

La souveraineté numérique et l'intelligence artificielle

Étude pluridisciplinaire

Cédric Durand, Yaniv Benhamou, Diego Kuonen et Gaia Valenti

Genève, 16 juin 2026

La souveraineté numérique et l'intelligence artificielle

Étude pluridisciplinaire^{*}

Prof. Durand Cédric

Économie politique, Faculté de Sciences de la Société / UNIGE

Prof. Benhamou Yaniv

Droit du numérique, Digital Law Center, Faculté de Droit / UNIGE

Prof. Diego Kuonen

Science des données, Geneva School of Economics and Management / UNIGE

Mme Gaia Valenti

Économie politique et histoire économique, Faculté de Sciences de la Société / UNIGE

Genève, 16 juin 2026

^{*} Cette étude a été réalisée sur mandat du Département des institutions et du numérique de la République et Canton de Genève. Elle a été nourrie par des entretiens dont la liste est fournie en annexe B p. 92.

Table des matières

RÉSUMÉ.....	5
ZUSAMMENFASSUNG	7
SINTESI	10
INTRODUCTION.....	12
1. UN LANGAGE COMMUN POUR UNE COMPRÉHENSION PARTAGÉE	19
1.1. L’IA COMME SYSTÈME SOCIO-TECHNIQUE	19
1.2. SOUVERAINETÉ NUMÉRIQUE ET MARGES DE MANŒUVRE	22
1.3. UNE APPROCHE HOLISTIQUE DE L’IA	23
1.4. ACTEURS ET CHAMPS D’APPLICATION	27
1.5. LE CONTEXTE HELVÉTIQUE	27
1.6. CONCLUSION	28
2. ENJEUX JURIDIQUES DE LA SOUVERAINETÉ NUMÉRIQUE À L’ÈRE DE L’IA.....	30
2.1. REMARQUES PRÉALABLES.....	30
2.2. UTILISATION DE MODÈLES D’IA DE FOURNISSEURS IA PAR L’ADMINISTRATION ET LES ACTEURS PRIVÉS : TRANSFERT DES DONNÉES	32
2.3. DÉVELOPPEMENT DE MODÈLES SOUVERAINS PAR L’ADMINISTRATION ET LES ACTEURS PRIVÉS : ACCÈS AUX DONNÉES	36
2.4. PROTECTION DES DROITS FONDAMENTAUX ET CONFIANCE	44
2.5. CONCENTRATION DES POUVOIRS	49
2.6. CONCLUSION SUR LES ENJEUX JURIDIQUES	54
3. UNE CROISSANCE FULGURANTE MAIS DIFFÉRENCIÉE DE L’EMPREINTE DE L’IA EN SUISSE....	56
3.1. PERSPECTIVE GÉNÉRALE	56
3.2. DIFFUSION DANS LE SECTEUR DES ENTREPRISES	58
3.3. DIFFUSION DANS LES ADMINISTRATIONS.....	60
4. LES DÉFIS SOCIOÉCONOMIQUES DE L’IA	63
4.1. DES DÉPENDANCES TECHNOLOGIQUES MARQUÉES MAIS DIFFÉRENCIÉES	63
4.2. DES RISQUES MAL MAÎTRISÉS.....	70
4.3. LE TRAVAIL EN DANGER	75
4.4. UNE TRAJECTOIRE MATÉRIELLE INSOUTENABLE	80
5. PRÉSERVER LES CAPACITÉS DE PILOTAGE ET RENFORCER L’AUTONOMIE STRATÉGIQUE	84
5.1. L’ADMINISTRATION PUBLIQUE DOIT CHOISIR LE RYTHME ET L’ÉTENDUE DU DÉPLOIEMENT DE L’IA EN FONCTION DE SES OBJECTIFS PROPRES	84
5.2. FAIRE DE L’ACTION PUBLIQUE EN MATIÈRE D’IA UN LEVIER DE LA SOUVERAINETÉ NUMÉRIQUE.....	86
5.3. PROTÉGER LES PERSONNES, PRÉSERVER LA NATURE	87
ANNEXES	92
A. ASPECTS SAILLANTS DE LA RÉGULATION AUX ÉTATS-UNIS, DANS L’UNION EUROPÉENNE ET EN CHINE	92
B. LISTE DES ENTRETIENS	96
C. DÉCLARATION DE TRANSPARENCE.....	96
RÉFÉRENCES.....	97

Liste des figures

FIGURE 1: LE SYSTÈME D'IA : DÉVELOPPEMENT DES MODÈLES (A) ET DÉPLOIEMENT (B).....	20
FIGURE 2: LE CYCLE DE VIE D'UN SYSTÈME D'IA	20
FIGURE 3: L'EMPILEMENT DE FONCTIONS DANS UN SYSTÈME DE GENAI AVEC DES EXEMPLES DES FIRMES QUI Y CONTRIBUENT	21
FIGURE 4 : INVESTISSEMENT DANS L'IA PAR LE SECTEUR PRIVÉ RAPPORTÉ À L'INVESTISSEMENT TOTAL EN CAPITAL FIXE (2013-2024)	57
FIGURE 5 : CATÉGORIES DES PROJETS IA REPORTÉS AU CNAI	61
FIGURE 6 : TRAFIC MONDIAL SUR LES PRINCIPAUX CHATBOTS D'IA EN JANVIER 2026 (SIMILARWEB)	66
FIGURE 7 : RÉPARTITION DU TRAFIC SUR LES PRINCIPAUX CHATBOTS D'IA EN SUISSE ET POUR UNE SÉLECTION D'AUTRES PAYS EN JANVIER 2026 (SIMILARWEB)	67
FIGURE 8 : LOCALISATION ET NOMBRE DES CENTRES DE DONNÉES EN SUISSE (HTTPS://WWW.DATACENTERMAP.COM/SWITZERLAND/, CONSULTÉ LE 25 FÉVRIER 2025)	68
FIGURE 9 : ÉVOLUTION DE LA RÉPARTITION MONDIALE DES REVENUS TIRÉS DES SERVICES D'INFRASTRUCTURE CLOUD AUX ENTREPRISES (SYNERGY GROUP, 2025)	70
FIGURE 10 : NOMBRES D'INCIDENTS ET DE SITUATIONS DANGEREUSES RECENSÉS DANS LE MONDE ET EN SUISSE DEPUIS 2022 (OCDE)	70
FIGURE 11 : LA POSSIBILITÉ D'UNE COURBE EN J INVERSÉ DE LA PRODUCTIVITÉ DU TRAVAIL AVEC LE DÉPLOIEMENT À GRANDE ÉCHELLE DE L'IA DANS LES ORGANISATIONS.....	80

Liste des tableaux

TABLEAU 1: APPROCHE HOLISTIQUE DU PILOTAGE STRATÉGIQUE DE L'IA.....	26
TABLEAU 2 : TYPES D'USAGES MALVEILLANTS DE FAUX CONTENUS GÉNÉRÉS PAR IA CONTRE LES PERSONNES	73
TABLEAU 3 : PROBLÈMES DE FIABILITÉ DOCUMENTÉS CHEZ LES SYSTÈMES D'IA GÉNÉRATIVE, LES AGENTS D'IA ET LES SYSTÈMES MULTI-AGENTS	77
TABLEAU 4. SYNTHÈSE DES RECOMMANDATIONS.....	90
TABLEAU 5: ANALYSE DE LA LOI CALIFORNIENNE SB-53 PAR LE CABINET BCLP	93

Résumé

Ce travail académique pluridisciplinaire explicite les enjeux de souveraineté numérique appliqués à l'IA. L'étude montre comment ces enjeux sont vitaux pour les administrations publiques, notamment au niveau cantonal, mais elle aborde aussi ces questions dans une perspective sociétale, en intégrant l'impact sur l'économie et la population. Étant donné l'hégémonie des grandes plateformes étasuniennes sur le territoire suisse et l'intensité des liens avec les autres pays européens, une attention particulière sera accordée à ces deux dimensions en ce qui concerne la réglementation et les questions techno-économiques.

