Intelligence artificielle et protection des données personnelles : analyse des législations suisse et européenne

DIAA AL HARIRI

10/24/25

Contents

Introduction

À l'ère du numérique, l'intelligence artificielle (IA) est devenue une composante essentielle de notre vie quotidienne. Elle s'intègre dans une multitude d'applications, allant des assistants personnels intelligents aux systèmes avancés de recommandation. Cette expansion rapide soulève toutefois des interrogations majeures concernant son impact sur la vie privée et la protection des données personnelles.

En Suisse, la **nouvelle Loi fédérale sur la protection des données (nLPD)**, entrée en vigueur le **1er septembre 2023**, renforce le cadre juridique afin de mieux protéger la vie privée face aux défis engendrés par l'utilisation croissante de l'IA. Cette loi met un accent particulier sur la **transparence**, la **minimisation des données** et le **respect des droits individuels** dans le traitement des informations personnelles. Elle impose ainsi aux entreprises et institutions une **conformité stricte** à ces principes.

Cependant, l'application de ces règles aux technologies d'intelligence artificielle demeure complexe. Les **algorithmes opaques**, la **difficulté d'interprétation des modèles** et le **manque de transparence** dans certains traitements de données rendent le contrôle juridique plus ardu. Des enquêtes menées sur l'utilisation des données des utilisateurs pour l'entraînement des modèles d'IA soulignent la nécessité d'une **application rigoureuse et efficace** de la loi pour garantir la protection des individus.

Ce travail vise à **analyser l'impact de l'intelligence artificielle sur la protection des données personnelles** en Suisse. Il mettra en lumière les **principaux défis** liés à la mise en œuvre de la nLPD face à l'IA, et proposera des **stratégies concrètes** permettant aux utilisateurs de mieux préserver leur vie privée dans un monde technologique en constante évolution.

Partie légale : Lois suisses et européennes

1. Loi fédérale suisse sur la protection des données (nLPD)

La **Loi fédérale suisse sur la protection des données révisée (nLPD)** est entrée en vigueur le **1er septembre 2023**, remplaçant l'ancienne loi (FADP) en vigueur depuis 1992.

Cette révision a pour objectif de **renforcer la protection des données personnelles** en Suisse, notamment face aux **avancées rapides des technologies numériques** telles que l'intelligence artificielle (IA).

Les principaux aspects de la nLPD sont les suivants :

- **Renforcement des droits des individus** : introduction de droits élargis, tels que le droit d'accès, de rectification et de suppression des données personnelles.
- **Transparence et consentement** : exigence d'un **consentement explicite et éclairé**, accompagné d'informations claires sur les finalités du traitement des données.
- **Responsabilité et reddition de comptes** : les entreprises sont désormais **pleinement responsables** de la protection des données qu'elles traitent et doivent suivre des **procédures précises** en cas de violation.
- **Conformité aux normes internationales** : la loi établit un **niveau de protection équivalent aux standards européens**, facilitant ainsi les **échanges de données entre la Suisse et l'Union européenne (UE)**.

2. Règlement général sur la protection des données (RGPD)

Le **Règlement général sur la protection des données (RGPD)**, adopté par l'**Union européenne** le **25 mai 2018**, constitue l'une des législations les plus strictes au monde en matière de confidentialité et de protection des données personnelles.

Il vise à **protéger les droits fondamentaux des individus** au sein de l'UE et à **garantir un contrôle accru** sur leurs informations personnelles.

Les principales caractéristiques du RGPD sont les suivantes :

- **Portée étendue** : le règlement s'applique à **toute entreprise** ou organisation offrant des produits ou services à des résidents de l'Union européenne, **indépendamment de son lieu d'établissement**.
- **Droits renforcés des individus** : les personnes concernées disposent de droits essentiels tels que **l'accès**, la **rectification**, la **suppression**, **l'opposition** et la **portabilité** de leurs données.
- **Consentement explicite** : tout traitement de données requiert un **consentement clair, spécifique et informé** de la part de l'utilisateur.
- **Mesures de sécurité et notification** : les entreprises ont l'obligation de **protéger les données** par des moyens techniques et organisationnels adaptés, et de **signaler toute violation** de données dans un délai de **72 heures**.
- **Sanctions sévères** : les infractions peuvent entraîner des **amendes allant jusqu'à 20 millions d'euros** ou **4 % du chiffre d'affaires annuel mondial**, selon le montant le plus élevé.

