

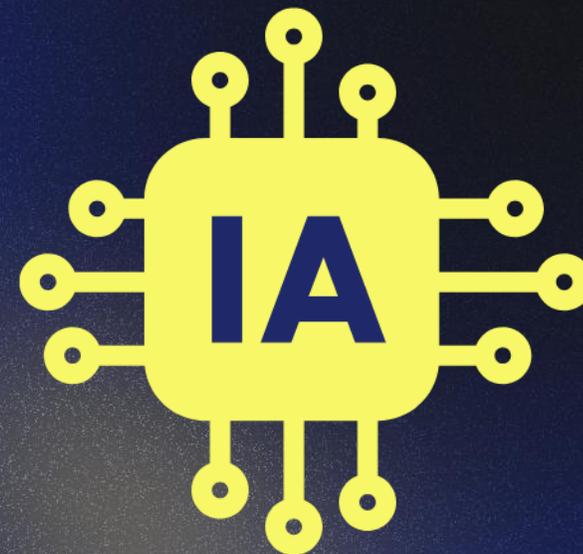
AI Act & IA digne de confiance

Victor Jourdren

Doctorant au CRDP (Université de Lille)

Juriste chez Polar.ia

Octobre 2025



P*lar.ia

Introduction. Les lignes directrices en matière d'éthique du GEHN IA pour une IA digne de confiance.

Définition.

- ❑ **La licéité (1).** Le respect des législations et réglementations applicables.
- ❑ **L'éthique (2).** L'alignement sur les normes éthiques.
- ❑ **La robustesse (3).** Les systèmes devraient être mis en œuvre de manière sûre, sécurisée et fiable

Les principes éthiques de l'IA

Le principe de respect de l'autonomie humaine. Les SIAs ne doivent pas empêcher les humains de conserver leur autodétermination.

Le principe de l'équité.

- Volet matériel : veiller à une répartition égale des bénéfices et des coûts & contrôler les biais injustes, de discrimination et de stigmatisation ;
- Volet procédural.

Le principe de la prévention de toute atteinte.

- Environnement sûr et sécurisé ;
- Porter une attention particulière aux utilisations malveillantes ;
- Protéger les personnes vulnérables ;
- Vérifier que l'IA n'amplifie pas les asymétries de pouvoir ou d'information ;
- Veiller au vivant et à l'environnement.

Le principe de l'explicabilité. Les capacités, les finalités d'IA doivent être communiqués aux personnes exposées directement ou indirectement.



Action humaine et
contrôle humain

Robustesse
technique et sécurité



Vie privée et
gouvernance des
données



Les exigences éthiques de l'IA



Transparence

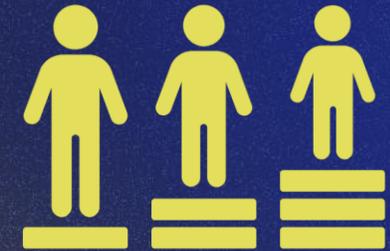


Bien-être sociétal
et environnemental



Responsabilité

Diversité, non-
discrimination et
équité



I. Un objectif du règlement européen

« l'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain **et digne de confiance** ». (Art. 1)

❑ « **parvenir** » à une IA digne de confiance ; (Cons. 3)

❑ « **faire en sorte** que l'IA soit digne de confiance » ; (Cons. 3 & 27)

❑ à « **soutenir** la consolidation et une trajectoire d'innovation d'une IA digne de confiance ». (Cons. 20)

Cela passe notamment par la **maîtrise de l'IA**, « **les compétences, les connaissances et la compréhension** qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, [...] de **procéder à un déploiement des systèmes d'IA en toute connaissance de cause**, ainsi que de prendre conscience **des possibilités et des risques** que comporte l'IA, ainsi que des **préjudices potentiels qu'elle peut causer** ». (Art. 3.57)

« Les fournisseurs et les déployeurs de SIA prennent des mesures pour garantir, dans toute la mesure du possible, **un niveau suffisant de maîtrise de l'IA** pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des SIA pour leur compte, en prenant en considération leurs connaissances techniques, leur expérience, leur éducation et leur formation, ainsi que le contexte dans lequel les systèmes d'IA sont destinés à être utilisés, et en tenant compte des personnes ou des groupes de personnes à l'égard desquels les systèmes d'IA sont destinés à être utilisés ». (Art. 4)

« la mise en œuvre à grande échelle de mesures relatives à **la maîtrise de l'IA** [...] pourrait contribuer [...] à terme, soutenir la consolidation et une trajectoire d'innovation **d'une IA digne de confiance dans l'Union** ». (Cons. 20)

II. Des principes éthiques à l'approche par les risques

À travers les différents niveaux de risque posés par le règlement, transparait **quasi explicitement l'idée d'une IA digne de confiance et plus encore des principes et des exigences éthiques** développés dans les lignes directrices.



(notamment le principe de prévention de toute atteinte)

Article 5. Risque inacceptable

Article 6. Risque élevé

Article 50. Risque limité

Article 2.12. Risque minimal

A. Risque inacceptable et interdictions de l'article 5.

- Manipulation.
- Exploitation de vulnérabilités.
- Évaluation et classification (la notation sociale).
- Pénal prédictif.
- Création de bases de données de reconnaissance faciale.
- Inférence d'émotion.
- Catégorisation biométrique individuelle.
- Identification biométrique à distance en temps réel.

Respect de l'autonomie humaine

Prévention de toute atteinte
(utilisations malveillantes, personnes vulnérables, asymétries de pouvoir ou d'information...)

Équité

Volet matériel
& procédural

B. Haut risque (art. 6 & suivants).

Concernant le haut-risque, le 7^{ème} considérant du règlement souligne que les règles concernant les SIA à haut-risque **doivent prendre compte les lignes directrices du GEHN IA.**

« les systèmes d'IA pourraient avoir **un impact négatif sur la santé et la sécurité des citoyens**, en particulier lorsque ces systèmes sont utilisés en tant que composants de sécurité de produits » (Considérant 47). Cet extrait fait le lien entre l'annexe I listant les produits liés à l'article 6 et le **principe de prévention de toute atteinte.**

Concernant les obligations :

- Le **principe d'explicabilité** se concrétise dans l'obligation d'une **documentation technique** (Art. 11) ainsi que d'une **conception transparente.** (Art 13.)
- On retrouve le **contrôle humain** (Art. 14), garantie de **l'autonomie humaine** des lignes directrices.
- « Un niveau adéquat d'exactitude, de **robustesse et de cybersécurité** ». (Art. 15)
- La **qualité des jeux de données** = IA digne de confiance (Cons. 68)

C. Risque limité (art. 50) & minimal

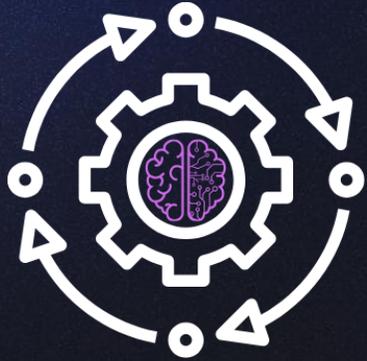
Concernant l'article 50 lien est évident avec le **principe d'explicabilité & l'exigence de transparence**.

D. Risque minimal

Concernant le risque minimal, c'ad les SIA soumis à aucune obligation, le règlement encourage **le volontarisme** et l'auto-application **d'exigences supplémentaires** : « Les fournisseurs et, le cas échéant, les déployeurs de tous les systèmes d'IA, à haut risque ou non, et modèles d'IA devraient aussi être encouragés à appliquer sur **une base volontaire des exigences supplémentaires** ». (Cons. 165)

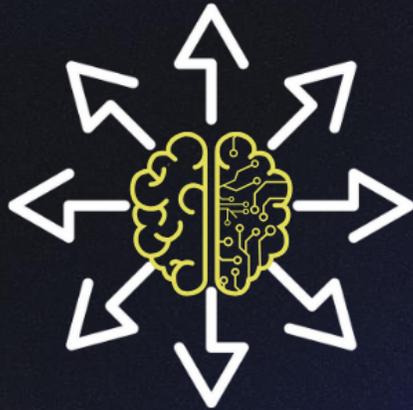
« Le Bureau de l'IA et les États membres facilitent l'élaboration **de codes de conduite concernant l'application volontaire** [...] d'exigences spécifiques à tous les SIA, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que, entre autres les éléments applicables prévus dans les lignes directrices en matière d'éthique pour une IA digne de confiance ». (Art. 95)

E. Concernant les modèles



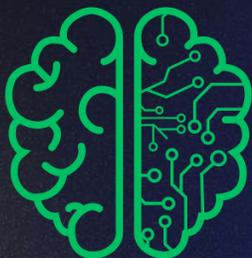
Article 51. Risque systémique d'un modèle d'IA à usage général (MIAUG)

Exemples. Discrimination à large échelle, perte de contrôle de l'IA, risques chimiques, biologiques, radiologiques et nucléaires etc... (First Draft General-Purpose AI Code of Practice)



Article 50 & 53. Risque de tous les MIAUG

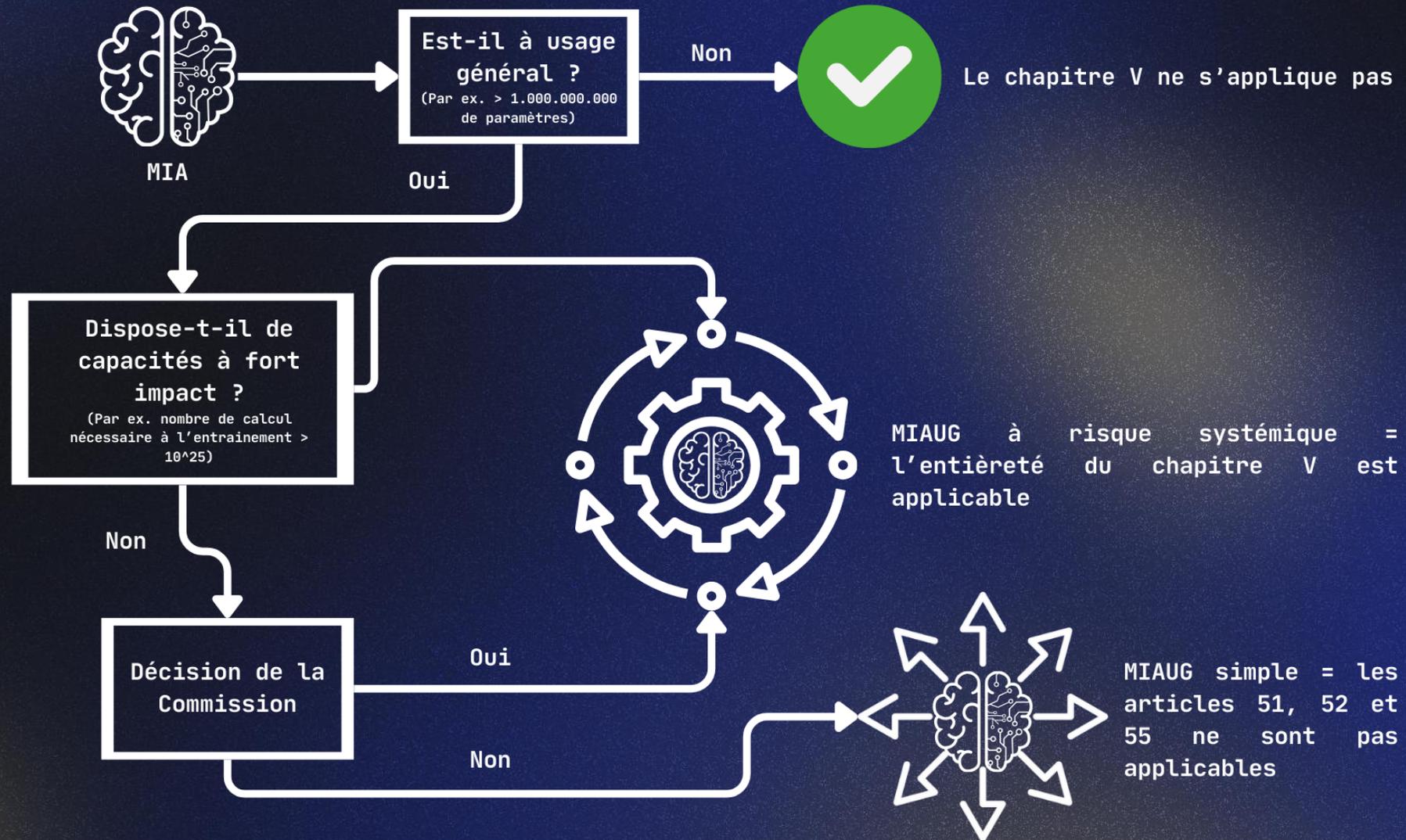
Risques liées à la transparence et risques liés à la propriété intellectuelle. (First Draft General-Purpose AI Code of Practice)



Modèle d'IA simple (MIA)

Sans risque particuliers.

E. Concernant les modèles



Transparence (Art. 53).

- Documentation technique
- Informations
- résumé suffisamment détaillé du contenu utilisé pour entraîner le MIAUG

Protection des droits de propriété littéraire & artistique (Art. 53). Mettre en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins.

Sécurité / Sûreté (Art. 54 & 55)

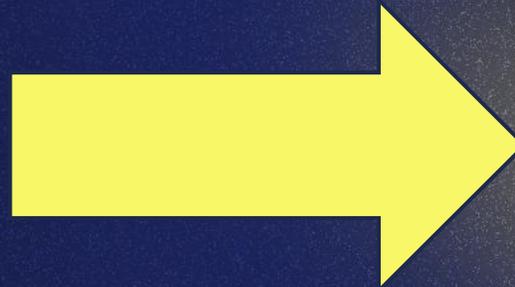
Prévention de toute atteinte (utilisations malveillantes, personnes vulnérables, asymétries de pouvoir ou d'information...)