Une compréhension systémique

Pour aborder rigoureusement les rapports entre l'IA et la souveraineté numérique, une clarification conceptuelle est indispensable. L'IA est un système sociotechnique dont l'analyse ne peut être sectorielle ou fragmentée. Elle exige une approche intégrée, prenant en compte l'ensemble des acteurs concernés et les différents niveaux auxquels se situent son développement, son déploiement et ses effets. Les problèmes les plus saillants se situent sur le plan technologique (infrastructure, capacité de calcul, logiciels et outils), sur le plan humain, sur le plan des capacités administratives (formation, risque de déqualification, compréhension des modèles et des cadres d'analyse), sur le plan des données (intégrité et protection) et sur le plan de l'impact matériel (notamment énergétique et écologique).

La souveraineté numérique ne s'apparente pas à une quête illusoire d'autarcie, mais pose la question de la faculté pour les autorités publiques d'orienter les interdépendances inhérentes à l'écosystème de l'IA en fonction d'une appréciation des risques ou des préjudices observés auxquels la société s'expose. Les marges de manœuvre de la puissance publique ne peuvent être appréciées uniquement sous l'angle technologique. Elles résultent d'un ensemble d'actes délibérés au niveau institutionnel, juridique, économique, organisationnel, culturel et géopolitique de manière à structurer un environnement numérique conforme aux attentes de la population.

Un cadre légal inachevé

La Confédération élabore actuellement un projet de loi IA qui vise à assurer la mise en œuvre de la Convention du Conseil de l'Europe, avec une régulation suivant trois objectifs : *(i)* le renforcement de la Suisse en tant que pôle d'innovation ; *(ii)* la protection des droits fondamentaux, et *(iii)* le renforcement de la confiance de la population en l'IA. Le cadre légal se veut assez souple pour permettre à la fois le déploiement des modèles d'IA (IA locale, en cloud encadré ou public) et le développement de modèles d'IA souverains développés par le secteur public.

Plusieurs points d'amélioration subsistent toutefois. Confrontée à une injonction d'adopter des modèles d'IA pour améliorer ses processus, l'administration doit simultanément se conformer à un cadre légal strict sur le plan de la protection des données et les droits fondamentaux. Or, ce respect du cadre légal peut être mis en péril, suivant les types de modèles d'IA et d'hébergement choisis. Le cadre légal ne prévoit par ailleurs pas, ou peu, de règles en matière de souveraineté numérique, ce qui n'incite pas l'administration et les acteurs privés à plus d'autonomie.

Une croissance fulgurante mais différenciée

Si l'IA est déjà une réalité dans les secteurs privé et public en Suisse, sa diffusion est loin d'être linéaire puisqu'elle varie en fonction du secteur et du type d'organisation. Par ailleurs, le phénomène d'IA fantôme (usages non encadrés) dans les entreprises et les administrations indique qu'elle n'obéit pas toujours à une stratégie coordonnée. La trajectoire de diffusion dépend donc des leviers institutionnels qui l'orientent. Or, les capacités gouvernementales de la Suisse sont sur ce plan insuffisantes, pointant la nécessité du renforcement des dispositifs de gouvernance de l'IA.

Des risques mal maîtrisés

Le déploiement des systèmes d'IA déjà révolutionnaires soulève des interrogations sérieuses. En dépit de capacités technologiques importantes, la situation de dépendance de la Suisse à tous les niveaux du stack de l'IA (modèle, capacités de calcul, données...) est patente. Ce qui pose des risques à la fois multiples et sévères, notamment sur le plan de la sécurité, des atteintes à la personnalité et aux droits politiques, en termes d'accroissement des coûts économiques et d'atteinte à l'intégrité de l'action publique.

Au-delà de ces menaces de subordination à des firmes hors de contrôle du législateur, s'ajoutent des problèmes qui concernent les effets de la technologie elle-même sur les processus de travail : fiabilité incertaine, déqualification, détérioration de la coopération, désinvestissements des personnes... Ces phénomènes se conjuguent et peuvent contrecarrer les gains attendus de l'automatisation, laissant le bilan d'ensemble sur le plan de l'efficacité incertain tandis que le risque d'une dégradation des rapports humains est aisément identifiable.

Préserver les capacités de pilotage et renforcer l'autonomie stratégique

Face à ces défis vitaux et aux effets de sidération associés à la multiplication des outils, il convient de ne pas précipiter le déploiement de systèmes d'IA au niveau des processus administratifs dans leur ensemble.

Nos recommandations s'articulent ainsi autour de trois axes.

1. Tenter de se situer à la frontière de l'innovation fait courir un risque de désorganisation de l'action publique, source à la fois d'inefficacité potentielle, d'insatisfaction des employé·e·s publics et des usagers et de failles de sécurité. Dès lors, il est crucial que **l'administration publique maîtrise le rythme et l'étendue du déploiement de l'IA et les subordonne à ses objectifs propres.**
2. L'action publique en matière d'IA comprend une multitude de leviers (formation, réglementation, commande publique, investissement...) mais elle ne s'insère dans une logique de souveraineté numérique que si **elle s'articule à un ensemble de mesures visant à garantir une autonomie stratégique sur l'ensemble du stack numérique**, notamment dans le domaine des données, des logiciels et des infrastructures.
3. Conformément à la volonté populaire de protection de l'intégrité numérique, les autorités cantonales doivent adopter une politique proactive en matière d'IA visant à **protéger les personnes dans leurs droits fondamentaux et à préserver la nature en contenant l'empreinte écologique.**

Zusammenfassung

Diese interdisziplinäre akademische Arbeit erläutert die Herausforderungen der digitalen Souveränität im Kontext von KI. Die Studie zeigt, wie zentral diese Fragen für die öffentliche Verwaltung – insbesondere auf Kantonsebene – sind, und beleuchtet sie zugleich aus einer gesellschaftlichen Perspektive, indem sie die Auswirkungen auf Wirtschaft und Bevölkerung einbezieht. Angesichts der Hegemonie grosser US-amerikanischer Plattformen auf Schweizer Territorium und der Intensität der Verflechtungen mit anderen europäischen Ländern gilt diesen beiden Dimensionen besondere Aufmerksamkeit – sowohl im Hinblick auf Regulierung als auch auf techno-ökonomische Fragestellungen.