3. Tableau Comparatif : nLPD et RGPD

Norme	nLPD (Suisse)	RGPD (UE)
Portée	Entreprises en Suisse et hors Suisse traitant des données suisses	Toutes les entreprises traitant des données dans l'UE
Droits des individus	Accès, correction, suppression	Accès, correction, suppression, opposition, portabilité
Consentement	Consentement clair et éclairé	Consentement explicite et spécifique
Sanctions	Amendes et mesures légales	Amendes jusqu'à 4 % du chiffre d'affaires ou 20 millions d'euros
Conformité internationale	Compatible avec le RGPD	Norme de référence dans l'UE

4. Relation entre la nLPD et le RGPD

Bien que la **Suisse** ne soit pas membre de l'**Union européenne**, la **nouvelle Loi fédérale sur la protection des données (nLPD)** a été élaborée de manière à être **largement compatible avec le Règlement général sur la protection des données (RGPD)**.

Cette compatibilité vise à **faciliter les échanges de données** entre la Suisse et les États membres de l'UE, tout en **assurant un niveau équivalent de protection** pour les individus. Elle contribue également à **renforcer la confiance internationale** dans le traitement des données personnelles et positionne la **Suisse comme un centre fiable et sécurisé** pour la gestion et le transfert de données en Europe.

Partie technique : Impact des outils d'intelligence artificielle sur la vie privée

Avec la **propagation rapide de l'intelligence artificielle (IA)** dans tous les domaines de la vie moderne — des **smartphones** aux **voitures autonomes**, en passant par les **assistants virtuels** — la **quantité de données personnelles collectées, stockées et analysées** connaît une croissance exponentielle. L'IA s'appuie sur le **Big Data** et les **modèles d'apprentissage automatique (Machine Learning)** pour prédire le comportement des utilisateurs et optimiser les services offerts. Cependant, cette dépendance aux données massives engendre de **grands défis en matière de vie privée, de sécurité numérique et d'éthique**.

1. Types de données collectées par l'IA

a. Données directes

- **Informations d'identification** : nom, adresse, numéro de téléphone, adresse e-mail.
- **Informations de paiement** : détails des cartes de crédit ou comptes bancaires.

b. Données comportementales

- **Habitudes de navigation** : historique de recherche, clics, interactions avec les applications ou sites web.
- **Utilisation des applications** : durée d'utilisation, fréquence d'accès et types de contenus consultés.

c. Données biométriques

- **Reconnaissance faciale** sur les smartphones ou les systèmes de vidéosurveillance.
- **Reconnaissance vocale** via des assistants intelligents tels qu'**Alexa** ou **Google Assistant**.
- **Empreintes digitales** et **mouvements oculaires** utilisés pour interagir avec des appareils ou renforcer la sécurité.

d. Données dérivées (Derived Data)

- **Inférences comportementales et psychologiques** issues de l'analyse des données brutes (personnalité, intérêts, préférences, habitudes).
- **Prévisions et analyses prédictives** utilisées pour la publicité ciblée, la recommandation de produits ou, parfois, la **manipulation du comportement des utilisateurs**.

2. Modes d'impact de l'intelligence artificielle sur la vie privée

L'intelligence artificielle influence la vie privée de multiples façons, principalement à travers la **collecte massive**, l'**analyse prédictive**, et l'**utilisation avancée de données personnelles et biométriques**. Ces mécanismes, bien qu'ils améliorent l'efficacité des services, soulèvent d'importants **risques éthiques et juridiques**.

a. Analyse de Big Data

Les systèmes d'IA exploitent des **volumes considérables de données** provenant de diverses sources telles que les **réseaux sociaux**, les **smartphones**, les **capteurs connectés** ou encore les **caméras de surveillance**.