Explicabilité

III. Au-delà du règlement

Environnement :

- ❑ Principe de **prévention de toute atteinte** : « veiller au vivant et à l'environnement ».
- ❑ Exigence de **bien être social et environnemental**



Incident grave,
traitement à postériori
(Art. 73)



Que faire de plus ?

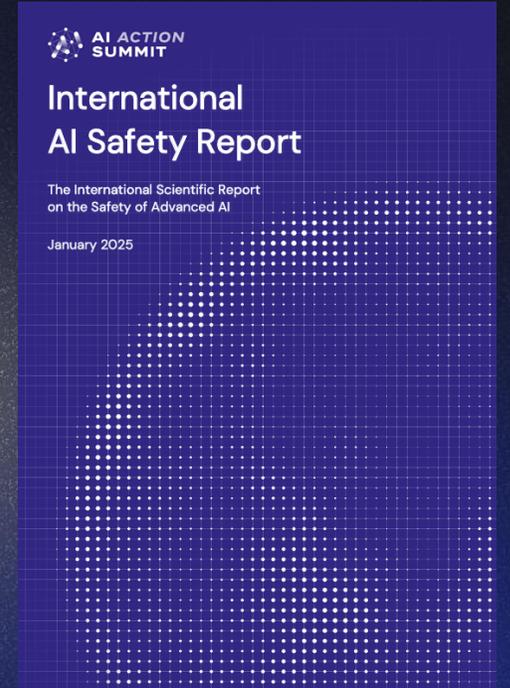
Pour aider à la conformité

European Commission >

EUSurvey



Pour aller plus loin



Charte d'utilisation de l'Intelligence Artificielle

IA digne de confiance & AI ACT :

Passons du côté technique !

2025

Ikram Chraibi Kaadoud

Chargée de projet européen IA digne de confiance et Management Ethique

Chercheuse associée IA explicable & Sciences cognitives

<https://ikramchraibik.com/>



www.dihynamic.eu



Cofinancé par
l'Union européenne



RÉGION
**Nouvelle-
Aquitaine**

Projet cofinancé par la
Région Nouvelle-Aquitaine

©Chraibi Kaadoud Ikram, INRIA x Dihynamic, oct 2025.

Ce document est sous licence CC BY 4.0.

<https://creativecommons.org/licenses/by/4.0/>

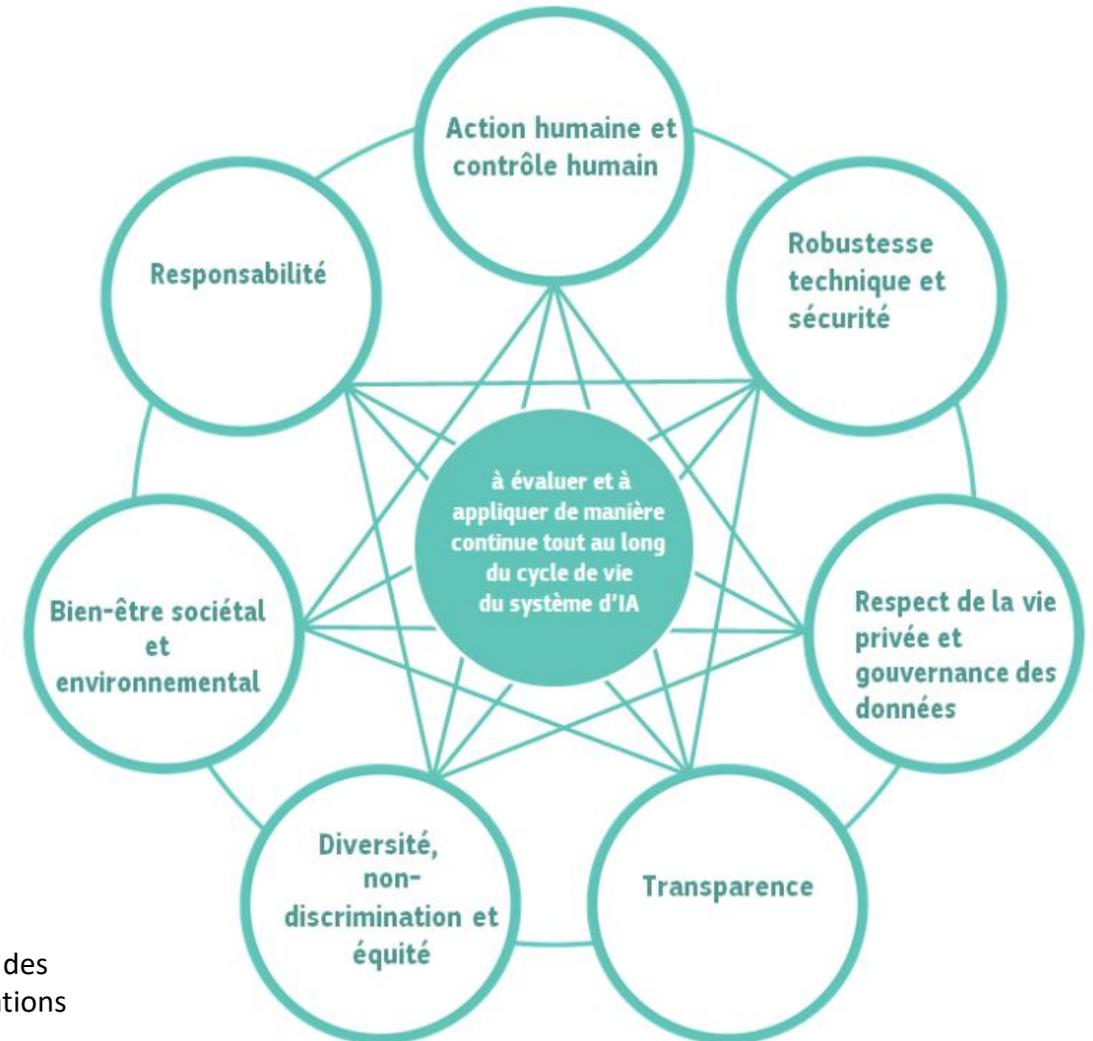
Inria



Une IA digne de confiance selon l'Europe

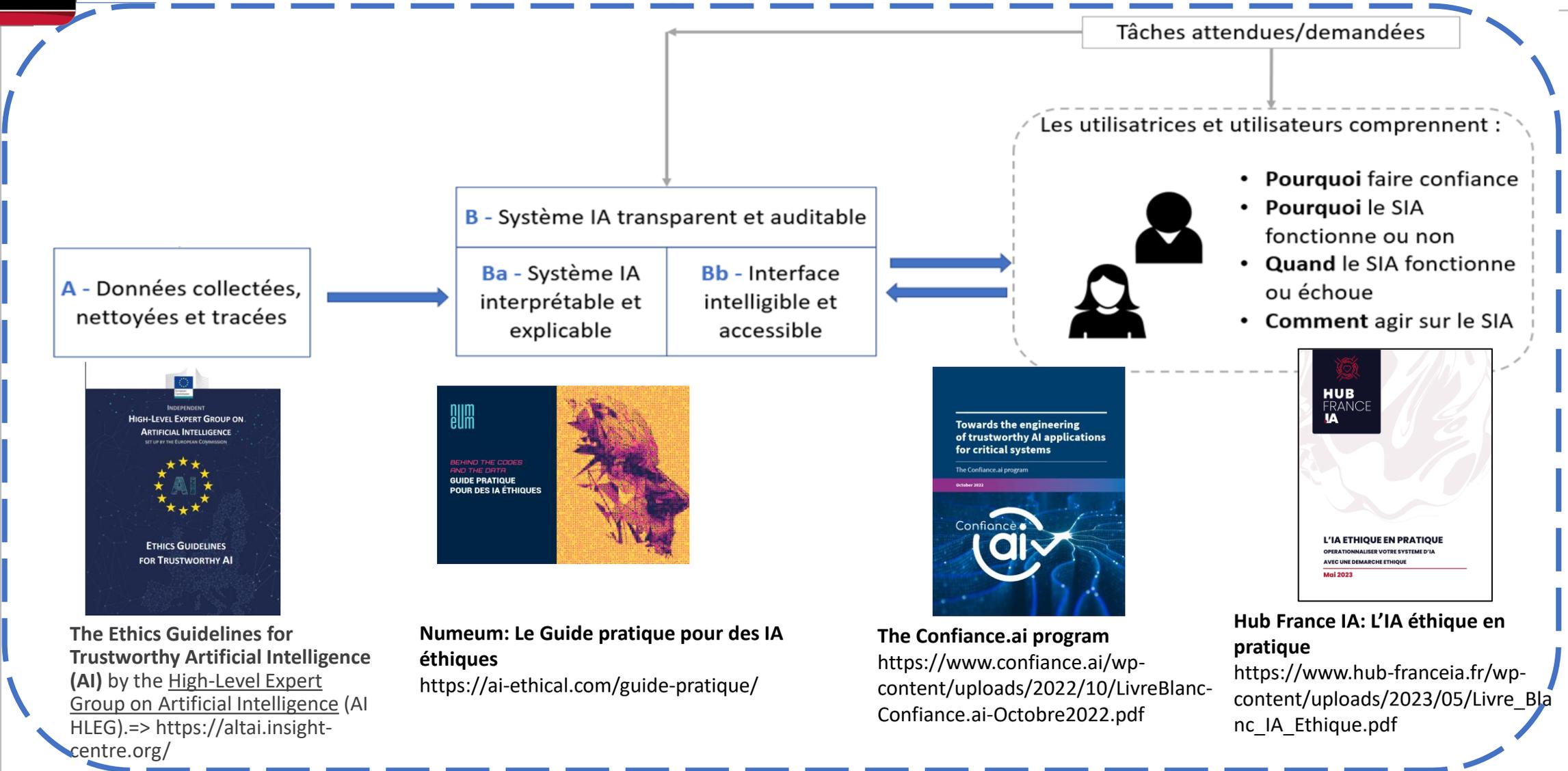


- **Licite** : en accord avec la réglementation nationale et européenne
- **Ethique**: en accord avec des principes et valeurs éthiques
- **Robuste**: sur le plan technique et social





Qu'est-ce qu'un système IA digne de confiance concrètement ?





Comment parvenir à un système d'IA non génératif



Comment parvenir à un système d'IA non génératif

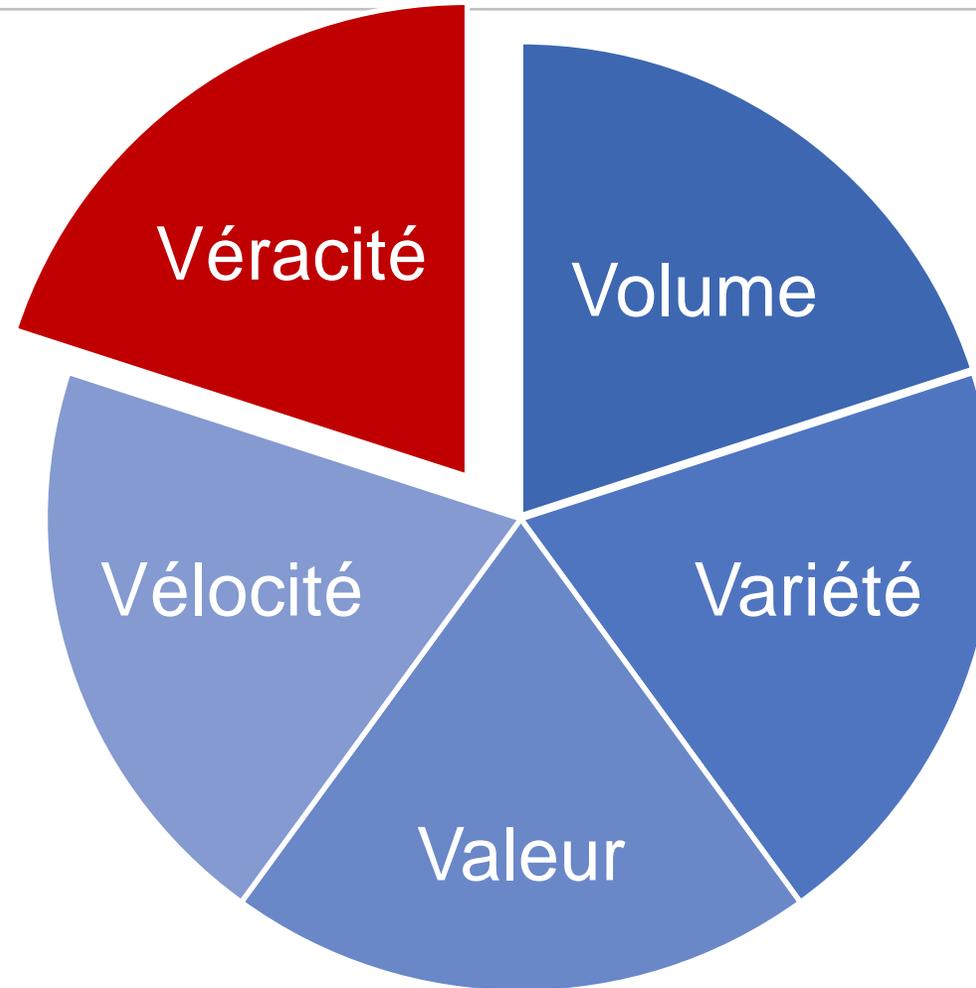
1- Analyser le problème
métier du client