Ein systemisches Verständnis

Um die Beziehungen zwischen KI und digitaler Souveränität fundiert zu analysieren, ist eine begriffliche Klärung unerlässlich. KI ist ein soziotechnisches System, dessen Analyse nicht sektoral oder fragmentiert erfolgen kann. Sie erfordert einen integrierten Ansatz, der alle relevanten Akteure sowie die verschiedenen Ebenen berücksichtigt, auf denen sich ihre Entwicklung, ihr Einsatz und ihre Wirkungen vollziehen. Die markantesten Probleme liegen auf der technologischen Ebene (Infrastruktur, Rechenkapazität, Software und Werkzeuge), auf der menschlichen Ebene, auf der Ebene der administrativen Fähigkeiten (Ausbildung, Risiko der Dequalifizierung, Verständnis der Modelle und Analyse-Frameworks), auf der Ebene der Daten (Integrität und Schutz) sowie auf der Ebene der materiellen Auswirkungen (insbesondere Energie- und Umweltaspekte).

Digitale Souveränität ist nicht als illusorische Suche nach Autarkie zu verstehen, sondern stellt die Frage, inwiefern öffentliche Behörden die für das KI-Ökosystem inhärenten Interdependenzen auf Grundlage einer Bewertung der Risiken und potenziellen Schäden, denen die Gesellschaft ausgesetzt ist, steuern können. Der Handlungsspielraum der öffentlichen Hand lässt sich dabei nicht allein aus technologischer Perspektive beurteilen. Er ergibt sich vielmehr aus einem Bündel bewusst gesetzter institutioneller, rechtlicher, wirtschaftlicher, organisatorischer, kultureller und geopolitischer Massnahmen, um ein digitales Umfeld zu gestalten, das den Erwartungen der Bevölkerung entspricht.

Ein unvollständiger Rechtsrahmen

Der Bund erarbeitet derzeit ein KI-Gesetzesprojekt, das die Umsetzung der Konvention des Europarats sicherstellen soll, mit einer Regulierung entlang dreier Zielsetzungen: (i) die Stärkung der Schweiz als Innovationsstandort; (ii) der Schutz der Grundrechte; und (iii) die Stärkung des Vertrauens der Bevölkerung in KI. Der Rechtsrahmen soll ausreichend flexibel sein, um sowohl den Einsatz von KI-Modellen (lokale KI, regulierte Cloud oder Public Cloud) als auch die Entwicklung souveräner KI-Modelle durch den öffentlichen Sektor zu ermöglichen.

Mehrere Verbesserungspunkte bleiben jedoch bestehen. Die Verwaltung steht unter dem Druck, KI-Modelle zur Verbesserung ihrer Prozesse einzusetzen, und muss sich gleichzeitig an einen strengen Rechtsrahmen im Bereich Datenschutz und Grundrechte

halten. Diese Einhaltung kann jedoch je nach gewähltem KI-Modell und Hosting-Ansatz gefährdet sein. Der Rechtsrahmen enthält zudem keine oder nur wenige Vorgaben zur digitalen Souveränität, was weder die Verwaltung noch private Akteure zu mehr Autonomie anreizt.

Ein rasantes, aber differenziertes Wachstum

Während KI im privaten und öffentlichen Sektor in der Schweiz bereits Realität ist, verläuft ihre Verbreitung keineswegs linear, sondern variiert je nach Sektor und Organisationstyp. Zudem zeigt das Phänomen der Schatten-KI (nicht geregelte Nutzungen) in Unternehmen und Verwaltungen, dass ihr Einsatz nicht immer einer koordinierten Strategie folgt. Die Diffusionsbahn hängt somit von institutionellen Hebeln ab, die sie steuern. In dieser Hinsicht sind die staatlichen Kapazitäten der Schweiz derzeit unzureichend, was die Notwendigkeit einer Stärkung der Governance-Strukturen für KI unterstreicht.

Unzureichend beherrschte Risiken

Der Einsatz bereits heute revolutionärer KI-Systeme wirft ernsthafte Fragen auf. Trotz erheblicher technologischer Fähigkeiten ist die Abhängigkeit der Schweiz auf allen Ebenen des KI-Stacks (Modelle, Rechenkapazitäten, Daten usw.) offensichtlich. Daraus ergeben sich vielfältige und erhebliche Risiken, insbesondere in Bezug auf Sicherheit, Persönlichkeitsrechte und politische Rechte, steigende wirtschaftliche Kosten sowie die Integrität staatlichen Handelns.

Über diese Gefahren einer Abhängigkeit von Unternehmen ausserhalb der Kontrolle des Gesetzgebers hinaus treten zusätzliche Probleme auf, die die Auswirkungen der Technologie selbst auf Arbeitsprozesse betreffen: unsichere Zuverlässigkeit, Dequalifizierung, Verschlechterung der Zusammenarbeit, sinkendes Engagement der Mitarbeitenden. Diese Entwicklungen verstärken sich gegenseitig und können die erwarteten Effizienzgewinne durch Automatisierung untergraben. Insgesamt bleibt die Bilanz hinsichtlich der Effizienz unsicher, während das Risiko einer Verschlechterung zwischenmenschlicher Beziehungen klar erkennbar ist.

Steuerungsfähigkeit sichern und strategische Autonomie stärken

Angesichts dieser zentralen Herausforderungen und der mit der Vielzahl neuer Werkzeuge verbundenen Schockeffekte ist es angezeigt, den Einsatz von KI-Systemen in administrativen Prozessen nicht vorschnell voranzutreiben.

Unsere Empfehlungen gliedern sich entlang von drei Achsen:

1. Der Versuch, sich an der Innovationsgrenze zu positionieren, birgt das Risiko einer Desorganisation staatlichen Handelns – mit potenzieller Ineffizienz, Unzufriedenheit bei Mitarbeitenden der öffentlichen Verwaltung und Nutzenden sowie Sicherheitslücken. Daher ist es entscheidend, dass **die öffentliche Verwaltung das Tempo und den Umfang der KI-Einführung selbst bestimmt und diese ihren eigenen Zielsetzungen unterordnet.**
2. Das staatliche Handeln im Bereich KI umfasst eine Vielzahl von Hebeln (Ausbildung, Regulierung, öffentliche Beschaffung, Investitionen usw.). Es fügt sich jedoch nur dann in eine Logik digitaler Souveränität ein, wenn **es mit einem**

Bündel von Massnahmen verknüpft wird, das darauf abzielt, eine strategische Autonomie über den gesamten digitalen Stack hinweg sicherzustellen – insbesondere in den Bereichen Daten, Software und Infrastrukturen.

3. Im Einklang mit dem Volkswillen zum Schutz der digitalen Integrität müssen die kantonalen Behörden eine proaktive Politik im Bereich KI verfolgen, die darauf abzielt, **Menschen in ihren Grundrechten zu schützen und die Natur zu bewahren, indem der ökologische Fussabdruck begrenzt wird.**

Sintesi

Basandosi su un approccio multidisciplinare, il presente lavoro accademico evidenzia le sfide della sovranità digitale applicate all'IA. Si tratta di sfide fondamentali per le amministrazioni pubbliche, soprattutto a livello cantonale. Quest'analisi adotta anche un punto di vista societale, integrando ai suoi risultati l'impatto sull'economia e sulla popolazione. Data l'egemonia delle grandi piattaforme statunitensi sul territorio svizzero e l'intensità dei legami che vincolano la Svizzera agli altri paesi europei, lo studio della regolamentazione e delle questioni techno-economiche svizzere portano un'attenzione particolare a queste due dimensioni.