Cette analyse permet aux entreprises d'**anticiper le comportement des utilisateurs** et d'améliorer leurs services. Cependant, elle peut également **révéler des informations sensibles** que les individus n'ont **jamais choisi de partager explicitement**, mettant ainsi en péril leur vie privée.

b. Systèmes de recommandation et personnalisation

Des plateformes populaires telles que **Netflix** ou **Spotify** utilisent des **algorithmes d'apprentissage automatique** pour établir des **profils détaillés** des utilisateurs.

Ces systèmes collectent en continu des données sur les **habitudes, préférences et comportements** afin d'offrir un contenu personnalisé.

Toutefois, cette personnalisation accrue comporte le risque de créer des **profils sensibles** pouvant être exploités à des fins **commerciales, politiques** ou de **manipulation ciblée**.

c. Traitement des données biométriques

L'utilisation de l'IA dans la **reconnaissance faciale** et **vocale** renforce les préoccupations en matière de **sécurité et de surveillance**.

Une **fuite de données biométriques** ou une **utilisation non autorisée** peut entraîner des conséquences graves telles que le **vol d'identité**, la **surveillance illégale** ou le **chantage numérique**.

d. Entraînement sur données personnelles

De nombreux modèles d'IA nécessitent de vastes ensembles de données pour l'apprentissage, parfois **sans le consentement explicite** des utilisateurs.

Par exemple, certains **modèles génératifs** (de texte ou d'images) sont entraînés à partir de **données réelles collectées en ligne**, soulevant des questions cruciales relatives à la **propriété des données** et à la **confidentialité**.

3. Défis techniques pour la protection de la vie privée

La mise en œuvre de l'intelligence artificielle pose plusieurs **défis techniques majeurs** en matière de **protection de la vie privée**. Ces difficultés concernent à la fois la **transparence des algorithmes**, la **sécurité des données**, et les **risques de discrimination** liés aux biais dans les modèles d'apprentissage.

a. Manque de transparence (Black-box AI)

Les algorithmes d'intelligence artificielle, en particulier ceux fondés sur le **deep learning**, fonctionnent souvent comme des **boîtes noires**. Leur complexité rend difficile la compréhension du **processus décisionnel interne**, aussi bien pour les utilisateurs que pour les développeurs. Ce manque de transparence complique la **vérification de la conformité légale et éthique** du traitement des données, et nuit à la **confiance du public** envers les systèmes d'IA.

b. Fuites et risques de sécurité

Les données personnelles sont fréquemment **stockées sur des serveurs externes** ou dans le **cloud**, ce qui augmente les risques de **piratage** ou d'**accès non autorisé**.

Des incidents tels que des **fuites massives de bases de données** ou le **piratage de services d'IA** utilisant des informations sensibles illustrent la vulnérabilité croissante des infrastructures numériques face aux cyberattaques.

c. Extraction non autorisée de données (Unauthorized Data Mining)

Certaines entreprises exploitent des **techniques d'exploration de données** pour collecter et analyser des informations **sans le consentement explicite** des utilisateurs.

Ce type de **minage de données non autorisé** constitue une **violation directe de la vie privée**. Des cas concrets concernent la **collecte illégale de données** sur les réseaux sociaux ou d'autres plateformes en ligne à des fins de **publicité ciblée** ou d'**entraînement de modèles d'IA**.

d. Risque de discrimination et biais

Les modèles d'intelligence artificielle reposent sur des ensembles de données souvent **incomplets ou déséquilibrés**, ce qui peut conduire à des **décisions biaisées**.

Ces biais peuvent se traduire par des pratiques discriminatoires, telles que le **refus de prêts bancaires**, d'**assurances**, ou d'**offres d'emploi** fondées sur le **sexe**, l'**âge** ou l'**origine ethnique**. Un tel phénomène soulève de **graves enjeux éthiques et juridiques**, remettant en question la **justice algorithmique** et la **protection des droits fondamentaux** des utilisateurs.