Comment parvenir à un système d'IA non génératif

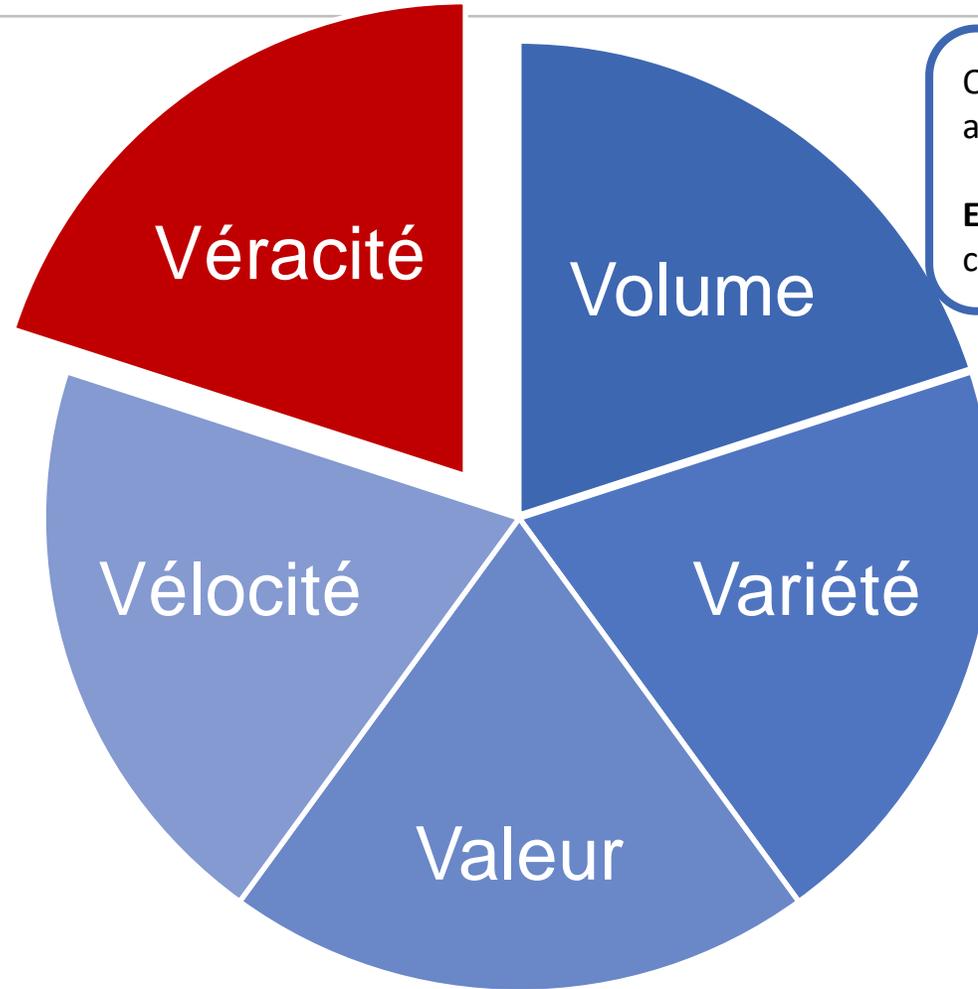
1- Analyser le problème métier du client

2- Récolter et traiter les données





Défis et objectifs liés aux données - Les 5V

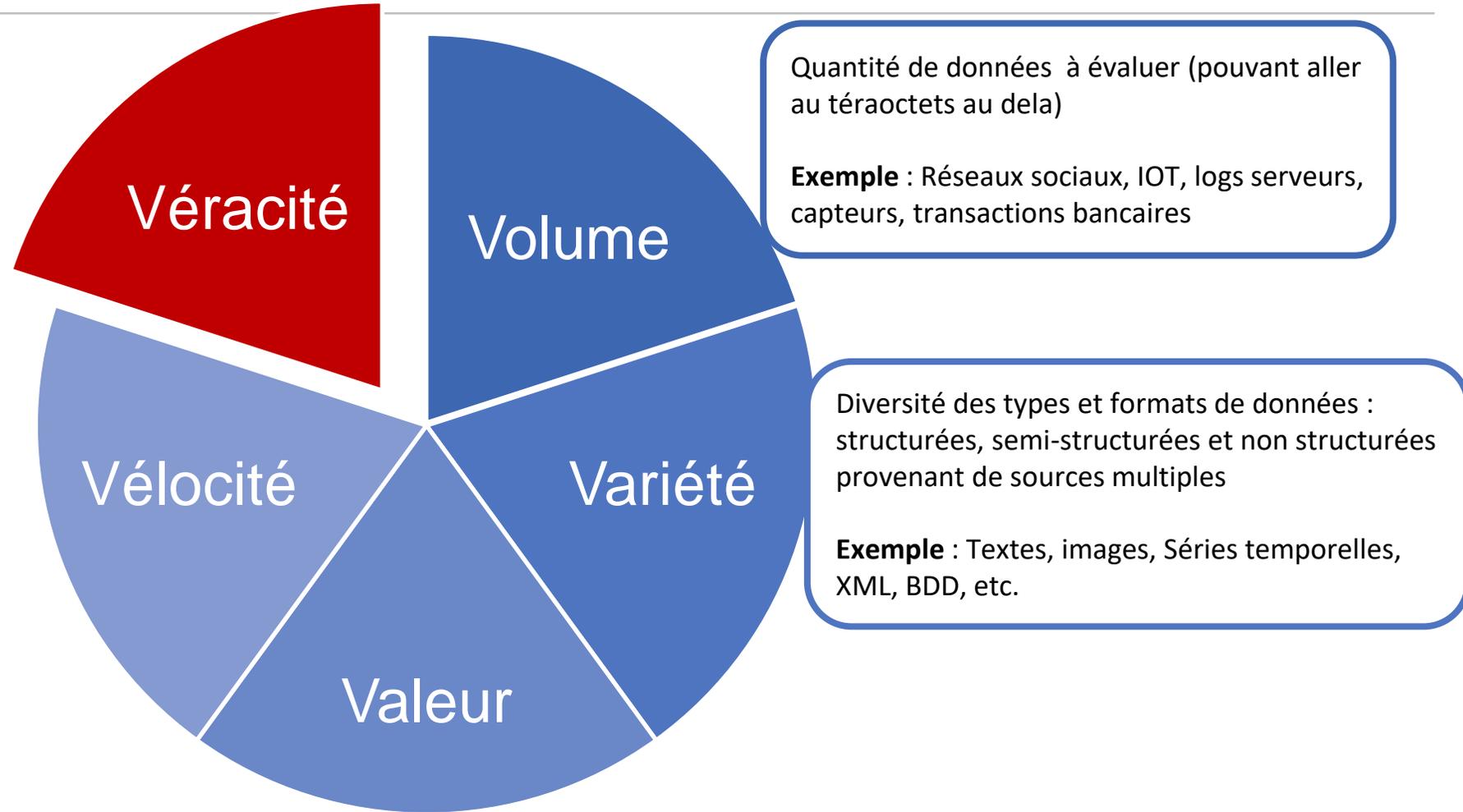


Quantité de données à évaluer (pouvant aller au téraoctets au dela)

Exemple : Réseaux sociaux, IOT, logs serveurs, capteurs, transactions bancaires

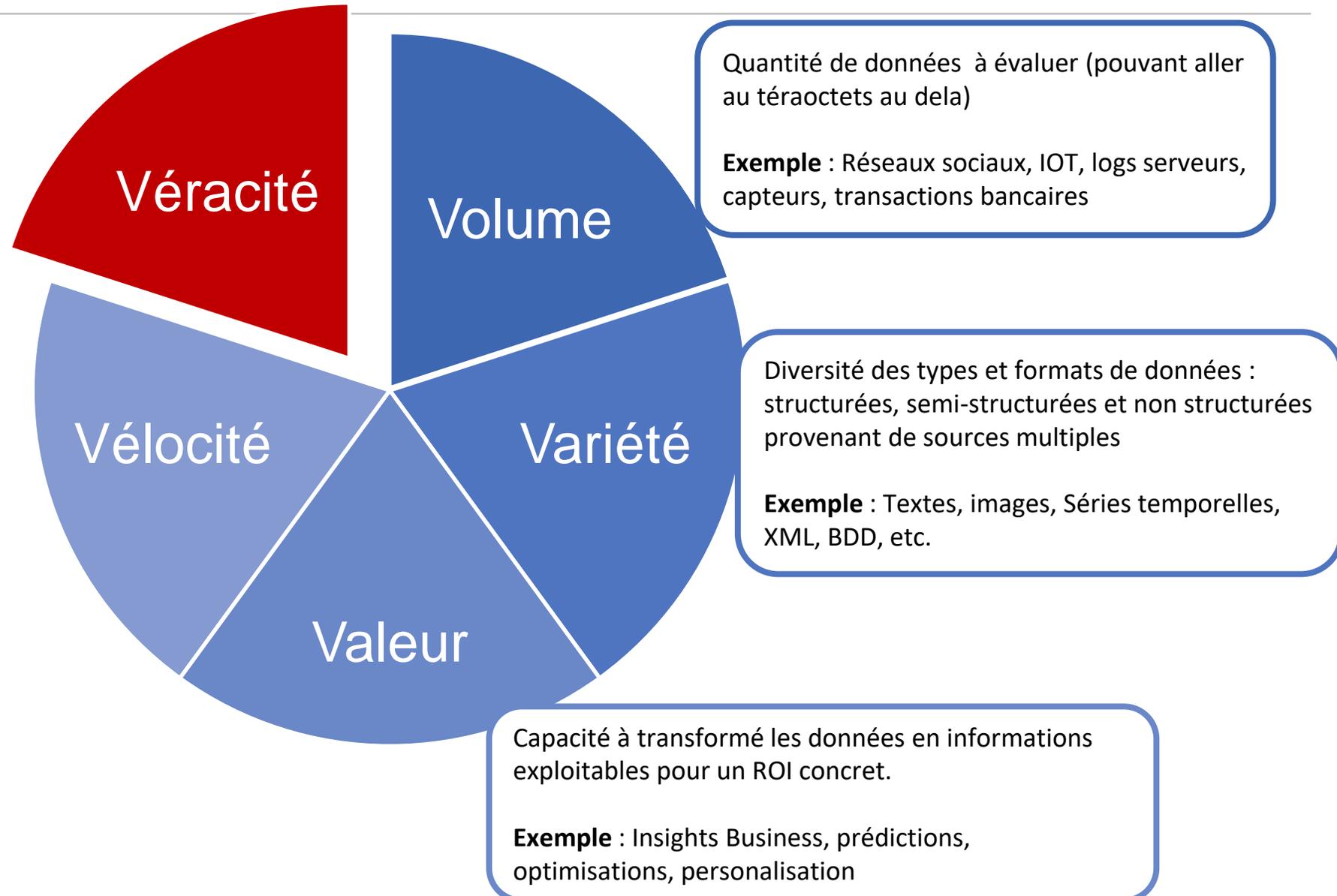


Défis et objectifs liés aux données - Les 5V



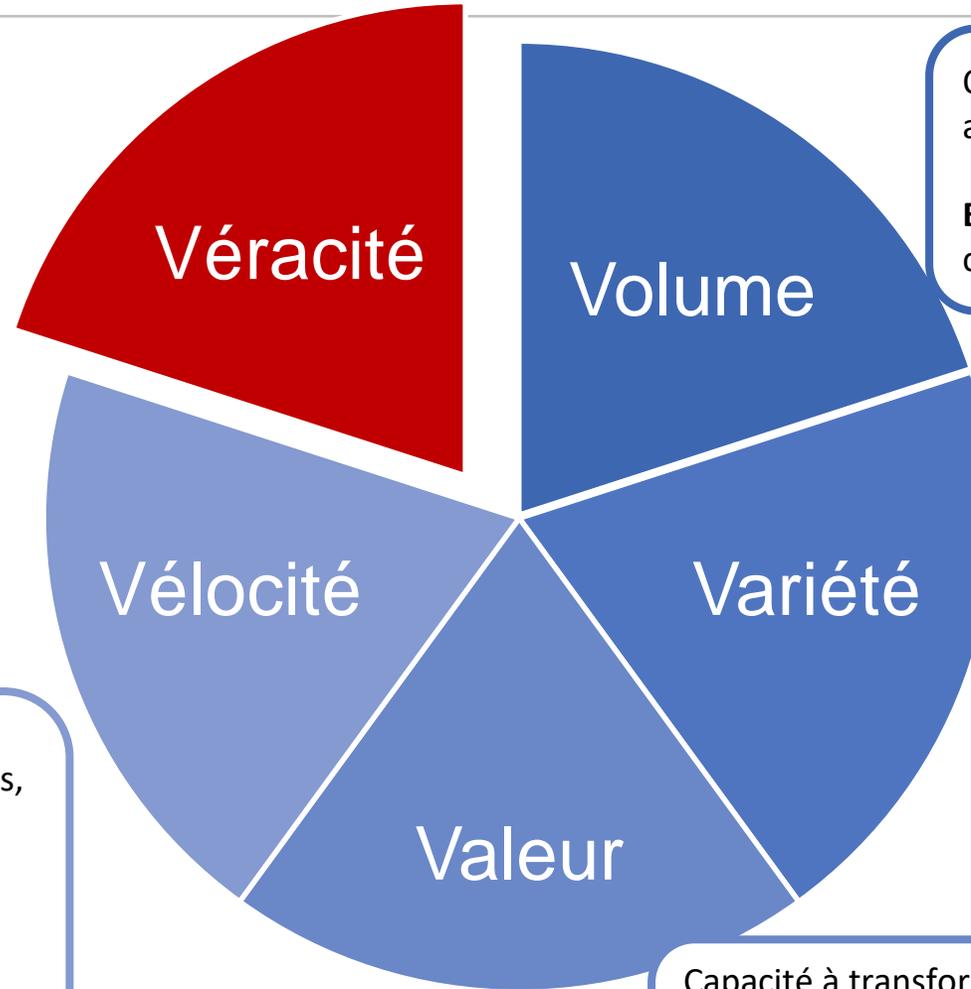


Défis et objectifs liés aux données - Les 5V





Défis et objectifs liés aux données - Les 5V



Quantité de données à évaluer (pouvant aller au téraoctets au dela)

Exemple : Réseaux sociaux, IOT, logs serveurs, capteurs, transactions bancaires

Diversité des types et formats de données : structurées, semi-structurées et non structurées provenant de sources multiples

Exemple : Textes, images, Séries temporelles, XML, BDD, etc.

Vitesse à laquelle les données sont générées, traitées et analysées. Les données peuvent être en temps réelle ou en flux continu

Exemple : Streaming de données, trading, haute fréquence, capteurs en temps réel.

