Lexique des notions clés

27 notions - Droit , éthique et responsabilité

Catégories

- **Fil rouge du cours** (1 notion)
- **Conformité & Réglementation** (9 notions)
- **Droits & Libertés** (4 notions)
- **Gouvernance juridique** (5 notions)
- **Responsabilité** (3 notions)
- **Secteurs régulés** (3 notions)
- **Souveraineté & Dépendance** (2 notions)

Glossaire - ordre alphabétique

AI Act - *Conformité & Réglementation*

Réglementation européenne sur l'IA (en vigueur depuis août 2024) classifiant les systèmes d'IA par niveau de risque et imposant des obligations proportionnelles : interdiction, haut risque, risque limité, risque minimal.

A noter : *Quatre niveaux. Les usages RH, santé, crédit et éducation sont classifiés haut risque et soumis à des obligations renforcées d'audit, de documentation et de supervision humaine.*

Algorithme de décision automatisée - *Responsabilité*

Système qui prend ou influence des décisions sans intervention humaine directe, à partir de données et de règles préétablies.

A noter : *Toute décision automatisée impactant une personne doit pouvoir être expliquée et contestée. C'est une obligation légale sous le RGPD et l'AI Act.*

Anonymisation - *Conformité & Réglementation*

Processus irréversible de suppression de tout lien entre une donnée et la personne qu'elle concerne. Une donnée anonymisée sort du champ du RGPD.

A noter : *À distinguer de la pseudonymisation qui est réversible. L'anonymisation complète est difficile à garantir avec des modèles d'IA avancés.*

Charte IA - *Gouvernance juridique*

Document interne qui définit les règles d'usage de l'IA dans une organisation : cas d'usage autorisés et interdits, responsabilités, supervision humaine, sanctions.

A noter : *Premier outil managérial concret pour encadrer le déploiement de l'IA. De plus en plus exigée par les directions juridiques et les comités de conformité.*

Cloud Act - *Souveraineté & Dépendance*

Loi américaine (2018) autorisant les autorités US à accéder aux données détenues par des opérateurs américains, même si les serveurs sont situés hors des Etats-Unis.

A noter : *Des données hébergées chez AWS, Azure ou Google Cloud peuvent être requises par le gouvernement américain sans notification préalable. Ce n'est pas qu'un sujet politique - c'est une responsabilité juridique.*

Conformité (Compliance) - *Conformité & Réglementation*

Respect de l'ensemble des obligations légales, réglementaires et normatives applicables à une organisation dans ses usages de l'IA.

A noter : *La conformité n'est pas une contrainte administrative - c'est un outil de décision qui conditionne ce qui est possible. Un projet non conforme n'est pas abandonné, il est recadré.*

Consentement - *Conformité & Réglementation*

Base légale du RGPD permettant le traitement de données personnelles lorsque la personne concernée a donné son accord libre, éclairé, spécifique et univoque.

A noter : *Le consentement doit couvrir l'usage précis. Entraîner un modèle sur des données RH collectées à d'autres fins sans nouveau consentement constitue un détournement de finalité.*

DORA - *Secteurs régulés*

Digital Operational Resilience Act. Règlement européen en application depuis janvier 2025 imposant aux institutions financières des exigences strictes de résilience opérationnelle numérique.

A noter : *Couvre les banques, assurances et sociétés d'investissement. Impose l'audit des prestataires IA, des tests de résilience et une gouvernance renforcée des risques informatiques.*

DPO - Délégué à la Protection des Données - *Gouvernance juridique*

Rôle obligatoire pour les organisations traitant des données personnelles à grande échelle. Garant de la conformité RGPD en interne, interlocuteur de la CNIL.

A noter : *Tout projet IA impliquant des données personnelles doit être soumis au DPO avant lancement. L'ignorer expose l'organisation à des sanctions et le manager à une responsabilité personnelle.*

Droit à l'explication - *Droits & Libertés*

Droit de toute personne impactée par une décision automatisée d'obtenir une explication sur la logique et les critères utilisés par le système d'IA.

A noter : *Obligation légale sous le RGPD (article 22) et renforcée par l'AI Act pour les systèmes à haut risque. Question centrale : comment expliquer une décision prise par un modèle que l'on ne comprend pas soi-même ?*

Droit à l'oubli - *Droits & Libertés*

Droit d'une personne de demander la suppression de ses données personnelles des systèmes d'une organisation, y compris des modèles d'IA entraînés sur ces données.

A noter : *Difficile à mettre en oeuvre pour les modèles d'IA. Comment 'oublier' une donnée d'un modèle déjà entraîné ? Un problème technique et juridique non encore résolu.*

Finalité - *Conformité & Réglementation*

Principe du RGPD imposant que les données personnelles ne soient collectées que pour des objectifs précis, explicites et légitimes, et ne soient pas utilisées de façon incompatible avec ces objectifs.

A noter : *Utiliser des données clients collectées pour la facturation pour entraîner un modèle de recommandation constitue un détournement de finalité illégal.*

HDS - Hébergement de Données de Santé - *Secteurs régulés*

Certification obligatoire en France pour toute organisation qui héberge, traite ou exploite des données de santé à caractère personnel.

A noter : *Un projet IA sur des données patients sans hébergeur certifié HDS est illégal en France. Les données de santé constituent la catégorie la plus protégée du RGPD.*

IA à haut risque - *Conformité & Réglementation*

Sous l'AI Act, systèmes d'IA déployés dans des domaines sensibles (RH, santé, crédit, éducation, infrastructure critique, justice) soumis à des obligations renforcées d'audit et de supervision.