Exemples récents de fuites de données liées à l'intelligence artificielle

Les incidents récents démontrent que même les grandes entreprises mondiales ne sont pas à l'abri des **violations de données** liées à l'utilisation de systèmes d'intelligence artificielle. Ces cas illustrent la **nécessité d'une sécurité renforcée**, d'une **gestion rigoureuse des accès**, et d'une **surveillance continue des infrastructures numériques**.

1. McDonald's (juillet 2025)

En **juillet 2025**, **McDonald's** a été victime d'une **cyberattaque** ciblant sa plateforme de recrutement intelligente, **McHire**, qui repose sur l'intelligence artificielle pour analyser et sélectionner les candidatures.
L'incident a entraîné la **fuite des données personnelles de millions de candidats** à travers le monde. L'attaque ne résultait pas d'une faille technique complexe, mais d'un **manque de sécurisation de l'interface administrative** de la plateforme.

Cet événement met en évidence l'importance de **protéger les systèmes d'IA utilisés dans les processus de recrutement** et de **renforcer les contrôles d'accès internes**.

(Source : PKWARE®)

2. Snowflake (2024)

En **2024**, la société de stockage de données en nuage **Snowflake** a subi une **violation de sécurité majeure**. Des attaquants ont utilisé des **identifiants volés** pour accéder aux comptes de plusieurs clients importants, provoquant la **fuite de données sensibles** appartenant à des entreprises telles qu'**AT&T**, **Ticketmaster** et **Santander**.

Cet incident démontre l'importance de **sécuriser les identifiants d'accès**, d'**imposer l'authentification multifactorielle (MFA)** et de **surveiller activement les connexions suspectes** dans les systèmes basés sur l'IA et le cloud. *(Source : Cloud Security Alliance)*

4. Outils et techniques pour contrer les défis liés à la vie privée

Pour répondre aux **risques croissants liés à l'utilisation de l'intelligence artificielle**, plusieurs **méthodes et outils techniques** ont été développés afin de renforcer la protection des données personnelles et garantir la conformité légale.

a. Chiffrement (Encryption)

Le chiffrement permet de **protéger les données** à la fois **en transit** (pendant leur transfert sur les réseaux) et **au repos** (lorsqu'elles sont stockées sur des serveurs).

Cette technique empêche l'accès non autorisé aux informations sensibles et réduit le risque de fuite de données.

b. Apprentissage fédéré (Federated Learning)

L'**apprentissage fédéré** permet d'**entraîner des modèles d'IA** sur des données locales, **sans transférer les données brutes vers un serveur central**.

Cette approche réduit les risques liés à la centralisation des données et améliore la **confidentialité des utilisateurs** tout en maintenant l'efficacité des modèles.

c. Anonymisation et confidentialité différentielle (Data Anonymization / Differential Privacy)

Ces techniques visent à **protéger l'identité réelle des utilisateurs** lors de l'analyse de données.

- **Anonymisation** : suppression ou modification des informations identifiables.
- **Confidentialité différentielle** : ajout de bruit statistique aux données pour garantir qu'aucune information individuelle ne puisse être isolée ou identifiée.

d. Audit et révision périodique

La **révision régulière des systèmes et algorithmes d'IA** permet de **vérifier la conformité aux lois sur la protection des données** et d'identifier les vulnérabilités potentielles.

Cette pratique favorise une **surveillance proactive**, garantissant que les modèles respectent la **vie privée et les droits des utilisateurs**.

Partie pratique : Protection des données utilisateurs face à l'intelligence artificielle

Avec l'**expansion rapide de l'IA** dans notre quotidien, la **protection des données personnelles** devient un enjeu crucial, tant pour les **utilisateurs** que pour les **développeurs et entreprises** exploitant ces informations pour améliorer leurs services.

Sur la base de mon expérience en **développement web** et **gestion de systèmes numériques**, les mesures de protection peuvent être organisées en **niveaux pratiques, techniques et stratégiques**.