Capacité à transformé les données en informations exploitables pour un ROI concret.

Exemple : Insights Business, prédictions, optimisations, personnalisation



Défis et objectifs liés aux données - Les 5V

Qualité, fiabilité et précision des données. Garantir que les données sont exactes, cohérentes et dignes de confiance.

Exemple : validation des données, détection d'anomalies, nettoyage des données

Véracité

Quantité de données à évaluer (pouvant aller au téraoctets au delà)

Exemple : Réseaux sociaux, IOT, logs serveurs, capteurs, transactions bancaires

Volume

Diversité des types et formats de données : structurées, semi-structurées et non structurées provenant de sources multiples

Exemple : Textes, images, Séries temporelles, XML, BDD, etc.

Variété

Vitesse à laquelle les données sont générées, traitées et analysées. Les données peuvent être en temps réel ou en flux continu

Exemple : Streaming de données, trading, haute fréquence, capteurs en temps réel.

Vélocité

Valeur

Capacité à transformer les données en informations exploitables pour un ROI concret.

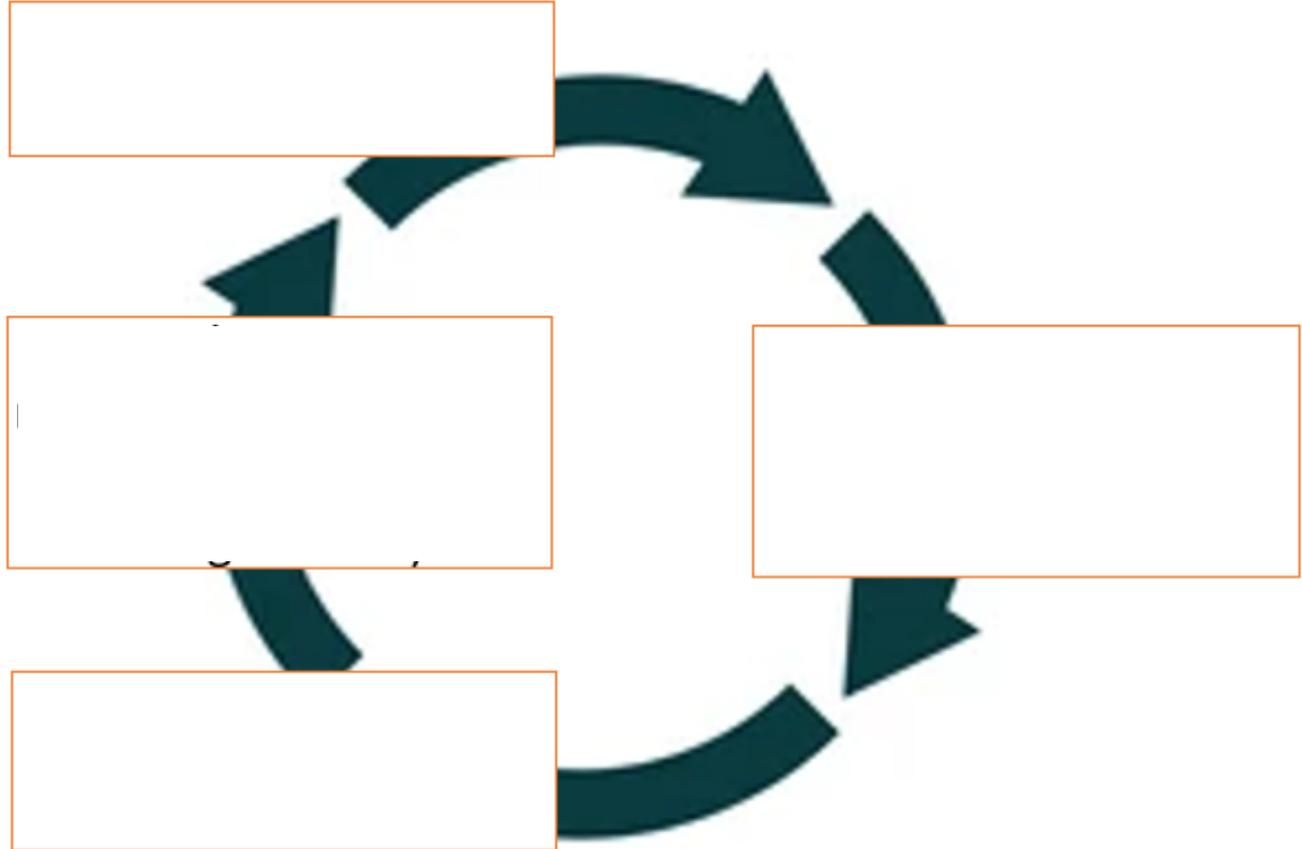
Exemple : Insights Business, prédictions, optimisations, personnalisation



Comment parvenir à un système d'IA non génératif

1- Analyser le problème métier du client

2- Récolter et traiter les données



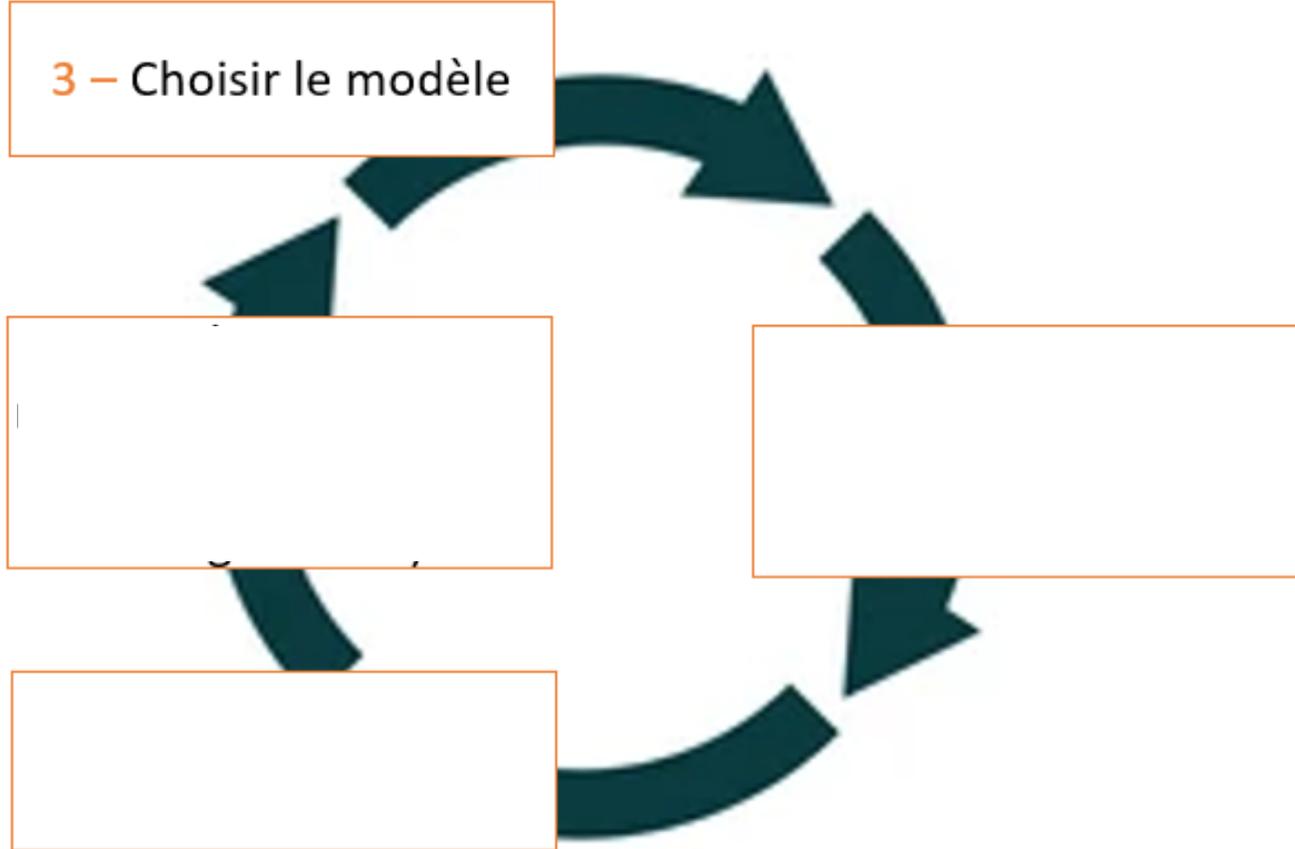


Comment parvenir à un système d'IA non génératif

1- Analyser le problème
métier du client

2- Récolter et traiter les
données

3 – Choisir le modèle





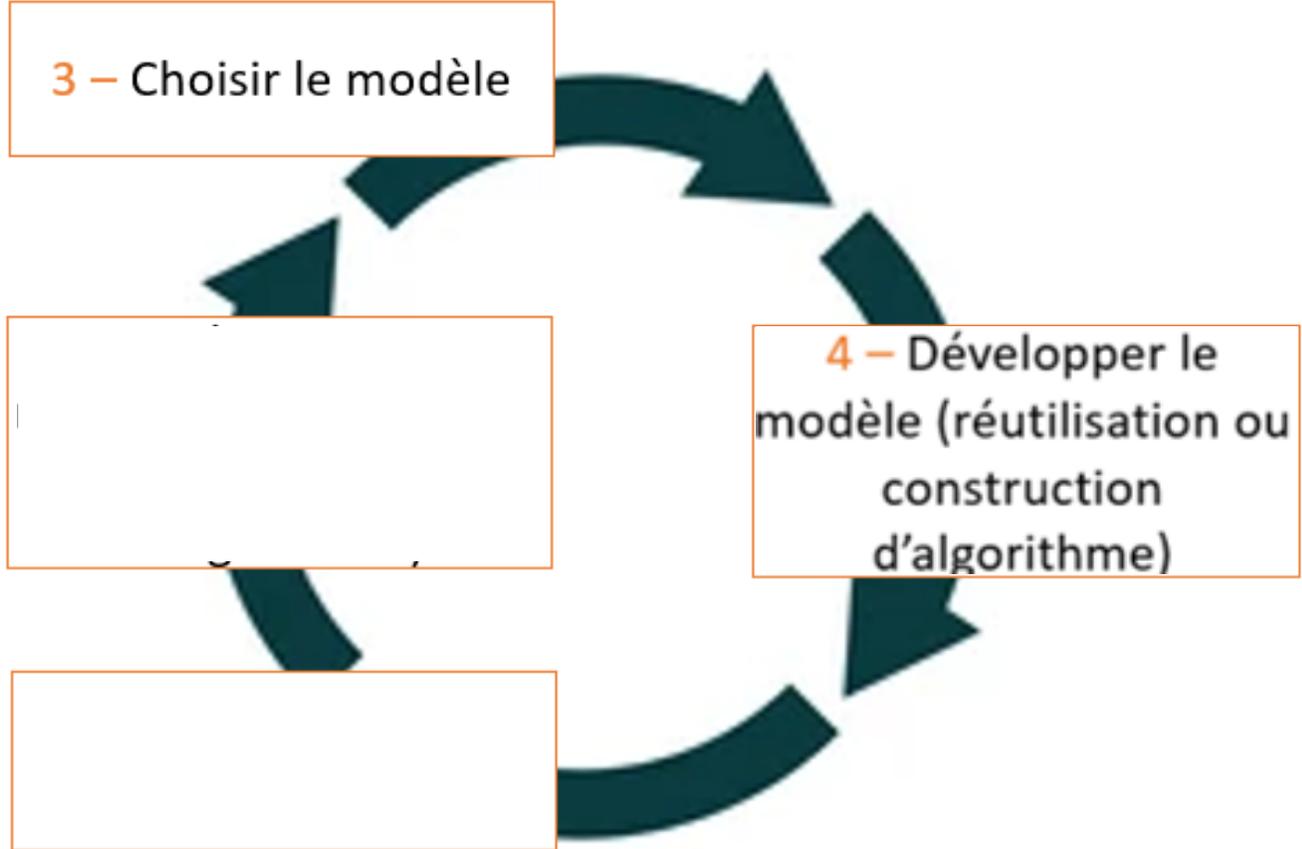
Comment parvenir à un système d'IA non génératif

1- Analyser le problème
métier du client

2- Récolter et traiter les
données

3 – Choisir le modèle

4 – Développer le
modèle (réutilisation ou
construction
d'algorithme)





Comment parvenir à un système d'IA non génératif

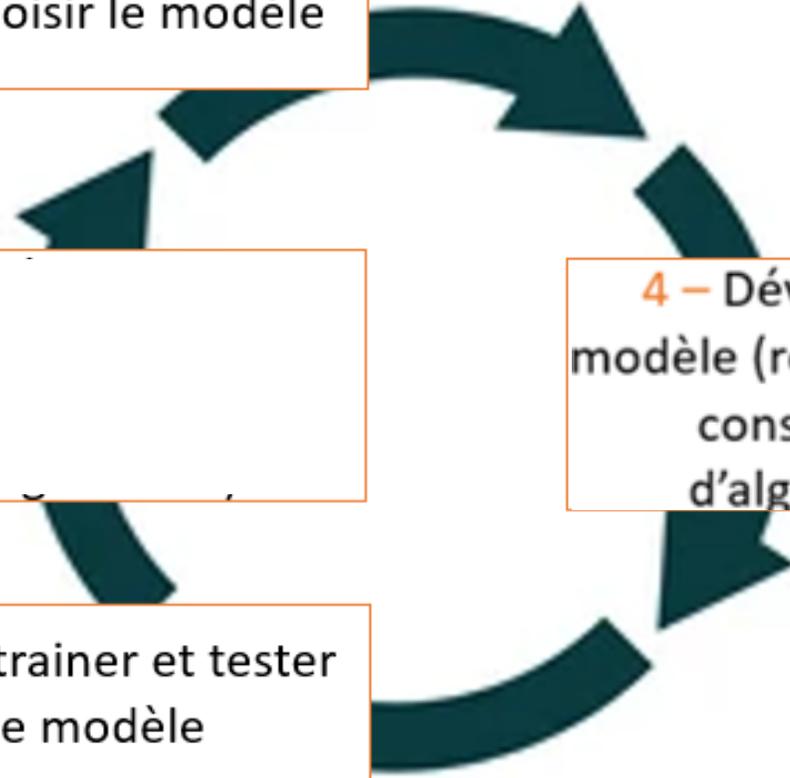
1- Analyser le problème métier du client