A noter : *Avant tout déploiement : évaluation de conformité, documentation technique, inscription au registre européen, supervision humaine obligatoire. Ces cas d'usage sont exactement ceux dans lesquels vous allez travailler.*

IA interdite - *Conformité & Réglementation*

Sous l'AI Act, systèmes d'IA dont le déploiement est strictement interdit sur le territoire européen en raison du risque inacceptable qu'ils représentent.

A noter : *Exemples : notation sociale généralisée des citoyens, manipulation cognitive subliminale, reconnaissance biométrique en temps réel dans l'espace public (sauf exceptions sécurité nationale).*

Minimisation des données - *Conformité & Réglementation*

Principe du RGPD imposant de ne collecter et traiter que les données strictement nécessaires à la finalité déclarée. Toute donnée supplémentaire constitue une exposition juridique.

A noter : *Contre-intuitif dans le contexte de l'IA où 'plus de données = meilleur modèle'. La minimisation impose une discipline de sélection rigoureuse avant tout projet.*

Privacy by Design - *Gouvernance juridique*

Principe imposant d'intégrer la protection des données personnelles dès la conception d'un système ou d'un projet, et non en correction a posteriori.

A noter : *Obligation légale sous le RGPD (article 25). En pratique : consulter le DPO dès le cadrage du projet IA, pas après le développement.*

Propriété intellectuelle et IA - *Droits & Libertés*

Ensemble des droits relatifs aux créations intellectuelles appliqués aux contenus générés par ou avec l'IA, ainsi qu'aux données utilisées pour entraîner les modèles.

A noter : *Qui est l'auteur d'un texte co-écrit avec ChatGPT ? Le contenu produit par une IA est-il protégeable ? Ces questions ne sont pas encore tranchées définitivement par le droit.*

Pseudonymisation - *Conformité & Réglementation*

Traitement réversible des données personnelles permettant de ne plus les attribuer directement à une personne sans information supplémentaire. Les données pseudonymisées restent dans le champ du RGPD.

A noter : *A distinguer de l'anonymisation qui est irréversible. La pseudonymisation réduit les risques mais ne dispense pas des obligations RGPD.*

Registre des traitements - *Gouvernance juridique*

Document obligatoire sous le RGPD recensant l'ensemble des traitements de données personnelles réalisés par une organisation : finalité, données traitées, durée de conservation, destinataires.

A noter : *Tout projet IA impliquant des données personnelles doit être inscrit au registre. C'est le premier document demandé en cas de contrôle CNIL.*

Responsabilité algorithmique - *Responsabilité*

Obligation pour une organisation de rendre compte des décisions prises ou influencées par ses systèmes d'IA, d'en assumer les conséquences et de mettre en place des mécanismes de correction.

A noter : *La responsabilité ne se délègue pas au modèle. L'organisation qui déploie et le manager qui signe restent responsables des décisions produites - y compris des erreurs.*

RGPD - *Conformité & Réglementation*

Règlement Général sur la Protection des Données. Règlement européen (2018) encadrant la collecte, le traitement et la conservation des données personnelles des résidents européens.

A noter : *Sanctions jusqu'à 4% du chiffre d'affaires mondial. Avant tout projet IA impliquant des données personnelles : vérifier la finalité, le consentement et la durée de conservation.*

SecNumCloud - *Souveraineté & Dépendance*

Certification délivrée par l'ANSSI attestant du niveau de sécurité et de la non-dépendance à des acteurs étrangers d'un prestataire de services cloud.

A noter : *Référence pour les organisations souhaitant héberger des données sensibles sur un cloud souverain. Scaleway, OVH, Bleu (Microsoft) et Sens (Google) sont parmi les acteurs certifiés ou en cours.*

Secteurs régulés et IA - *Secteurs régulés*

Secteurs disposant de cadres réglementaires spécifiques qui s'ajoutent au RGPD et à l'AI Act : santé (HDS), finance (DORA, ACPR), énergie, transport, défense, secteur public.

A noter : *Travailler dans un secteur régulé signifie naviguer entre plusieurs couches de conformité simultanément. Le manager doit connaître le cadre sectoriel de son organisation avant tout projet IA.*

Supervision humaine - *Responsabilité*

Obligation légale pour les systèmes d'IA à haut risque de maintenir un contrôle humain effectif sur les décisions produites, avec capacité d'intervention et d'interruption.

A noter : *La supervision humaine n'est pas symbolique. Elle implique que l'humain comprend la décision, peut la contester et dispose d'un 'kill switch' en cas de dérive du modèle.*

Traçabilité - *Gouvernance juridique*

Capacité à retracer l'historique complet d'une donnée ou d'une décision produite par un système d'IA : origine des données, transformations subies, résultats produits.

A noter : *Obligation pour les systèmes à haut risque sous l'AI Act. Sans traçabilité, impossible de prouver la conformité en cas de contrôle ou de litige.*

Transparence algorithmique - *Droits & Libertés*

Obligation d'informer les utilisateurs de l'existence et du fonctionnement d'un système d'IA, notamment lorsqu'il produit des décisions ou génère du contenu les concernant.

A noter : *Obligation légale sous l'AI Act pour les systèmes à risque limité (chatbots, deepfakes). Le silence sur l'usage de l'IA constitue une violation réglementaire.*

Valeur x Risque x Dépendance - *Fil rouge du cours*

Grille d'analyse du cours pour évaluer tout outil ou projet IA selon trois dimensions simultanées : la valeur créée, le risque juridique et opérationnel exposé, la dépendance induite.

A noter : *En séance 4, le risque prend une dimension juridique concrète. RGPD, AI Act, responsabilité managériale - ce sont les composantes du risque que tout manager doit évaluer avant de signer.*