1. Niveau utilisateur individuel : pratiques essentielles

a. Gestion des comptes et identité numérique

- **Mots de passe complexes et uniques** pour chaque service : combinaison de **lettres, chiffres et symboles**.

  Exemple : créer un mot de passe comme Diaa@2025!WebAI au lieu d'un mot simple.

- **Authentification à deux facteurs (2FA)**: indispensable pour les **courriels** et les **services cloud**. *Applications recommandées : Google Authenticator, Authy.*

- **Gestion de l'identité numérique** : utilisation d'outils tels que **1Password** ou **Bitwarden** pour **stocker et gérer les mots de passe** de manière sécurisée, et pour **surveiller toute tentative d'intrusion**.

b. Contrôle des données des applications

- **Vérification régulière des permissions** : de nombreuses applications demandent des accès inutiles. Il est recommandé de **désactiver l'accès à la caméra, au microphone ou à la localisation** si ces fonctionnalités ne sont pas nécessaires.

- **Limitation du partage avec des tiers** : certaines extensions ou bibliothèques externes collectent des données à l'insu des utilisateurs. Il faut **désactiver les services qui collectent des informations non essentielles**.

- **Suppression des données anciennes** : supprimer les comptes inactifs ou réduire les données stockées dans le cloud afin de **minimiser les risques de fuite ou de piratage**.

2. Niveau technique et outils numériques

Les utilisateurs et développeurs peuvent renforcer la protection des données grâce à des **mesures techniques concrètes**, adaptées aux environnements numériques actuels.

a. Navigateurs et protection en ligne

- Utiliser des navigateurs **axés sur la vie privée** tels que **Brave** ou **Firefox**.

- Installer des extensions comme **uBlock Origin** et **Privacy Badger** pour **limiter le suivi des données** et le pistage publicitaire.

- Activer le **blocage des cookies** et la **protection de la navigation avancée** pour réduire la collecte d'informations par les sites web.

b. Réseaux privés virtuels (VPN) et chiffrement

- Utiliser un **VPN fiable** pour **chiffrer le trafic Internet** et masquer la **localisation**, surtout lors de l'utilisation de **réseaux Wi-Fi publics**.

- Chiffrer les **courriels et communications** à l'aide de services sécurisés tels que **ProtonMail** ou **Tutanota**, afin de protéger les échanges sensibles.

c. Protection des données lors de l'utilisation des outils d'IA

- Éviter d'entrer **directement des données sensibles** dans les IA accessibles publiquement.

- Utiliser des **données anonymes ou de test** lors de l'expérimentation ou de l'intégration des IA sur des sites web, afin de **préserver la sécurité des informations réelles**.
- Vérifier attentivement les **politiques de confidentialité** des outils d'IA pour garantir la **conformité aux lois locales et internationales**, telles que le **nLPD suisse** et le **RGPD européen**.

3. Niveau expertise pratique : stratégies avancées

Pour les **entreprises et développeurs**, il existe des **stratégies avancées** permettant de concilier l'utilisation de l'IA avec la **protection des données personnelles** et le respect des réglementations.

a. Apprentissage fédéré (Federated Learning)

L'**apprentissage fédéré** permet de **former des modèles IA** sans transférer les données brutes vers un serveur central.

Exemple pratique : lors du développement d'un **système de recommandation** sur un site web, les données restent sur l'appareil de l'utilisateur et seules les **mises à jour chiffrées** sont envoyées au modèle central, préservant ainsi la **confidentialité des informations personnelles**.

b. Confidentialité différentielle (Differential Privacy)

La **confidentialité différentielle** est un outil puissant pour protéger les données des utilisateurs lors de l'analyse de **big data**.

Exemple pratique : ajouter du **« bruit »** statistique aux données avant leur traitement afin de conserver l'efficacité analytique tout en **préservant l'anonymat** des individus.

c. Audit et révision régulière (Auditing)

Il est essentiel de **vérifier périodiquement** les données stockées et les services associés afin de détecter toute **fuite ou utilisation illégale**.