2- Récolter et traiter les données

3 – Choisir le modèle

4 – Développer le modèle (réutilisation ou construction d'algorithme)

5 – Entraîner et tester le modèle





Comment parvenir à un système d'IA non génératif

1- Analyser le problème métier du client

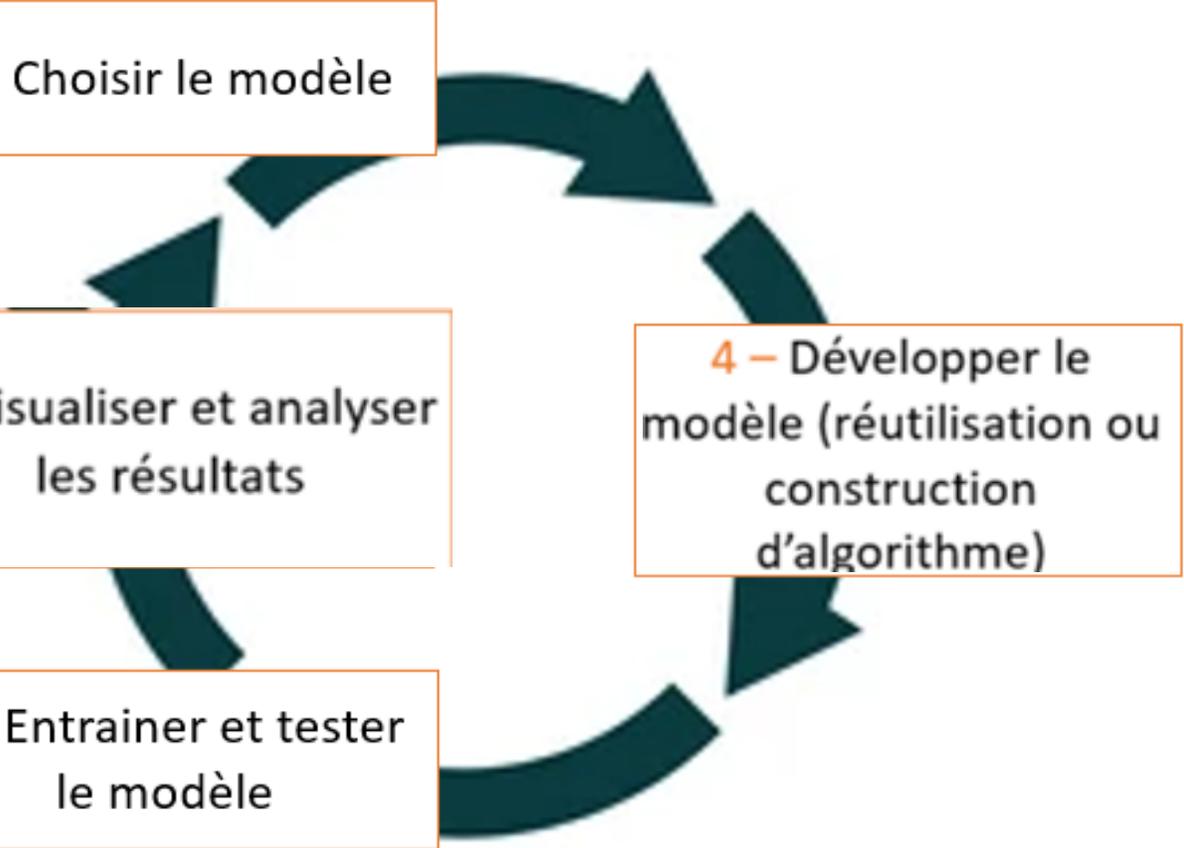
2- Récolter et traiter les données

3 – Choisir le modèle

6 -Visualiser et analyser les résultats

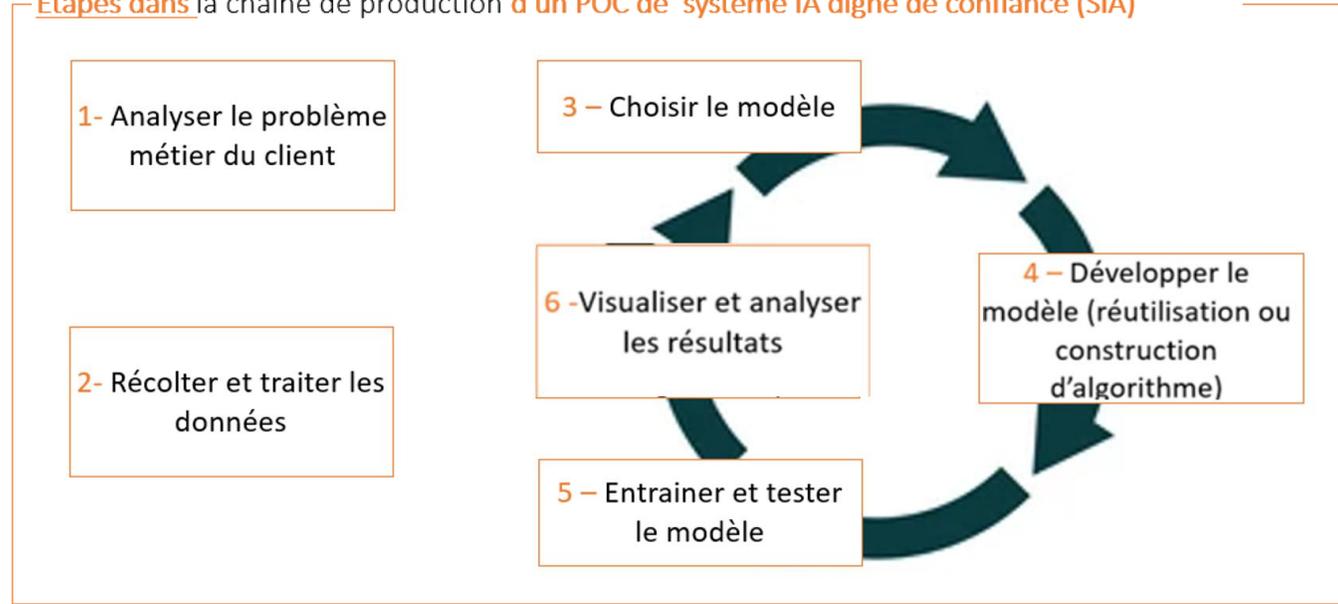
5 – Entraîner et tester le modèle

4 – Développer le modèle (réutilisation ou construction d'algorithme)

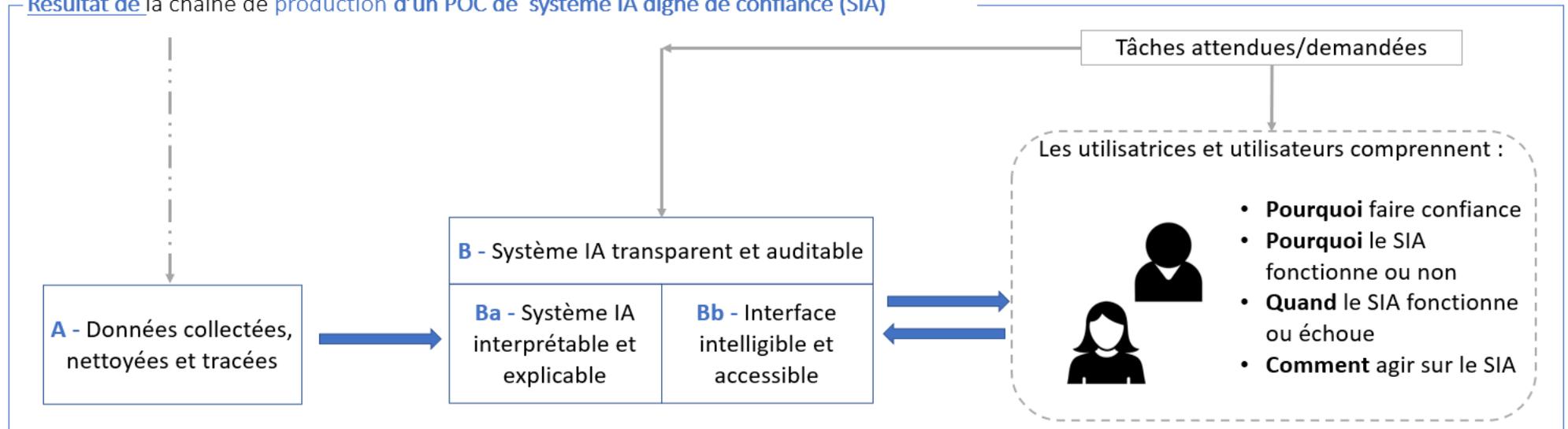




Etapes dans la chaîne de production d'un POC de système IA digne de confiance (SIA)



Résultat de la chaîne de production d'un POC de système IA digne de confiance (SIA)





SIA digne de confiance selon la charte Dihynamic

**Une charte :
Des guidelines en accord avec
les priorités opérationnelles et
la réglementation en vigueur**

🌐 Lien : <https://www.dihynamic.eu/fr/dihynamic-publie-sa-charte-ia-digne-de-confiance/>



Charte Dihynamic Intelligence Artificielle de Confiance & Éthique pour le Numérique



Co-financé par l'Union européenne



Nouvelle-Aquitaine

www.dihynamic.eu



CONTACT



Ikram CHRAIBI KAADOUD
INRIA
Ikram.chraibi-kaadoud@inria.fr



1- Analyser le problème métier du client



2- Récolter et traiter les données



3 – Choisir le modèle

6 - Visualiser et analyser les résultats

5 – Entraîner et tester le modèle

4 – Développer le modèle (réutilisation ou construction d’algorithme)

Guidelines Charte et sigles associées



Action humaine et contrôle humain



Robustesse technique et sécurité



Respect de la vie privée et gouvernance des données



Transparence



Non-discrimination, équité et diversité



Bien-être sociétal et environnemental



Responsabilité (sociale et sociétale)

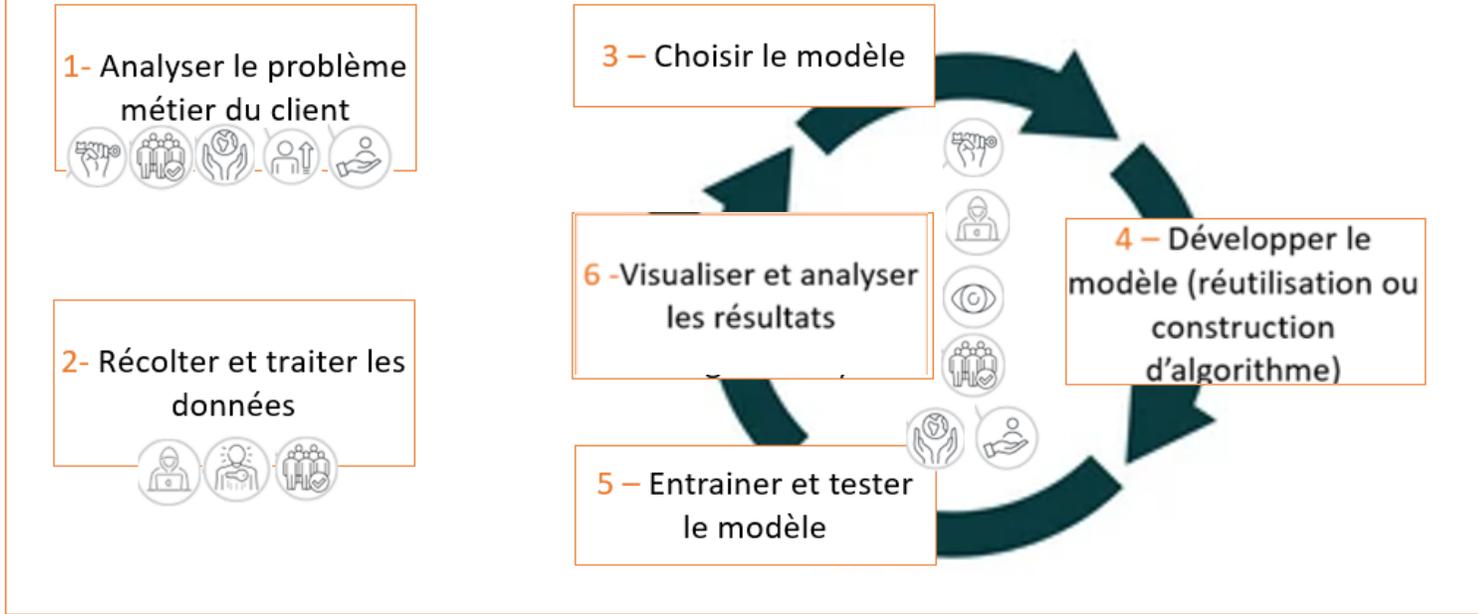


Dignité



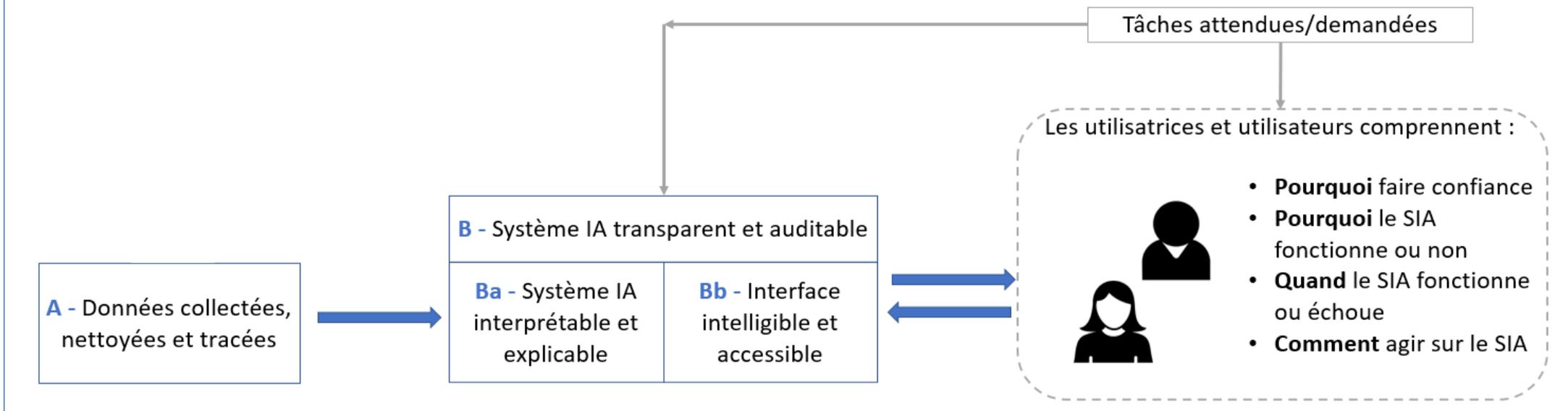
Etapes de la chaîne de conception d'un POC système IA digne de confiance (SIA) et des **résultats associés** depuis la donnée à l'interaction utilisateur-système IA