Un approccio sistemico

Per analizzare in modo rigoroso i rapporti tra IA e sovranità digitale, è indispensabile una chiarificazione concettuale. L'IA è un sistema sociotecnico la cui analisi non può essere settoriale o frammentata. Richiede un approccio integrato, che tenga conto dell'insieme degli attori coinvolti e dei diversi livelli in cui si collocano il suo sviluppo, il suo dispiegamento e i suoi effetti. Le problematiche più rilevanti emergono sul piano tecnologico (infrastrutture, capacità di calcolo, software e strumenti), sul piano umano, su quello delle capacità amministrative (formazione, rischio di dequalificazione, comprensione dei modelli e dei quadri di analisi), sul piano dei dati (integrità e protezione) e su quello dell'impatto materiale (in particolare energetico ed ecologico).

La sovranità digitale non equivale a una ricerca illusoria di autarchia, ma pone la questione delle capacità delle autorità pubbliche ad orientare le interdipendenze proprie dell'ecosistema dell'IA in funzione di una valutazione dei rischi o dei danni ai quali la società viene esposta. I margini di manovra del potere pubblico non possono essere valutati unicamente sotto l'angolo tecnologico: essi derivano da un insieme di atti deliberati a livello istituzionale, giuridico, economico, organizzativo, culturale e geopolitico finalizzati a strutturare un ambiente digitale conforme alle aspettative della popolazione.

Un quadro giuridico incompleto

La Confederazione sta attualmente elaborando un progetto di legge sull'IA che garantisca l'applicazione della Convenzione del Consiglio d'Europa, mediante una regolamentazione basata su tre obiettivi: *(i)* rafforzare la Svizzera come polo di innovazione, *(ii)* proteggere i diritti fondamentali, e *(iii)* rafforzare la fiducia della popolazione nell'IA. Il quadro giuridico in questione si propone di essere piuttosto flessibile, in modo da consentire sia la diffusione di modelli di IA specifici (locale, in cloud regolamentato o pubblico) sia lo sviluppo di modelli d'IA sovrani sviluppati dal settore pubblico.

Persistono tuttavia diversi punti di miglioramento. Obbligata ad adottare modelli di IA esistenti per migliorare i propri processi, l'amministrazione deve anche conformarsi a un quadro giuridico rigoroso in materia di protezione dei dati e diritti fondamentali. Tuttavia, il rispetto di tale quadro può risultare compromesso dal tipo di modello e dalle soluzioni di hosting adottate. Inoltre, il quadro giuridico di cui sopra prevede poche, se non

nessuna, norme in materia di sovranità digitale, il che non incentiva l'amministrazione e gli attori privati a ricercare attivamente una maggiore autonomia.

Una crescita rapida ma differenziata

Pur costituendo una realtà nei settori privati e pubblici, la diffusione dell'IA in Svizzera è tutt'altro che lineare, poiché varia a seconda del settore e del tipo di organizzazione. Inoltre, la frequenza degli usi non regolamentati, o "AI ombra" nelle imprese e nelle amministrazioni indica che la diffusione dell'IA sul territorio non è sempre frutto di una strategia coordinata. In linea generale, la traiettoria di diffusione dell'IA dipende dalle leve istituzionali che la orientano. Tuttavia, le capacità governative della Svizzera sono su questo piano insufficienti, evidenziando la necessità di rafforzare i dispositivi di gestione del dispiegamento dell'IA.

Rischi mal gestiti

Il dispiegamento di sistemi di IA già rivoluzionari solleva interrogativi seri. Nonostante le sue importanti capacità tecnologiche, la dipendenza della Svizzera a tutti i livelli dello stack dell'IA (modelli, capacità di calcolo, dati,...) è evidente. Ciò comporta molteplici rischi gravi, in particolare sul piano della sicurezza, delle violazioni della personalità e dei diritti politici, dell'aumento dei costi economici e dell'integrità dell'azione pubblica. Oltre a queste minacce di subordinazione a imprese fuori dal controllo del legislatore, si aggiungono problemi legati agli effetti della tecnologia stessa sui processi di lavoro: affidabilità incerta, dequalificazione, deterioramento della cooperazione, disinteresse personale... Combinati, tali fenomeni negativi sono sufficienti a contrastare i benefici attesi dell'automazione, rendendo incerto il bilancio complessivo in termini di efficienza e, soprattutto, deteriorando la qualità delle relazioni umane.

Preservare le capacità di governo e rafforzare l'autonomia strategica

Di fronte a queste sfide vitali e agli effetti di disorientamento di fronte alla moltiplicazione degli strumenti, è opportuno non affrettare il dispiegamento dei sistemi di IA nei processi amministrativi nel loro complesso.

Le nostre raccomandazioni si articolano intorno a tre linee direttrici.

1. Cercare di posizionarsi alla frontiera dell'innovazione comporta un rischio di disorganizzazione dell'azione pubblica, fonte sia di potenziale inefficienza sia di insoddisfazione dei dipendenti pubblici e degli utenti, nonché di carenze di sistemi di sicurezza. È quindi fondamentale **che l'amministrazione pubblica controlli il ritmo e l'estensione del dispiegamento delle IA e li subordini ai propri obiettivi.**
2. L'azione pubblica in materia di IA comprende una molteplicità di leve (formazione, regolamentazione, appalti pubblici, investimenti...), ma **per inserirsi in una logica di sovranità digitale essa deve essere accompagnata da un insieme di misure volte a garantire un'autonomia strategica su tutto lo stack digitale**, in particolare nei settori dei dati, del software e delle infrastrutture.
3. In conformità alla volontà popolare di protezione dell'integrità digitale, le autorità cantonali devono adottare una politica proattiva in materia di IA, volta a **proteggere le persone nei loro diritti fondamentali e a proteggere l'ambiente contenendo l'impronta ecologica.**

Introduction

Dans le sillage de l'engouement suscité par l'outil ChatGPT lors de son lancement en octobre 2022 et de la diffusion d'outils tels que Gemini, Copilot et Claude, les systèmes d'intelligence artificielle générative (GenAI) sont entrés dans le quotidien des personnes et des organisations et, avec leur perfectionnement, semblent sur le point de déstabiliser des pans entiers de nos sociétés.

Les systèmes de GenAI constituent la pointe avancée d'un ensemble plus large de systèmes d'intelligence artificielle (IA) capables, par exemple, d'automatiser des processus de travail, d'effectuer des prédictions, de systématiser des prises de décision et de communiquer en langage naturel. Leur déploiement à grande échelle soulève, dans de nouveaux termes, la question de la souveraineté numérique. Si ces dispositifs d'automatisation du travail intellectuel laissent entrevoir des gains considérables en termes d'efficacité et de robustesse des processus administratifs, leur généralisation soulève des interrogations majeures quant à l'intégrité de l'action publique et, plus généralement, quant aux risques de subordination de l'activité économique et sociale aux acteurs dominants du secteur de la technologie et/ou aux États dans lesquels ils sont établis. Au-delà des vulnérabilités associées à la monopolisation des informations et aux dépendances technologiques, ce qui est en jeu, c'est la préservation des capacités humaines, technologiques et administratives nécessaires à l'exercice de la souveraineté.