Des outils comme **OWASP ZAP** ou **Burp Suite** peuvent être utilisés pour **identifier les vulnérabilités** des applications manipulant des informations sensibles.

d. Protection contre le suivi et l'analyse externe

- Appliquer des techniques telles que **Content Security Policy (CSP)** et les **cookies SameSite** pour empêcher le **suivi des données par des tiers**.
- Limiter l'utilisation de **bibliothèques externes non fiables** susceptibles de **collecter des données à l'insu des utilisateurs**.

4. Éducation et sensibilisation numérique

La **sensibilisation numérique** constitue un **élément fondamental** pour la protection des données personnelles face à l'intelligence artificielle.

- **Connaissance des droits des utilisateurs** : comprendre les **droits accordés par le nLPD suisse** et le **RGPD européen**, afin de pouvoir exercer un contrôle effectif sur ses données.

- **Compréhension des méthodes de fraude numérique** : se familiariser avec le **phishing**, les **arnaques en ligne** et autres techniques de manipulation visant à collecter des informations personnelles.
- **Mises à jour régulières des systèmes et applications** : suivre les **patchs de sécurité** et les **mises à jour logicielles** pour réduire les vulnérabilités exploitables par des acteurs malveillants.

Cette approche permet aux utilisateurs de **développer une vigilance proactive** et de **réduire les risques liés à la collecte et au traitement des données par les technologies d'IA**.

5. Intégration de l'expérience pratique à la protection des données

L'expérience montre que la **protection des données personnelles** face à l'IA est plus efficace lorsqu'elle repose sur une **approche combinée** :

- **Technologies numériques modernes** : chiffrement, VPN, outils anti-tracking et autres dispositifs techniques pour sécuriser les données.
- **Pratiques légales** : respect du **consentement**, de la **transparence**, et mise en place de mécanismes pour la **suppression des données**.
- **Sensibilisation et éducation numérique** : formation des utilisateurs et des développeurs aux bonnes pratiques et aux risques potentiels.

Cette combinaison permet de **créer un environnement plus sûr** pour l'utilisateur, même dans un contexte d'**utilisation avancée d'outils d'IA**.
La protection des données n'est pas uniquement une **responsabilité individuelle**, mais fait partie intégrante de la **conception et du développement éthique et responsable** des systèmes intelligents.

Conclusion et recommandations : Combiner la loi et la technologie pour une protection efficace

Avec l'expansion rapide des **technologies d'intelligence artificielle (IA)** et leur adoption croissante dans notre quotidien, la **protection des données personnelles** représente un **défi majeur**. Pour y répondre efficacement, il est essentiel de combiner **cadres légaux stricts** et **pratiques techniques avancées**. Comme démontré dans les sections précédentes, il ne suffit pas de se fier uniquement aux lois ou aux outils techniques sans une **compréhension complète** de la manière dont les données sont collectées, traitées et protégées.

1. Synthèse

- **Lois suisses et européennes** : la **nLPD** et le **RGPD** constituent la **base légale** pour protéger les droits des individus, en mettant l'accent sur la **transparence**, le **consentement éclairé**, et le **droit des individus à contrôler leurs données**.
- **Impact de l'IA sur la vie privée** : les effets se manifestent notamment dans l'**analyse de Big Data**, les **systèmes de recommandation**, le **traitement des données biométriques**, et l'**entraînement des modèles sur des données personnelles**.

- **Mesures pratiques et techniques** : l'**authentification à deux facteurs**, le **chiffrement**, l'**apprentissage fédéré**, la **confidentialité différentielle**, et les **audits réguliers** permettent une **protection efficace des données** au niveau individuel et institutionnel.

2. Tendances futures de l'IA et protection des données

IA générative et protection des données

- **Risques** : les modèles génératifs peuvent **mémoriser ou reproduire des données sensibles** issues de l'entraînement, entraînant des **fuites d'informations personnelles** ou de **propriété intellectuelle**.
- **Solutions légales** :
  - Le **RGPD** et la **nLPD** s'appliquent aux traitements de données utilisés pour l'entraînement des modèles, exigeant un **consentement explicite** ou l'usage de **données anonymisées**.
  - Les **futures lois sur l'IA**, telles que l'**EU AI Act**, imposent une **évaluation préalable des risques de sécurité et éthiques** avant de déployer tout système génératif auprès des utilisateurs.

