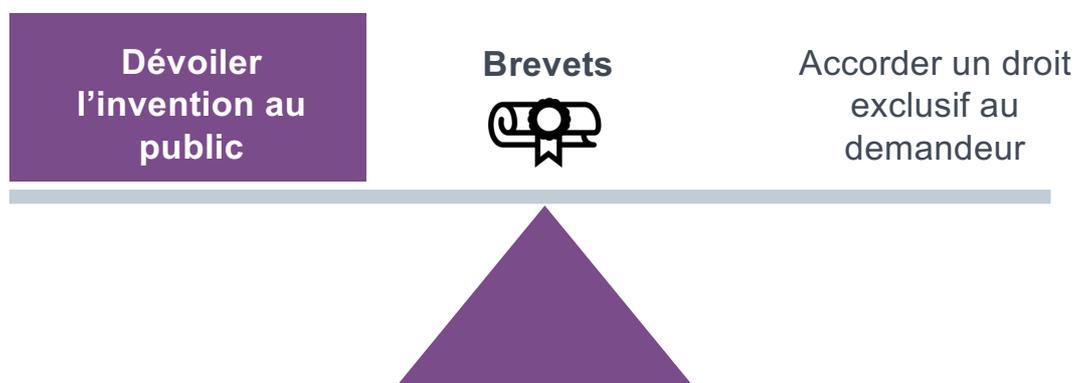
the computing unit for transforming the measured blood pressure signal includes **an artificial neural network, the weighting values of which are determined by a learning process.**



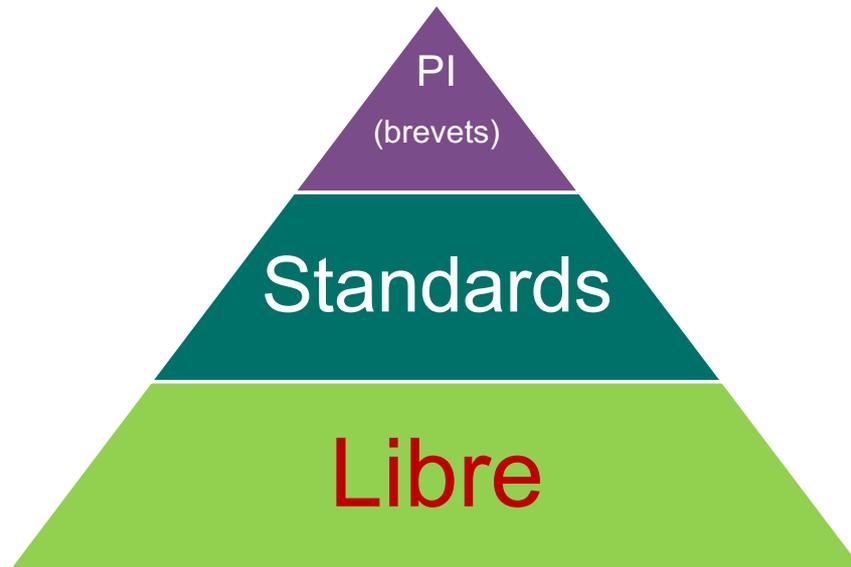
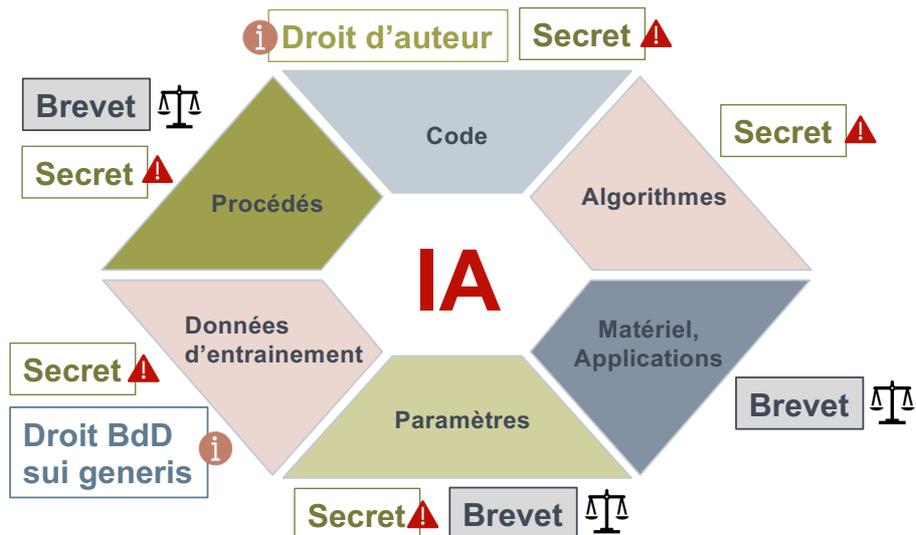
Données d'entraînement et défaut d'enseignement

- *“The present application merely discloses that the input data should cover a broad spectrum of patients of different ages, genders, constitutional types, health status and the like, so that there is no specialization of the network itself (...)”*
- **Selon la chambre, la demande n'indique pas quelles données sont nécessaires à un entraînement effectif du réseau de neurones (...)** en conséquence, la personne du métier **n'est pas à même de reproduire l'invention.**
- **Donc**, la demande ne remplit pas les conditions **de suffisance de l'exposé.**

Brevets et IA : respecter l'équilibre



Équilibre (bis)

IA & PI : un ensemble de protections... **et de conditions**

Conclusion

- L'IA – création, source d'investissement, moteur d'innovation – peut nécessiter et justifier d'une protection au titre de la PI.
- **Droit d'auteur, secret des affaires, droit sui generis sur les bases de données** peuvent protéger différentes composantes d'une application IA (sous certaines conditions / avec certaines limites).
- **Les procédés/systèmes IA sont susceptibles de protection par le brevet**
 - L'évaluation de l'évidence doit prendre en **compte l'ensemble des caractéristiques** contribuant au caractère technique.
 - La contribution technique des étapes algorithmiques est établie selon deux dimensions : **implémentation spécifique et/ou application.**