Ce travail académique pluridisciplinaire (économie politique, droit, science des données) à destination des décideurs politiques vise à expliciter ces enjeux de souveraineté numérique appliqués à l'IA afin d'informer les choix stratégiques qui seront pris au niveau cantonal, intercantonal, voire national. Les problèmes les plus saillants posés par l'IA se situent sur le plan technologique (infrastructure, capacité de calcul et logiciels), sur le plan humain des capacités administratives (formation, risque de déqualification, maîtrise des modèles et des cadres d'analyse), sur le plan des données (intégrité et protection) et sur le plan de l'impact matériel (notamment énergétique et écologique).

L'étude va montrer comment ces enjeux sont vitaux pour les administrations publiques, notamment au niveau cantonal, mais elle aborde aussi ces questions dans une perspective sociétale, en intégrant l'impact sur l'économie et la population. Étant donné l'hégémonie des grandes plateformes étasuniennes sur le territoire suisse et l'intensité des liens avec les autres pays européens, une attention particulière sera accordée à ces deux dimensions en ce qui concerne, la réglementation et les questions techno-économiques.

Définitions

L'idée d'automatiser le raisonnement humain est très ancienne, et des dispositifs matériels permettant de déployer la pensée algorithmique existent depuis plusieurs

millénaires². Le terme d'*intelligence artificielle* a été introduit en 1956 à la conférence de Dartmouth dont l'objectif est de faire en sorte que « les machines utilisent le langage, forment des abstractions et des concepts, résolvent des problèmes aujourd'hui réservés aux humains et s'améliorent elles-mêmes »³. Dans la même période, les premiers travaux sur les réseaux neuronaux menaient à l'invention du perceptron, un appareil capable d'interpréter et de réagir à des signaux lumineux⁴. Pendant une longue période, les recherches ont principalement visé à reproduire le raisonnement logique sous la forme de systèmes experts. En parallèle, les techniques dites de « machine learning » (apprentissage automatique) ont suivi une autre piste, associant l'entraînement sur des réseaux neuronaux multicouche (l'apprentissage profond), l'utilisation de processeurs graphiques (GPU) et des données massives. À partir des années 2010, la première piste de l'IA symbolique a été supplantée par la seconde centrée sur les données. Dans la foulée, les progrès de la génération de données par les algorithmes aboutissent à la production d'images et de vidéos très réalistes et de textes. Ces capacités sont associées à la notion de GenAI.

Différentes définitions de la notion d'IA et de GenAI ont été proposées⁵. Dans ce rapport, nous reprenons celles adoptées par la Confédération qui conçoit un système d'IA comme :

un système automatique capable d'inférer, sur la base des « inputs » (entrées) qu'il reçoit et pour des objectifs explicites ou implicites, comment générer des « outputs » (sorties) tels que des prévisions, des contenus, des recommandations ou des décisions, et qui, ce faisant, peut exercer une influence sur des environnements physiques ou virtuels.⁶

Et qui considère la GenAI comme :

une notion large qui se réfère aux systèmes d'IA entraînés sur la base de grandes quantités de données provenant du monde physique et virtuel afin de générer des données de manière autonome (textes, images, enregistrements sonores, vidéos, simulations, codes, etc.). Ils sont souvent multimodaux, avec par exemple des inputs et/ou des outputs selon une ou plusieurs modalités (texte, image, vidéo, etc.).⁷

Dans cette étude, nous nous appuyons sur un précédent rapport préparé pour la conférence latine des directeurs·trices du numérique dans lequel il est proposé de définir la souveraineté numérique comme :

le développement d'une autonomie stratégique en matière de numérique. Il s'agit du droit et de la capacité des entités politiques à pouvoir utiliser et contrôler de manière

² Matteo Pasquinelli, *The eye of the master: a social history of artificial intelligence*, London New York, Verso, 2023, chap. 1.

³ John McCarthy et al., « A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955 », *AI magazine*, 2006, vol. 27, n° 4, p. 13.

⁴ National Museum of American History, *Electronic Neural Network, Mark I Perceptron*, https://americanhistory.si.edu/collections/object/nmah_334414, 2026, (consulté le 13 février 2026).

⁵ Par exemple, celle des économistes Martin Neil Baly, David Byrne, Aidan Kane et Paul Soto pour qui « Les systèmes GenAI produisent des artefacts adaptés au contexte à l'aide d'un processus stochastique ouvert basé sur des modèles entraînés à partir d'un ensemble de données. Les artefacts peuvent être divers, c'est-à-dire pas uniquement du texte, mais notamment du code informatique, des images, de la musique, des structures chimiques, des environnements de jeu, des preuves mathématiques ou des mouvements de danse, pour n'en citer que quelques-uns ». Martin Baily et al., « Generative AI at the Crossroads: Light Bulb, Dynamo, or Microscope? », *arXiv preprint arXiv:2505.14588*, 2025, p. 73-83.

⁶ Chancellerie fédérale, *Réseau de compétences en intelligence artificielle*, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/kuenstliche_intelligenz/kinetzwirk.html, janvier 2026, (consulté le 3 mars 2026).

⁷ Chancellerie fédérale, « Terminologie - Réseau de compétences en intelligence artificielle ».

autonome (i.e. de manière indépendante et/ou autodéterminée) les biens matériels et immatériels et les services numériques qui impactent significativement la démocratie, l'économie et la société.⁸

La question de la souveraineté numérique à l'âge de l'IA consiste alors à étudier dans quelles conditions l'utilisation de l'IA est compatible avec la préservation d'une autonomie stratégique. Comme nous le verrons au fil de ce rapport, si l'indépendance technologique complète est un horizon inaccessible et pas nécessairement souhaitable, il existe en revanche des leviers pour, selon les domaines, préserver ou accroître l'autonomie stratégique que les autorités publiques exercent au nom de leurs citoyens, en particulier au niveau cantonal et fédéral. Ces leviers concernent d'un côté, les outils eux-mêmes, c'est-à-dire les couches matérielles et logicielles qui participent à l'IA et, d'un autre côté, la manière dont ceux-ci sont utilisés, notamment au sein des administrations. En d'autres termes, la souveraineté numérique ne doit pas être comprise comme une autosuffisance technologique, mais comme la capacité d'un État ou d'une administration à conserver ou accroître ses marges de manœuvre et à maîtriser ses dépendances critiques au niveau des données, des infrastructures, des modèles, des plateformes et des compétences.

Contexte général

Au moment de la rédaction de ce rapport, dans le premier tiers de l'année 2026, le contexte est marqué par deux évolutions qui donnent un caractère particulièrement aigu aux questions traitées. En premier lieu, un peu plus de 3 ans après le succès grand public de ChatGPT, la qualité et la robustesse des produits d'IA générative ont fortement progressé. Pour autant, le destin économique de cette technologie reste incertain. Sur le plan opérationnel, les progrès spectaculaires réalisés laissent penser que de larges pans de l'économie sont menacés par une puissante vague d'automatisation⁹. La diffusion virale en Chine d'OpenClaw – un agent d'IA capable de mener de manière autonome des flux de travail combinant des tâches dispersées entre plusieurs services numériques sur un ordinateur (par exemple réserver des billets) – semble marquer une étape supplémentaire dans l'imprégnation de la technologie, qui va de pair avec des risques de sécurité accrus¹⁰. Cependant, au niveau global, les montants vertigineux investis¹¹, le rôle des montages financiers circulaires¹², les coûts colossaux des requêtes¹³, les difficultés à monétiser les gains de productivité¹⁴, mais aussi les besoins énergétiques

⁸ Yaniv Benhamou, Frédéric Bernard et Cédric Durand, *Souveraineté numérique: étude pluridisciplinaire pour la Suisse*, 2023, Genève, Digital Law Center, 2023, p. 48.