Cette conclusion souligne que la **protection des données face à l'IA** nécessite une approche **intégrée**, combinant **légalité, technologie et sensibilisation**, pour garantir la **sécurité, la confidentialité et le respect des droits des utilisateurs** dans un environnement numérique en constante évolution.

3. Exemples pratiques, législation future et recommandations

a. Exemples pratiques pour la protection des données

- **Entraînement sur données anonymisées** : former un modèle d'IA pour la recherche ou l'amélioration des services **sans accéder aux données originales**, réduisant ainsi les risques pour la vie privée.
- **Intégration de la Differential Privacy** : appliquer cette technique dans les modèles génératifs pour **empêcher la récupération de données sensibles** issues des ensembles d'entraînement.

b. Législation et conformité future

Les **réglementations évoluent** pour couvrir de nouveaux cas liés à l'IA :

- **Responsabilité des entreprises** : les développeurs d'IA peuvent être tenus responsables si leurs modèles produisent du contenu contenant **des données personnelles non protégées**.
- **Obligation de mesures de sécurité** : les entreprises doivent mettre en œuvre des **techniques de protection et des contrôles stricts** lors de l'utilisation d'IA générative dans des services **commerciaux, médicaux ou éducatifs**.

c. Exemples pratiques de conformité

- Les fournisseurs d'IA pour la **génération de texte ou d'images** doivent s'assurer qu'il est **impossible d'extraire les données originales** utilisées pour l'entraînement.
- Intégrer une **évaluation régulière des risques liés à l'IA** dans les politiques internes et relier ces évaluations aux **rapports de conformité légale**.

4. Recommandations

- **Combiner lois et technologies** : respecter les régulations locales et internationales tout en appliquant **les meilleures pratiques techniques** pour protéger les données.
- **Permettre aux utilisateurs de contrôler leurs données** : fournir des interfaces simples pour **gérer les permissions**, **supprimer les données** et **vérifier leurs profils**.
- **Sensibilisation numérique continue** : renforcer la conscience des utilisateurs sur le fonctionnement de l'IA, leurs **droits légaux** et les **bonnes pratiques** pour protéger leurs informations.
- **Adopter des méthodes avancées de protection** : telles que le **chiffrement**, l'**apprentissage fédéré**, la **confidentialité différentielle** et les **audits réguliers**, garantissant la sécurité des données sans compromettre l'efficacité des services.
- **Développer des politiques de confidentialité claires et transparentes** : ces documents doivent être **compréhensibles, à jour**, et expliquer comment les données sont **collectées, utilisées et partagées**, en conformité avec le **nLPD suisse** et le **RGPD européen**.

5. Résumé

La **protection des données à l'ère de l'intelligence artificielle** nécessite un **équilibre harmonieux** entre **législation**, **technologies avancées** et **pratiques opérationnelles efficaces**. En combinant ces éléments, les **utilisateurs** et les **entreprises** peuvent **préserver la confidentialité**, **minimiser les risques liés aux données personnelles** et **assurer un usage sûr et performant de l'IA** dans une variété d'applications numériques.

Références

- Federal Act on Data Protection (nLPD). (2023). *Switzerland: Federal Data Protection and Information Commissioner (FDPIC)*. https://edoeb.admin.ch
- European Parliament and Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
- PKWARE. (2025, July). *McDonald's McHire Data Breach Advisory*. https://www.pkware.com/
- Cloud Security Alliance. (2024). *Snowflake Data Breach Report*. https://cloudsecurityalliance.org/
- TrustArc. (2024). *AI Privacy and Generative AI Guidelines*. https://trustarc.com/resources/
- ArtificialIntelligenceAct.eu. (2025). EU AI Act – Overview and Key Information on the Artificial Intelligence Regulation. *https://artificialintelligenceact.eu*
- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202401689*