Etapes dans la chaîne de production d'un POC de système IA digne de confiance (SIA)



- Rappel des guidelines de la charte et sigles associées
- Action humaine et contrôle humain
 - Robustesse technique et sécurité
 - Respect de la vie privée et gouvernance des données
 - Transparence
 - Non-discrimination, équité et diversité
 - Bien-être sociétal et environnemental
 - Responsabilité (sociale et sociétale)
 - Dignité

Résultat de la chaîne de production d'un POC de système IA digne de confiance (SIA)





Enjeu n°1 : Les données

Les étapes 1 et 2 associés au résultat « A - Données collectées, nettoyées et tracées », pour cela il faut:



Robustesse technique et sécurité

Résilience des systèmes et des équipes
Sécurité des données au niveau des installations physiques et au niveau cyber



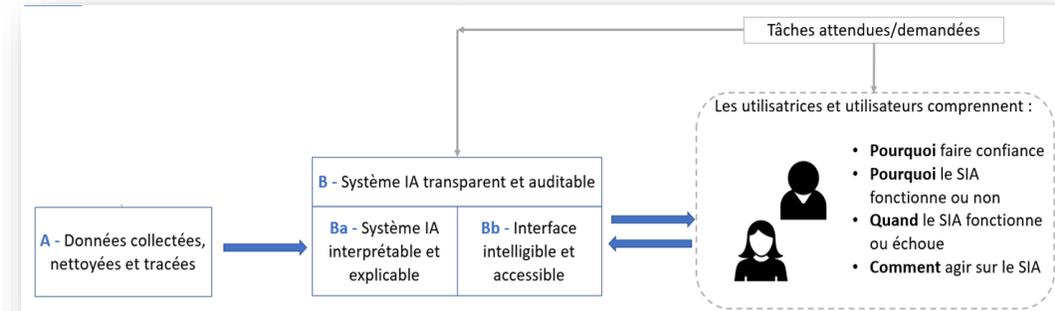
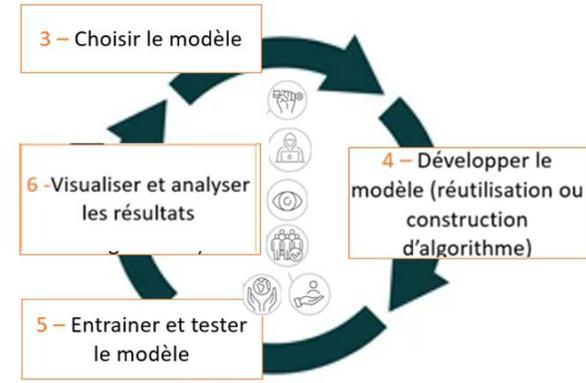
Respect de la vie privée et gouvernance des données

Gouvernance des données : Qualité, précision, validité, etc.
Traçabilité de toute les opérations impactant les données et des responsabilités associées



Non-discrimination, équité et diversité

Equité des données vis-à-vis des populations impliquées
Data Ethics et biais statistiques





Enjeu n°2 : Le système d'IA de confiance

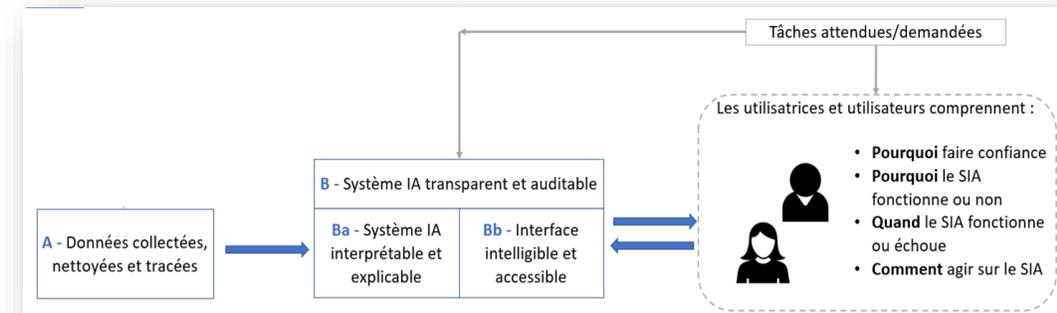
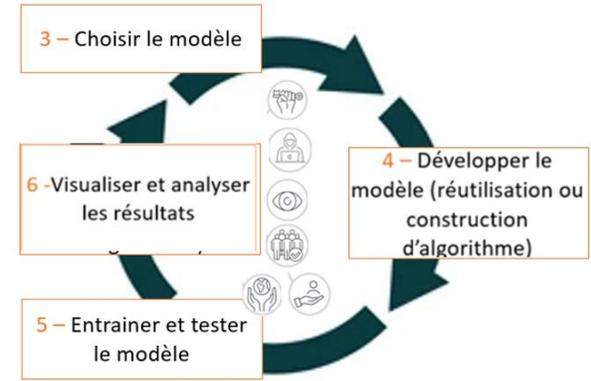
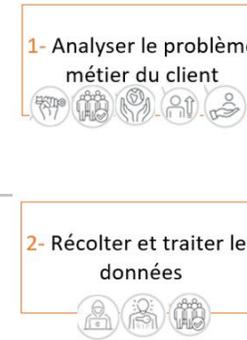
Les étapes 3, 4 et 5 sont associés au résultat Ba « système IA interprétable et explicable », pour cela il faut :

- Proposer un modèle ou ensemble de modèles :
- Selon un **compromis performance / consommation** énergétique (puissance de calcul et budget client)
 - Selon un **compromis explicabilité / contraintes métier**

Attention au contexte d'utilisation : système critique?
Comportement en temps réel?

Tracer les actions et responsabilités en lien avec le choix du modèle et de ses caractéristiques (nombre de paramètres, architecture) et de ses phases d'entraînement et de test

Audit des modèles existants et accompagner aux certifications de ces modèles lorsque possible





Exemple de méthode non technique: Model Card

« Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., ... & Gebru, T. (2019, January). Model cards for model reporting. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 220-229). »

Model Card

- **Model Details.** Basic information about the model.
 - Person or organization developing model
 - Model date
 - Model version
 - Model type
 - Information about training algorithms, parameters, fairness constraints or other applied approaches, and features
 - Paper or other resource for more information
 - Citation details
 - License
 - Where to send questions or comments about the model
- **Intended Use.** Use cases that were envisioned during development.
 - Primary intended uses
 - Primary intended users
 - Out-of-scope use cases
- **Factors.** Factors could include demographic or phenotypic groups, environmental conditions, technical attributes, or others listed in Section 4.3.
 - Relevant factors
 - Evaluation factors
- **Metrics.** Metrics should be chosen to reflect potential real-world impacts of the model.
 - Model performance measures
 - Decision thresholds
 - Variation approaches
- **Evaluation Data.** Details on the dataset(s) used for the quantitative analyses in the card.
 - Datasets
 - Motivation
 - Preprocessing
- **Training Data.** May not be possible to provide in practice. When possible, this section should mirror Evaluation Data. If such detail is not possible, minimal allowable information should be provided here, such as details of the distribution over various factors in the training datasets.
- **Quantitative Analyses**
 - Unitary results
 - Intersectional results
- **Ethical Considerations**
- **Caveats and Recommendations**

Figure 1: Summary of model card sections and suggested prompts for each.

Model Card - Smiling Detection in Images

Model Details

- Developed by researchers at Google and the University of Toronto, 2018, v1.
- Convolutional Neural Net.
- Pretrained for face recognition then fine-tuned with cross-entropy loss for binary smiling classification.

Intended Use

- Intended to be used for fun applications, such as creating cartoon smiles on real images; augmentative applications, such as providing details for people who are blind; or assisting applications such as automatically finding smiling photos.
- Particularly intended for younger audiences.
- Not suitable for emotion detection or determining affect; smiles were annotated based on physical appearance, and not underlying emotions.

Factors

- Based on known problems with computer vision face technology, potential relevant factors include groups for gender, age, race, and Fitzpatrick skin type; hardware factors of camera type and lens type; and environmental factors of lighting and humidity.
- Evaluation factors are gender and age group, as annotated in the publicly available dataset CelebA [36]. Further possible factors not currently available in a public smiling dataset. Gender and age determined by third-party annotators based on visual presentation, following a set of examples of male/female gender and young/old age. Further details available in [36].

Metrics

- Evaluation metrics include **False Positive Rate** and **False Negative Rate** to measure disproportionate model performance errors across subgroups. **False Discovery Rate** and **False Omission Rate**, which measure the fraction of negative (not smiling) and positive (smiling) predictions that are incorrectly predicted to be positive and negative, respectively, are also reported. [48]
- Together, these four metrics provide values for different errors that can be calculated from the confusion matrix for binary classification systems.
- These also correspond to metrics in recent definitions of “fairness” in machine learning (cf. [6, 26]), where parity across subgroups for different metrics correspond to different fairness criteria.
- 95% confidence intervals calculated with bootstrap resampling.
- All metrics reported at the .5 decision threshold, where all error types (FPR, FNR, FDR, FOR) are within the same range (0.04 - 0.14).

Training Data

- CelebA [36], training data split.

Evaluation Data

- CelebA [36], test data split.
- Chosen as a basic proof-of-concept.

Ethical Considerations

- Faces and annotations based on public figures (celebrities). No new information is inferred or annotated.

Caveats and Recommendations

- Does not capture race or skin type, which has been reported as a source of disproportionate errors [5].
- Given gender classes are binary (male/not male), which we include as male/female. Further work needed to evaluate across a spectrum of genders.
- An ideal evaluation dataset would additionally include annotations for Fitzpatrick skin type, camera details, and environment (lighting/humidity) details.

Quantitative Analyses

The figure contains four dot plots, each showing a metric across demographic groups: old-male, old-female, young-female, young-male, old, young, male, female, and all. Each plot includes a central dot representing the mean value and horizontal error bars representing 95% confidence intervals. The x-axis for all plots ranges from 0.00 to 0.14.

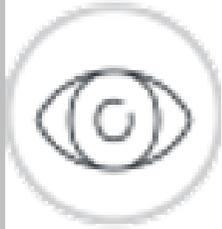
- False Positive Rate @ 0.5:** Values range from approximately 0.04 to 0.10.
- False Negative Rate @ 0.5:** Values range from approximately 0.04 to 0.10.
- False Discovery Rate @ 0.5:** Values range from approximately 0.04 to 0.10.
- False Omission Rate @ 0.5:** Values range from approximately 0.04 to 0.10.

Figure 2: Example Model Card for a smile detector trained and evaluated on the CelebA dataset.



Enjeu n°3 : l'interaction Humain- Machine

L'étape 6 est associée au résultat Bb « Interface intelligente et accessible », pour cela il faut:



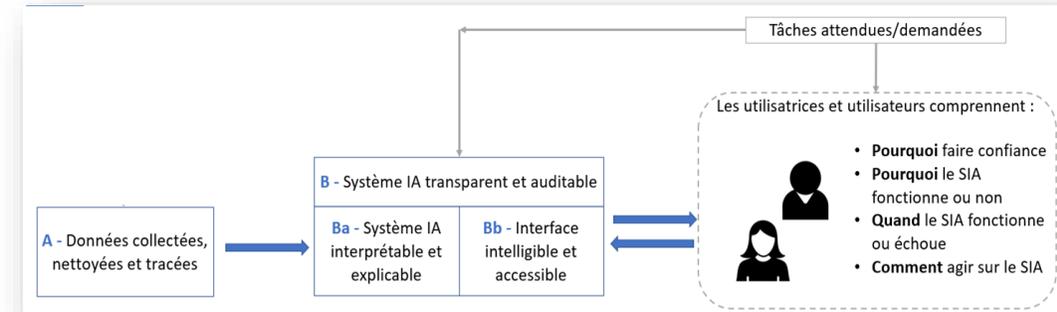
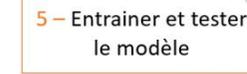
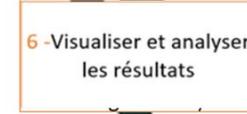
Transparence

Génération d'explications intelligentes pour les équipes techniques et les utilisateurs



Non-discrimination, équité et diversité

Accessibilité et conception personnalisée :
Interface prenant en compte les besoins cognitifs
et physique des utilisateurs