⁹ Daniel Thomas et al., « Are Anthropic's new AI work tools game-changing for professionals? », *Financial Times*, 16 févr. 2026p. ; Dario Amodei, *The Adolescence of Technology*, <https://www.darioamodei.com/essay/the-adolescence-of-technology>, janvier 2026, (consulté le 17 février 2026) ; Matt Shumer, *Something Big Is Happening*, <https://shumer.dev/something-big-is-happening>, 9 février 2026, (consulté le 17 février 2026).

¹⁰ Ken IP, *Opinion | Frenzy over AI agent OpenClaw shows the lobster has escaped the pot*, <https://www.scmp.com/opinion/china-opinion/article/3346562/frenzy-over-ai-agent-openclaw-shows-lobster-has-escaped-pot>, 18 mars 2026, (consulté le 18 mars 2026).

¹¹ Meghan Bobrowsky, Drew An-Pham et Alana Pipe, « Big Tech's AI Push Is Costing a Lot More Than the Moon Landing », *Wall Street Journal*, 7 févr. 2026p.

¹² Cédric Sam et al., « A Guide to the Circular Deals Underpinning the AI Boom », *Bloomberg.com*, 22 janv. 2026p.

¹³ Bryce Elder, « How high are OpenAI's compute costs? Possibly a lot higher than we thought », *Financial Times*, 12 nov. 2025p.

¹⁴ Dave Grow, *Unlocking AI's full potential requires operational excellence*, <https://www.technologyreview.com/2025/10/01/1124593/unlocking-ais-full-potential-requires-operational-excellence/>, 1 octobre 2025, (consulté le 3 janvier 2026).

gigantesques¹⁵ font douter de la viabilité des modèles actuels. Entre la bulle de l'IA et le vaste potentiel de restructuration de l'économie, les inconnues sont multiples. D'autant que sur le plan de la régulation, les États-Unis, l'Union Européenne (UE) et la Chine prennent des directions divergentes sans qu'un cadre multilatéral ne s'affirme clairement pour l'instant (voir Annexe A).

En second lieu, la faille qui s'est ouverte dans les relations transatlantiques depuis le début du second mandat de Donald Trump rebat les cartes géopolitiques. L'interdiction d'entrée aux États-Unis faite à l'ancien commissaire européen Thierry Breton qui a orchestré la loi sur les services numériques (DSA) ainsi qu'à quatre responsables européens d'ONG de lutte contre la désinformation¹⁶ témoigne de la détermination des États-Unis à contrer toute régulation de la part de pays tiers susceptible de menacer les rentes des géants du secteur. Au-delà des enjeux économiques, dans le sillage des menaces d'annexion du Groenland, le risque d'une instrumentalisation à des fins de coercition des dépendances numériques par les États-Unis est désormais une préoccupation majeure pour les pays de l'UE¹⁷. Par ailleurs, la Cour pénale internationale, dans la crainte de voir ses services informatiques coupés suite à des sanctions étasuniennes, déploie des solutions alternatives¹⁸. Jusqu'à ces dernières années, c'étaient surtout les investissements chinois qui suscitaient les inquiétudes dans les pays européens, ce n'est plus seulement le cas. La vulnérabilité stratégique associée aux dépendances numériques est une réalité pour l'ensemble des pays, à l'exception des États-Unis et de la Chine¹⁹. Dans ce contexte, les initiatives visant à réduire la dépendance des administrations européennes vis-à-vis des firmes des États-Unis se multiplient, avec notamment une volonté de remettre en cause l'omniprésence de Microsoft. En Allemagne le Land de Schleswig-Holstein est à l'avant-garde de ce mouvement et fait figure de modèle²⁰. En France, la volonté du gouvernement de réduire les dépendances numériques extra-européennes de l'État conduit à la sortie de Windows au profit de postes sous un système d'exploitation Linux²¹. En Suisse également, l'administration fédérale désormais « vise à réduire progressivement et durablement sa dépendance à l'égard de Microsoft »²².

¹⁵ Christian Bogmans et al., « Power hungry: How ai will drive energy demand », *IMF Working Papers*, 2025, vol. 81, n° 4, p. 2025.

¹⁶ Fabienne Schmitt, *Thierry Breton interdit d'entrée aux US : la guerre froide numérique est déclarée entre l'Europe et les États-Unis*, <https://www.lesechos.fr/monde/europe/sanctions-contre-thierry-breton-la-guerre-froide-numerique-est-declaree-entre-washington-et-bruxelles-2206708>, 24 décembre 2025, (consulté le 17 février 2026).

¹⁷ Sam Schechner, Berber Jin et Kim Mackrael, « Europe Prepares for a Nightmare Scenario: The U.S. Blocking Access to Tech », *Wall Street Journal*, 24 janv. 2026p.

¹⁸ Suzi Ring, « ICC staff print files and prepare for blackout as US sanctions loom », *Financial Times*, 30 sept. 2025p.

¹⁹ Cédric Durand et Cecilia Rikap, « “Pour sortir de la dépendance européenne aux Big Tech, il faut une politique numérique non alignée” », *Le Monde*, 9 janv. 2025p.

²⁰ Euractiv, *The German state pioneering digital sovereignty*, <https://www.euractiv.com/news/the-german-state-pioneering-digital-sovereignty/>, 15 septembre 2025, (consulté le 21 avril 2026).

²¹ DINUM, *Souveraineté numérique : l'État accélère la réduction de ses dépendances extra-européennes*, <https://www.numerique.gouv.fr/sinformer/espace-presse/souverainete-numerique-reduction-dependances-extra-europeennes/>, 8 avril 2026, (consulté le 21 avril 2026) ; Pascal Wassmer, *La France veut migrer de Windows à Linux pour sa souveraineté numérique*, <https://www.rts.ch/info/monde/2026/article/la-france-abandonne-windows-pour-linux-une-question-de-souverainete-29209373.html>, 11 avril 2026, (consulté le 21 avril 2026).

²² Stefanie Pauli Radunski Michael, *Bund will sich von Abhängigkeit von Microsoft lösen*, <https://www.nzz.ch/schweiz/plotzliche-kehrwende-der-bund-will-sich-von-abhaengigkeit-von-microsoft-loesen-ld.1934311>, 18 avril 2026, (consulté le 21 avril 2026).

Contexte local

À Genève, l'adoption par votation populaire du 18 juin 2023 d'un nouveau droit constitutionnel à l'intégrité numérique²³ témoigne d'une inquiétude, notamment en ce qui concerne le risque de traitement abusif des données. Plus récemment, les rapides transformations du contexte global trouvent des échos dans les interpellations nombreuses et pressantes adressées aux autorités des cantons romands qui manifestent les craintes du peuple, notamment à travers les questions et propositions des représentant·e·s. Celles-ci renvoient à deux grands types de préoccupations.

Les plus pressantes se situent dans le sillage de la volonté populaire exprimée par l'ajout d'un article dans la Constitution du Canton de Genève. Elles concernent le caractère effectif des garanties sur l'intégrité numérique et l'intégrité de l'action publique dans un contexte d'hégémonie des firmes étasuniennes et des transmissions routinières des données sur des serveurs à l'étranger. Dans la mesure où l'administration déploie des outils numériques, notamment d'IA, la question est celle de la sûreté et de la fiabilité de l'infrastructure informatique utilisée. Ainsi, des parlementaires des cantons de Genève et de Vaud²⁴ pointent les menaces géopolitiques et les risques de dépendance économique. Ils s'inquiètent aussi de la protection des données dès lors que ces firmes états-uniennes sont tenues de collaborer avec les autorités judiciaires de leurs pays et qu'elles travaillent étroitement avec les militaires et les agences de sécurité. La demande est alors celle d'une stratégie de protection et de souveraineté numérique passant notamment par la mobilisation des ressources et des entreprises locales et nationales, le refus de toute forme de transfert de données à des pays tiers, le désengagement des logiciels propriétaires et des solutions d'hébergement numérique états-uniens en général et des services de Microsoft en particulier.

Si les ressources locales ne font pas défaut pour entamer un tel désengagement, leur persistance dans le temps ne va pas de soi. Des entreprises suisses procèdent parfois à des acquisitions, mais ce qui domine, c'est le mouvement inverse avec l'acquisition d'un nombre important de start-ups par des groupes internationaux, témoignant de la vulnérabilité du tissu local²⁵. De la même manière, les efforts effectués pour construire l'infrastructure publique de calcul Alps et développer le grand modèle de langage (« large language model, LLM ») Apertus démontrent que des capacités avancées peuvent être construites localement, mais pour transformer ces essais en succès, leur inscription dans une stratégie de long terme est décisive. Enfin, puisque autonomie stratégique ne veut pas dire autarcie, les conditions de l'intégration de l'écosystème romand dans le contexte national et global constituent une question à part entière.

Un second type de préoccupation porte sur les capacités des administrations publiques à mener à bien leurs missions. Des élu·e·s s'interrogent sur la manière dont l'IA pourrait

²³ Le peuple de Genève, « Art. 21A3 Droit à l'intégrité numérique ».

²⁴ Adrien Genecand, *Stop à la dépendance vis-à-vis des systèmes américains – Pour des solutions IT 100% suisses*, s.l., 2025 ; Julien Nicolet-dit-Félix, *Pour un plan de désengagement des logiciels propriétaires et des solutions d'hébergement numérique états-uniens*, s.l., 2025 ; Guy Mettan, *Pour préserver la souveraineté numérique du canton de Genève*, s.l., 2025 ; Michael Wyssat, 25_POS_36 - *Pour une stratégie cantonale de gestion souveraine du cloud et des données*, <https://www.vd.ch/gc/seances-du-grand-conseil/pont-seance/pont/0f567d48-7d88-4781-b91a-fa9517472457/meeting/1029644>, 25 novembre 2025, (consulté le 18 mars 2026).

²⁵ *Le marché IT suisse bousculé par une vague d'acquisitions en 2025*, <https://www.ictjournal.ch/articles/2025-12-19/le-marche-it-suisse-bouscule-par-une-vague-dacquisitions-en-2025>, 19 décembre 2025, (consulté le 18 mars 2026).

permettre d'optimiser les processus administratifs en termes de réduction des charges, d'amélioration de la précision des décisions et de meilleure anticipation. Ce souci d'efficacité concerne en particulier les domaines de la santé, de la justice, de l'enseignement et de la formation, mais aussi l'administration dans son ensemble²⁶. La question ici posée est celle de la bonne utilisation des ressources publiques en phase avec les objectifs de service public et les valeurs éthiques fondamentales. Mais c'est aussi, au-delà des transformations de l'administration, la manière dont les autorités peuvent accompagner l'arrivée de l'IA dans la vie de tous les jours²⁷.

Parallèlement, des craintes s'expriment aussi sur les biais porteurs de discrimination que les algorithmes d'IA incorporent, répliquent et amplifient, à l'encontre notamment des femmes, des personnes racisées et des plus pauvres. La question ici posée est celle des garanties que se donnent les administrations pour ne pas porter préjudice aux personnes dans l'utilisation qu'elles font de dispositifs algorithmiques et des responsabilités et des recours possibles relativement à ces problèmes²⁸. Si les usagers des services publics sont concernés, la question se pose aussi pour les travailleur·es dans leur rapport avec l'administration qui les emploie.

Méthodologie

Les rapports entre souveraineté et IA se situent à l'intersection de ces différents enjeux technologiques, géopolitiques et locaux. De quelle manière une rupture technologique aussi forte affecte-t-elle les conditions d'exercice de la souveraineté au niveau des cantons, en particulier en ce qui concerne les processus de travail administratif, les usages dans l'économie et au sein de la population, et la manière dont ceux-ci sont modélisés par les rapports avec les acteurs dominants de l'IA ? De quelle manière cette question s'enchaîne-t-elle dans le contexte du fédéralisme helvétique mais aussi des relations asymétriques entre États ?

En examinant ces questions, il s'agit d'apporter aux décideurs des éléments pour éclairer les choix stratégiques à venir en matière de systèmes d'IA, notamment en ce qui concerne les infrastructures, les formations, l'énergie et la durabilité.

Le sujet sur lequel le mandat porte est en pleine évolution et la littérature scientifique n'est pas encore solidement établie, alors même que la production est très importante, en termes de volume, et hétérogène, tant du point de vue du statut des textes (rapports d'expert, analyses de cabinets de consultants, recherches fondamentales, enquêtes journalistiques...) que de la qualité. Pour faire face à cette difficulté, le choix a été fait de s'appuyer sur une grande diversité de sources. Ainsi, ce rapport consiste, pour

²⁶ Michael Wyss, 24_POS_57 - *Intégration de l'IA dans l'administration cantonale d'ici 2035 : Quels défis et transformations pour la santé, la justice et l'enseignement ?*, <https://www.vd.ch/gc/seances-du-grand-conseil/point-seance/point/a9c346c7-7696-4112-9225-d5a575c26eeb/meeting/1026866>, novembre 2024, (consulté le 18 mars 2026).

²⁷ Alexandre Rydlo, *Intervention parlementaire - Intelligence artificielle: accompagnement de l'administration*, <https://www.vd.ch/actualites/decisions-du-conseil-detat/seance-du-conseil-detat/decision/id/b2a0bd19-f4db-4225-99d4-10610d727ff7>, 21 mai 2024, (consulté le 18 mars 2026).

²⁸ Carine Carvalho, 25_POS_13 - *L'état doit prévenir la discrimination algorithmique dans son utilisation de l'intelligence artificielle (IA)*, <https://www.vd.ch/gc/seances-du-grand-conseil/point-seance/point/b988879d-5120-47b3-90bf-6c83aff02ade/meeting/1026879>, 25 février 2025, (consulté le 18 mars 2026).

l'essentiel, en une intégration raisonnée et problématisée de l'état des connaissances dans un domaine où celles-ci évoluent très rapidement. De surcroît, nous avons choisi de compléter cette analyse approfondie de la littérature par un petit nombre d'entretiens avec des expert·e·s académiques et professionnels pour être en phase avec l'état des discussions récentes au sein de la Confédération et d'ancrer l'analyse dans le contexte des cantons romands. A ce titre, ce rapport propose un « tour d'horizon » du sujet et les recommandations doivent être lues à cette aune.