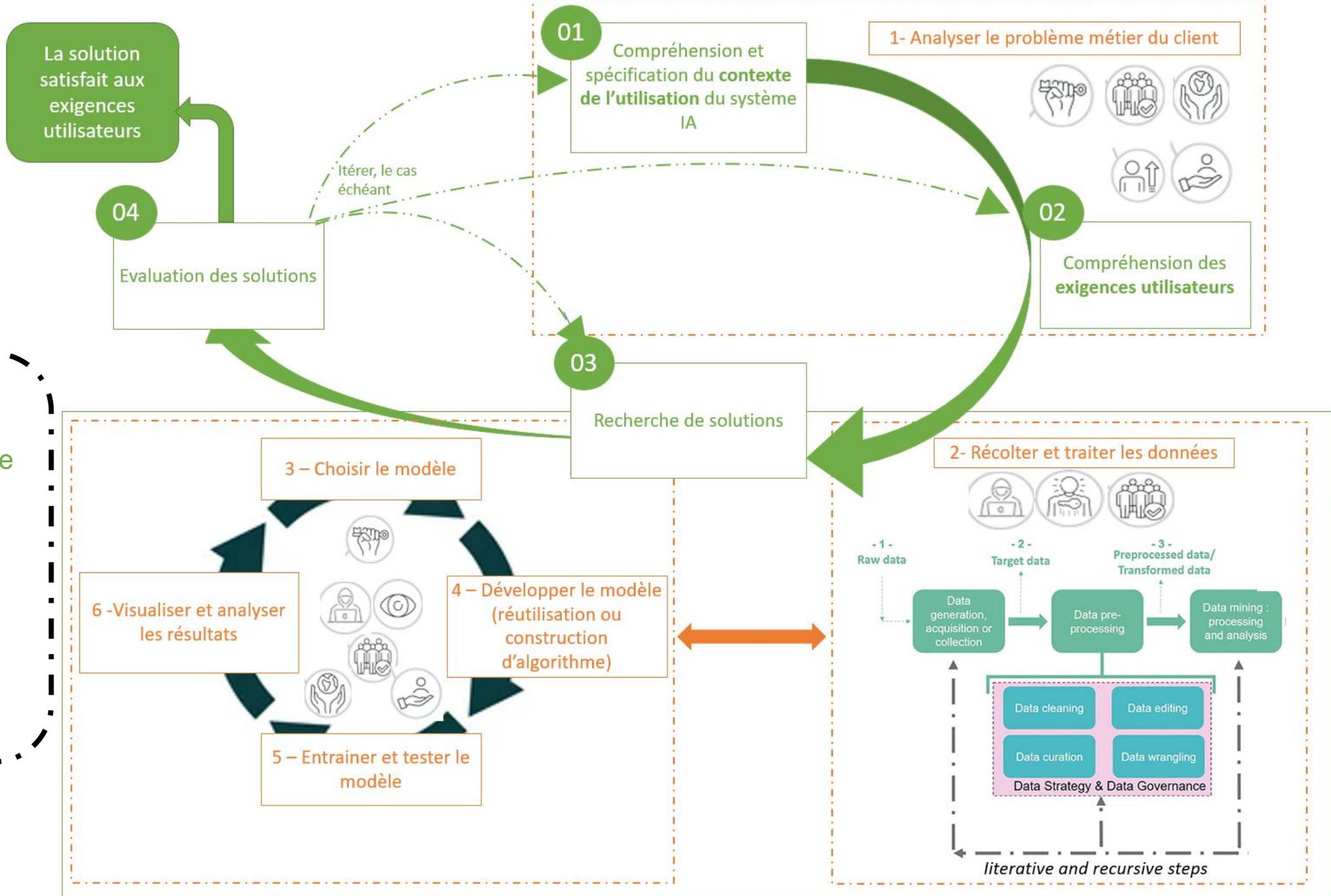


En résumé

Légende:

En vert les 4 étapes de la conception centrée utilisateur (norme iso 9241-2101)

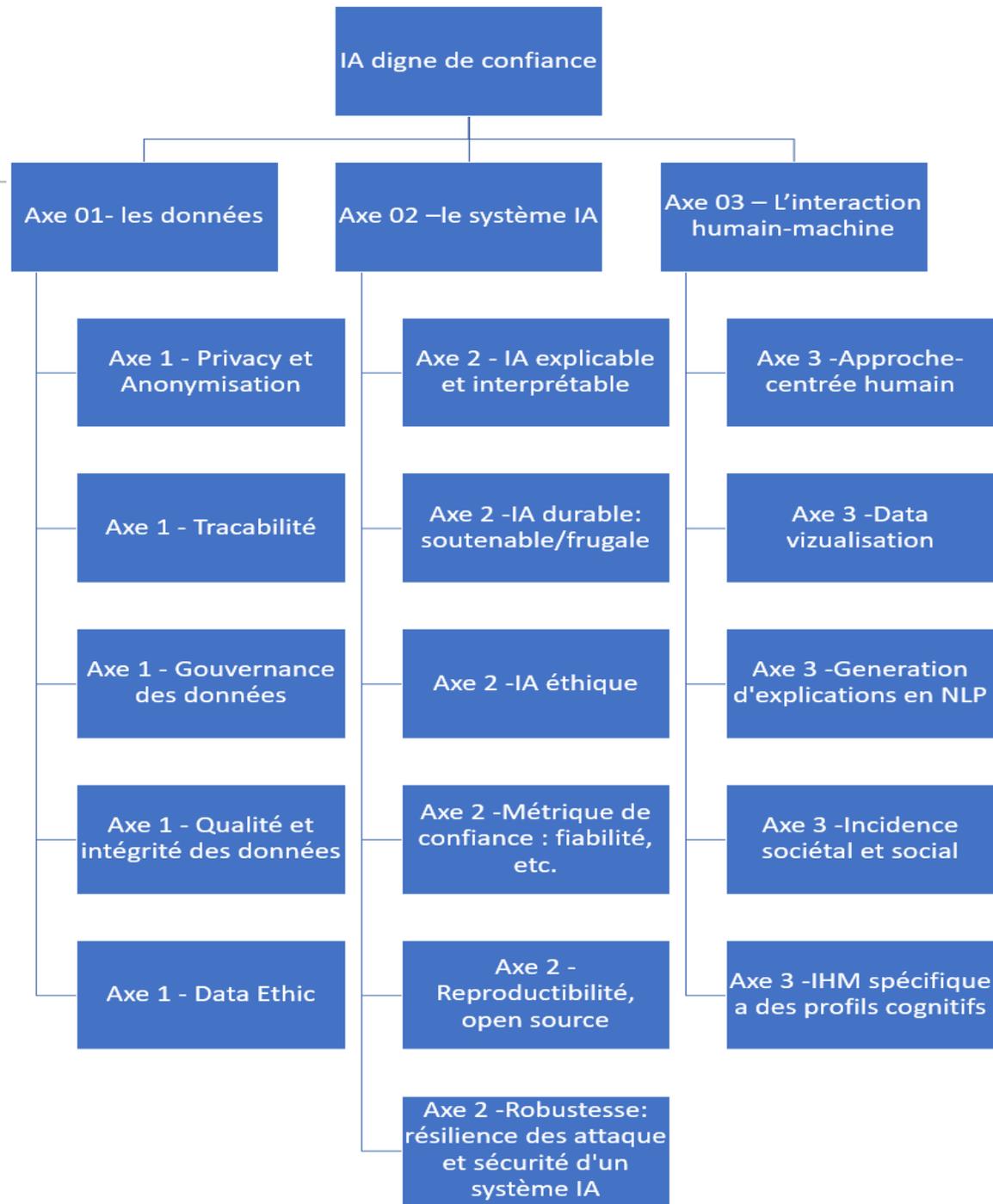
En orange, les étapes du cycle de vie d'un projet IA (développement)



La solution satisfait aux exigences utilisateurs

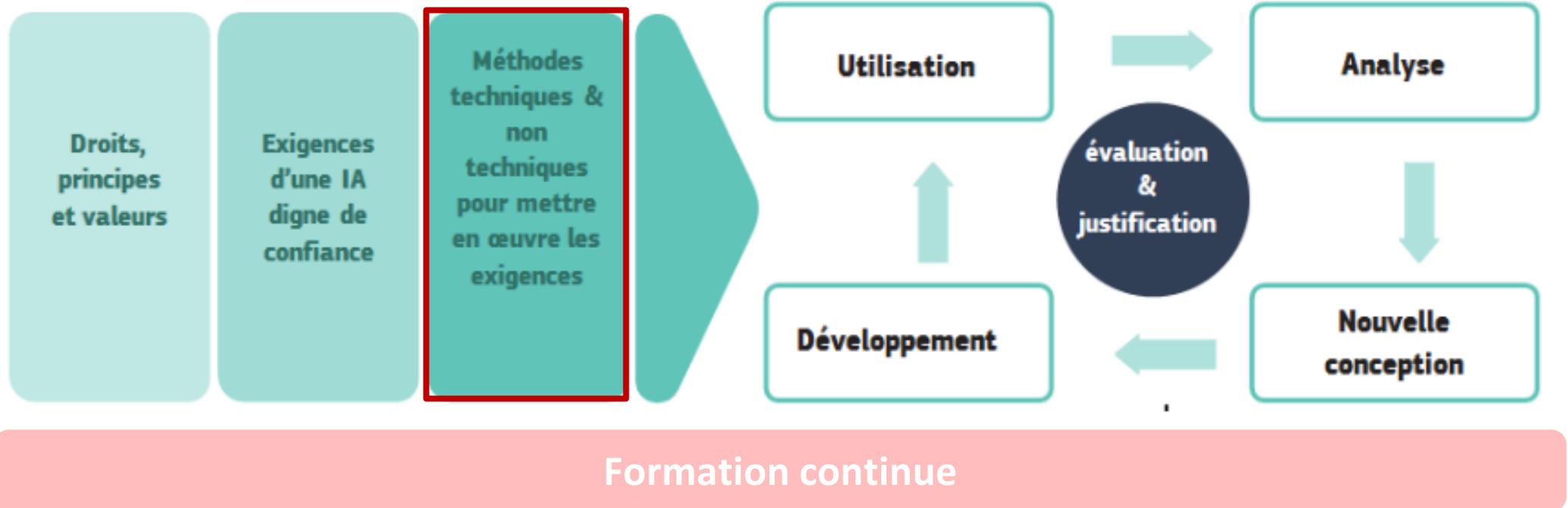


En résumé



L'IA digne de confiance, un processus continu

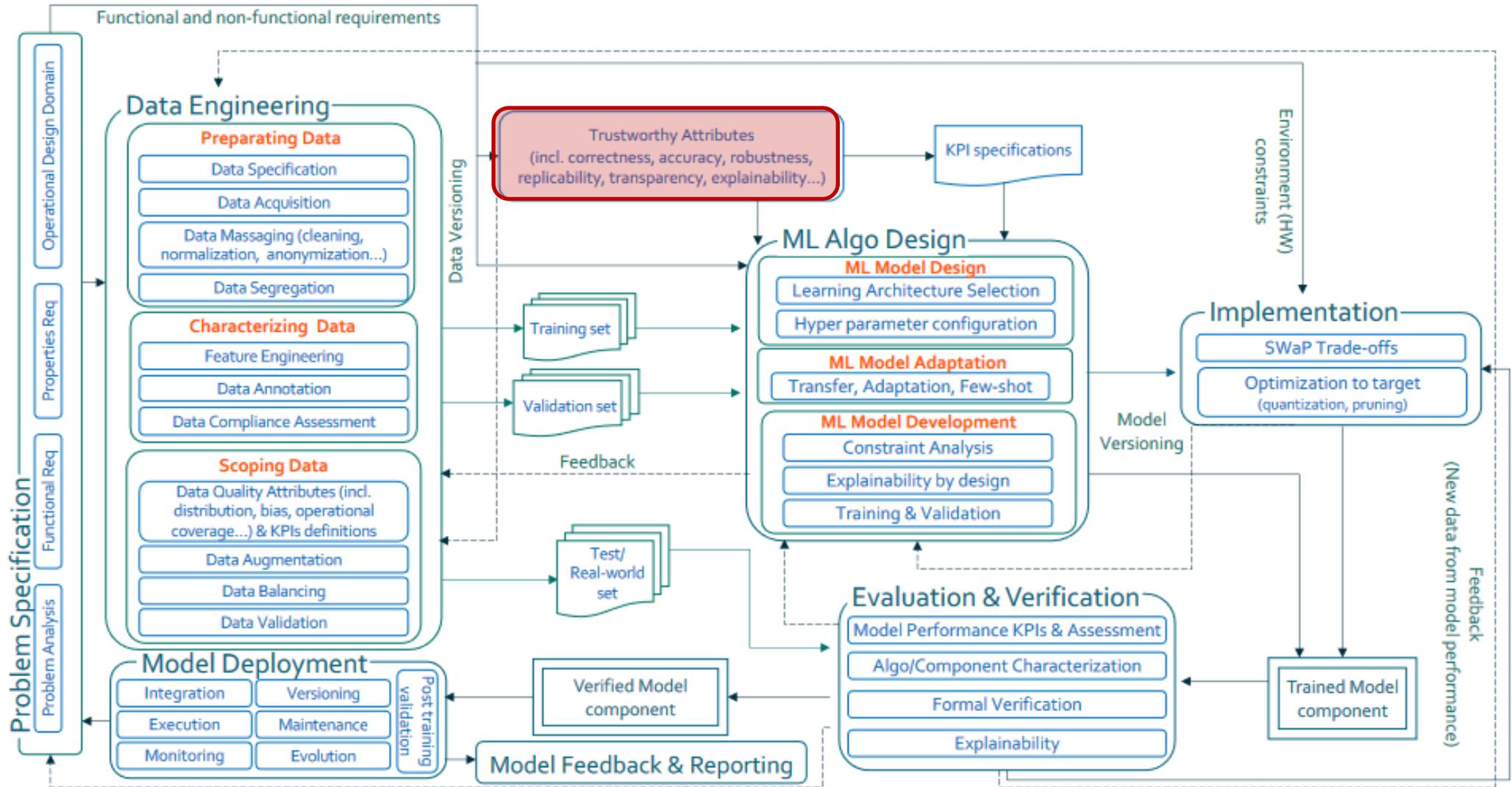
Parvenir à une IA digne de confiance **tout au long du cycle de vie du système IA**



> Image adaptée p.25 de « Ligne directrices en matière d'éthique pour une IA digne de confiance », juin 2018



Exemple de méthode technique : Pipeline d'ingénierie d'un système d'IA



Exemple Profil entreprise:

- PME de 40 personnes
- 20 ans d'existence
- A du personnel technique expert en Datascience et IA
- Produit et vend des tracteurs

Projets IA priorisés :

- IA comme composante de sécurité du tracteur
- Maintenance prédictive
- Inclure de l'IA générative pour la productivité (administratif)





Exemple de préconisations pour une IA digne confiance dans une entreprise

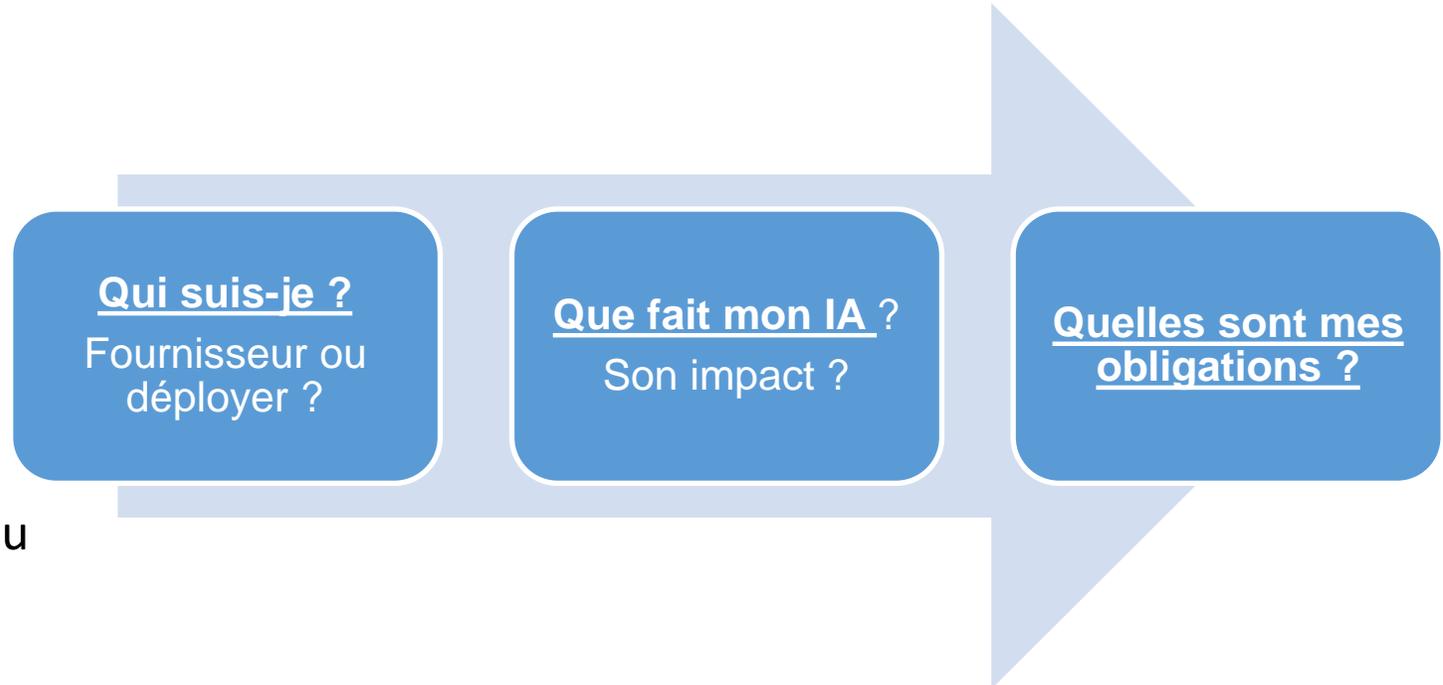
Exemple FICTIF à titre d'illustration

Exemple Profil entreprise:

- PME de 40 personnes
- 20 ans d'existence
- A du personnel technique expert en Datascience et IA
- Produit et vend des tracteurs

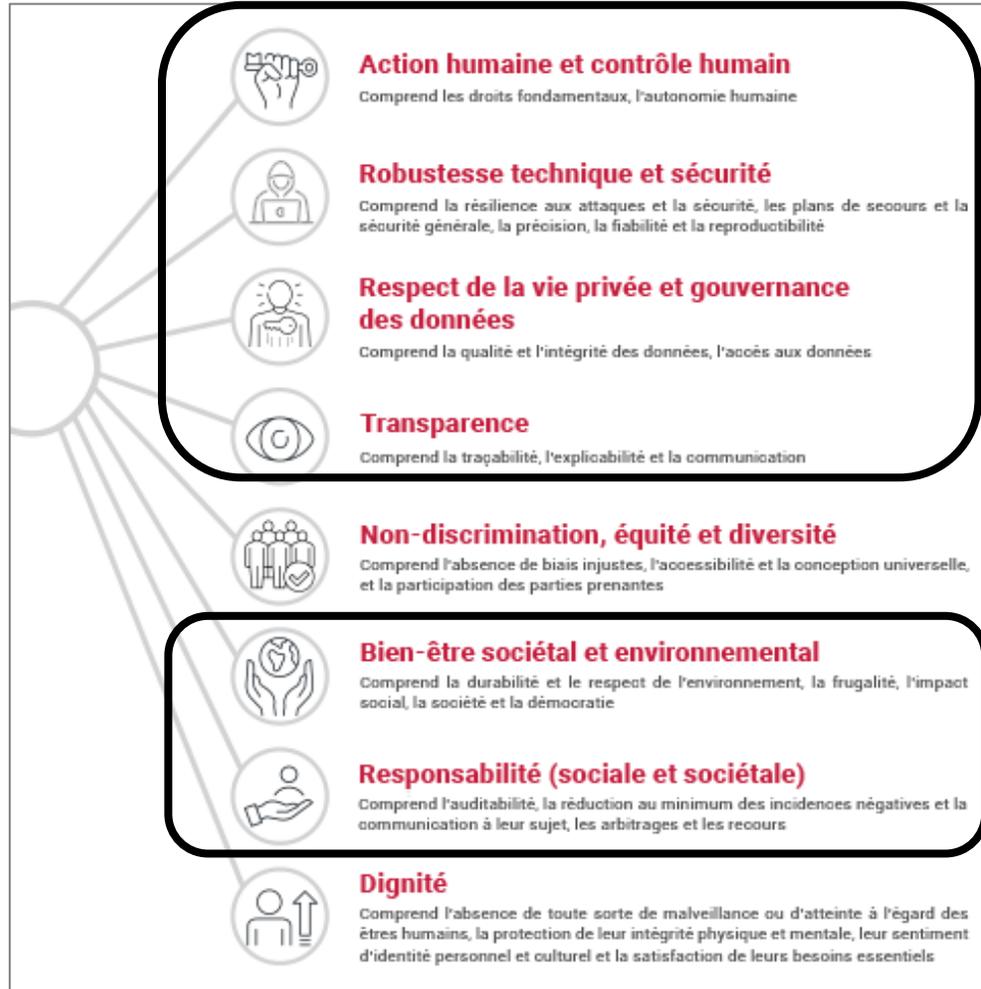
Projets IA priorisés :

- IA comme composante de sécurité du tracteur
- Maintenance prédictive
- Inclure de l'IA générative pour la productivité (administratif)



Ethique et IA digne de confiance :

Etape 1 – Détecter et prioriser les obligations



Le projet soulève plusieurs questions pour des SIA dignes de confiance.

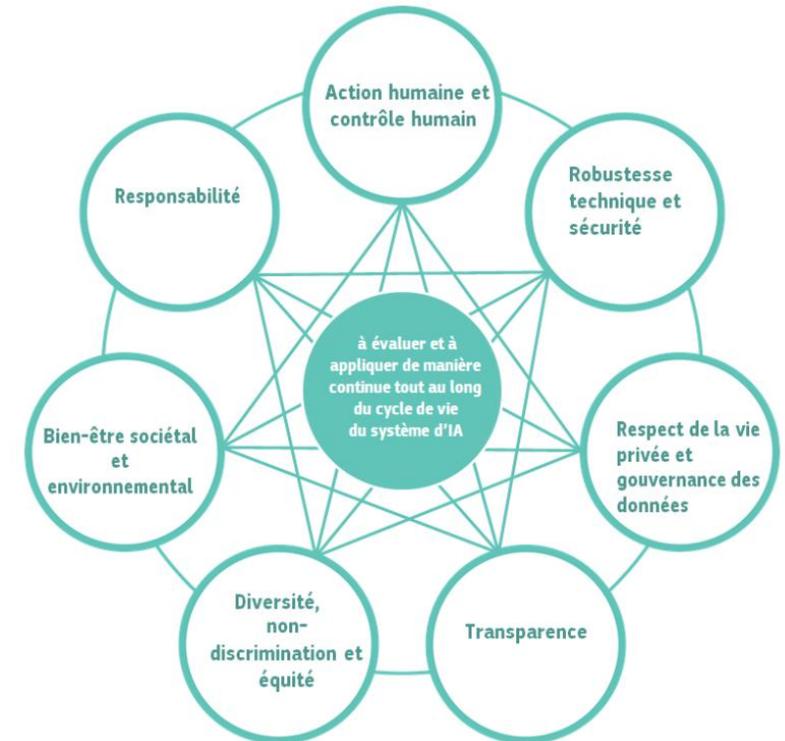
Lors du développement ultérieur des solutions attendues, le responsable doit être attentif à :

- (1) La robustesse , requérant un système sécurisé afin de veiller à la fiabilité des résultats et leur reproductibilité ainsi que la sécurité et sureté du SIA
- (2) La gouvernance des données permettra d'assurer la traçabilité, qualité et intégrité des données utilisées par les algorithmes de prises de décision
- (3) La transparence doit être inhérente au(x) SIA(s) qui doit également être explicable.
- (4) La responsabilisation
- (5) le contrôle humain

Conclusion

L'IA digne de confiance ...

- S'inscrit dans **la réalité métier**, RH, financière et socio-économique de l'entreprise
- Permet de responsabiliser et fédérer (documentation et traçabilité)
- Implique un ensemble de méthodes techniques et non techniques
- Nécessite un processus d'amélioration continue (i.e formation continue)





Charte Dihynamic Intelligence Artificielle de Confiance & Éthique pour le Numérique



Action humaine et contrôle humain
Comprend les droits fondamentaux, l'autonomie humaine



Robustesse technique et sécurité
Comprend la résilience aux attaques et la sécurité, les plans de secours et la sécurité générale, la précision, la fiabilité et la reproductibilité



Respect de la vie privée et gouvernance des données
Comprend la qualité et l'intégrité des données, l'accès aux données



Transparence
Comprend la traçabilité, l'explicabilité et la communication



Non-discrimination, équité et diversité
Comprend l'absence de biais injustes, l'accessibilité et la conception universelle, et la participation des parties prenantes



Bien-être sociétal et environnemental
Comprend la durabilité et le respect de l'environnement, la frugalité, l'impact social, la société et la démocratie



Responsabilité (sociale et sociétale)
Comprend l'auditabilité, la réduction au minimum des incidences négatives et la communication à leur sujet, les arbitrages et les recours



Dignité
Comprend l'absence de toute sorte de malveillance ou d'atteinte à l'égard des êtres humains, la protection de leur intégrité physique et mentale, leur sentiment d'identité personnel et culturel et la satisfaction de leurs besoins essentiels



www.dihynamic.eu

CONTACT



Ikram CHRAIBI KAADOUD
INRIA
Ikram.chraibi-kaadoud@inria.fr

© 2025 Nouvelle-Aquitaine - Mar 2025 | Tous droits réservés | Financé par l'Union européenne

CONTACTS :



Vincent Jourden
victorjourdren@orange.fr



Ikram Chraibi Kaadoud
ikram.chraibi-kaadoud@inria.fr
<https://ikramchraibik.com/>



Dihynamic
contact@dihynamic.eu



www.dihynamic.eu



DIHNAMIC



@dihynamic



Cofinancé par
l'Union européenne



RÉGION
Nouvelle-
Aquitaine

Projet cofinancé par la
Région Nouvelle-Aquitaine





Charte Dihynamic Intelligence Artificielle de Confiance & Éthique pour le Numérique



Action humaine et contrôle humain
Comprend les droits fondamentaux, l'autonomie humaine



Robustesse technique et sécurité
Comprend la résilience aux attaques et la sécurité, les plans de secours et la sécurité générale, la précision, la fiabilité et la reproductibilité



Respect de la vie privée et gouvernance des données
Comprend la qualité et l'intégrité des données, l'accès aux données



Transparence
Comprend la traçabilité, l'explicabilité et la communication



Non-discrimination, équité et diversité
Comprend l'absence de biais injustes, l'accessibilité et la conception universelle, et la participation des parties prenantes



Bien-être sociétal et environnemental
Comprend la durabilité et le respect de l'environnement, la frugalité, l'impact social, la société et la démocratie



Responsabilité (sociale et sociétale)
Comprend l'auditabilité, la réduction au minimum des incidences négatives et la communication à leur sujet, les arbitrages et les recours



Dignité
Comprend l'absence de toute sorte de malveillance ou d'atteinte à l'égard des êtres humains, la protection de leur intégrité physique et mentale, leur sentiment d'identité personnel et culturel et la satisfaction de leurs besoins essentiels



www.dihynamic.eu

CONTACT



Ikram CHRAIBI KAADOUD
INRIA
Ikram.chraibi-kaadoud@inria.fr

© 2025 Nouvelle-Aquitaine - Mar 2025 | Tous droits réservés | Financé par l'Union européenne

CONTACTS :



Vincent Jourden
victorjourdren@orange.fr



Ikram Chraibi Kaadoud
ikram.chraibi-kaadoud@inria.fr
<https://ikramchraibik.com/>



Dihynamic
contact@dihynamic.eu



www.dihynamic.eu



DIHNAMIC



@dihynamic



Cofinancé par
l'Union européenne



RÉGION
Nouvelle-
Aquitaine

Projet cofinancé par la
Région Nouvelle-Aquitaine