En adoptant une approche holistique de l'IA – intégrant les dimensions technologiques, juridiques, économiques, sociales et environnementales – ce rapport propose un cadre structurant pour analyser les enjeux actuels et identifier des leviers d'action concrets. Le cas suisse sert de fil conducteur pour illustrer ces enjeux dans un contexte institutionnel spécifique, tout en offrant des enseignements transférables à d'autres juridictions. Surtout, cette mise en perspective d'ensemble doit permettre d'éclairer les enjeux au niveau local et de nourrir le processus de décision dans les cantons romands.

La première section du rapport définit un cadre holistique et pose le langage commun afin de permettre une compréhension partagée du phénomène de l'IA. La seconde section revient sur les enjeux juridiques de la souveraineté numérique à l'âge de l'IA, faisant en particulier le point sur la pluralité des approches réglementaires actuelles et de l'état des discussions dans le contexte suisse. La troisième section apporte des éléments empiriques concernant l'empreinte de l'IA en Suisse. La quatrième section fait le point sur quelques débats saillants concernant les défis socio-économiques de l'IA. La cinquième section propose des pistes pour préserver des capacités de pilotage et renforcer l'autonomie stratégique, en particulier au niveau des cantons.

1. Un langage commun pour une compréhension partagée

L'IA est devenue une infrastructure stratégique. Pourtant, les débats et décisions qui l'entourent sont souvent entravés par des définitions floues et des visions fragmentées. Cette étude part du constat qu'il n'existe pas de pilotage efficace de l'IA sans langage commun ni compréhension partagée de ses implications. Or, sans langage commun, les responsabilités se brouillent, les priorités divergent, ce qui peut contribuer à l'installation de dépendances non maîtrisées ou même non reconnues.

Un langage commun, à l'inverse, constitue un cadre dans lequel il est envisageable d'aligner les acteurs, de structurer les décisions et d'assurer la cohérence stratégique. En effet, une compréhension partagée des concepts facilite l'échange d'expériences et de connaissances, simplifie la communication autour des idées, des projets et des prestations, et renforce la capacité collective à orienter et maîtriser l'action publique.

Afin de favoriser l'émergence d'un tel langage commun, ce chapitre propose de clarifier les notions clés et d'esquisser le cadre holistique déployé dans ses dimensions juridiques, socioéconomiques et stratégiques dans les chapitres suivants.

1.1. L'IA comme système socio-technique

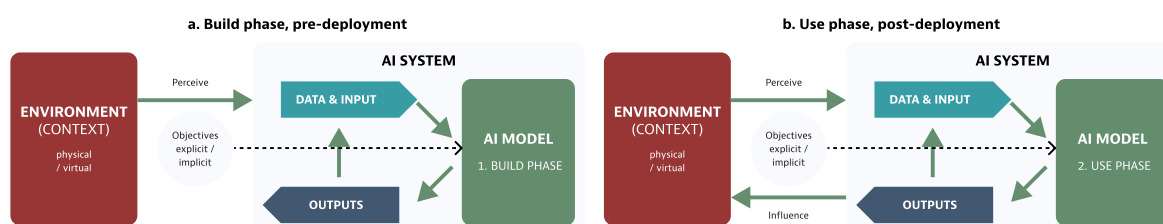
Cette étude s'appuie sur la terminologie adoptée par l'administration de la Confédération et qui s'appuie elle-même sur celle de l'Organisation de coopération et de développement économiques²⁹. Ce choix vise à assurer une cohérence conceptuelle avec les cadres de référence internationaux et fédéraux, condition essentielle à l'interopérabilité des approches, à la comparabilité des pratiques et à la clarté du pilotage public.

Ainsi, le Réseau de compétences en intelligence artificielle de la Confédération définit dans le cadre de l'administration, un **système d'IA** comme « un système automatique capable d'inférer, sur la base des « inputs » (entrées) qu'il reçoit et pour des objectifs explicites ou implicites, comment générer des « outputs » (sorties) tels que des prévisions, des contenus, des recommandations ou des décisions, et qui, ce faisant, peut exercer une influence sur des environnements physiques ou virtuels. Les systèmes d'IA peuvent être dotés d'une autonomie plus ou moins grande, allant des agents conversationnels qui prennent en charge les demandes des citoyens aux modèles de prévision pour la planification du trafic et des interventions, en passant par l'aide à la décision pour les demandes » (Figure 1).³⁰

²⁹ Chancellerie fédérale, « Réseau de compétences en intelligence artificielle », art cit ; OCDE, *Recommandations du Conseil sur l'intelligence artificielle*, <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449>, 3 mai 2024, (consulté le 3 mars 2026) ; Chancellerie fédérale, *SB021 - Stratégie pour l'utilisation de systèmes d'IA dans l'administration fédérale*, <https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben/sb021-strategie-einsatz-von-ki-systemen-in-der-bundesverwaltung.html>, 11 décembre 2025, (consulté le 3 mars 2026).

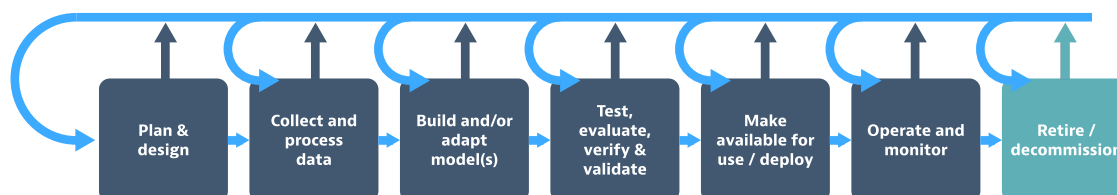
³⁰ Chancellerie fédérale, « Réseau de compétences en intelligence artificielle », art cit.

Figure 1: Le système d'IA : développement des modèles (a) et déploiement (b)³¹



Les systèmes d'IA doivent être compris de manière dynamique dans le cadre d'un **cycle de vie** qui comprend les phases suivantes : planification et conception ; collecte et traitement des données ; création et adaptation de modèles ; test, évaluation, vérification et validation ; mise à disposition et déploiement ; fonctionnement / surveillance ; mise hors service / décommissionnement. Ces phases se déroulent souvent de manière itérative et ne sont pas nécessairement séquentielles (Figure 2). Il est important pour les administrations de prendre en compte cette temporalité dans leur utilisation des systèmes d'IA, en particulier en ce qui concerne l'anticipation des effets de verrouillage.

Figure 2: Le cycle de vie d'un système d'IA³²



La production de prestations d'IA repose sur « trois couches principales : le calcul, les données et les modèles. La couche calcul fait référence à l'infrastructure physique et logicielle qui permet le développement et le déploiement de l'IA, notamment les processeurs spécialisés, les frameworks logiciels et les centres de données. Les logiciels peuvent également être considérés comme une couche transversale qui couvre l'ensemble de la pile IA. La couche données concerne le stockage, le traitement et le transfert des ensembles de données utilisés dans les phases pré et post-déploiement »³³.

Maintenant, si l'on s'en tient aux systèmes de GenAI plus spécifiquement, la Figure 3 schématise l'**empilement de fonctions matérielles et logicielles** qui lui correspond. Des puces de haute performance (1) sont déployées dans des centres de données spécialisés (2) afin de développer des modèles (3) qui sont ensuite déployés dans des centres de données qui traitent les requêtes (4) que les utilisateurs (7) font parvenir à travers les environnements système (6) qui mettent à leur disposition des applications

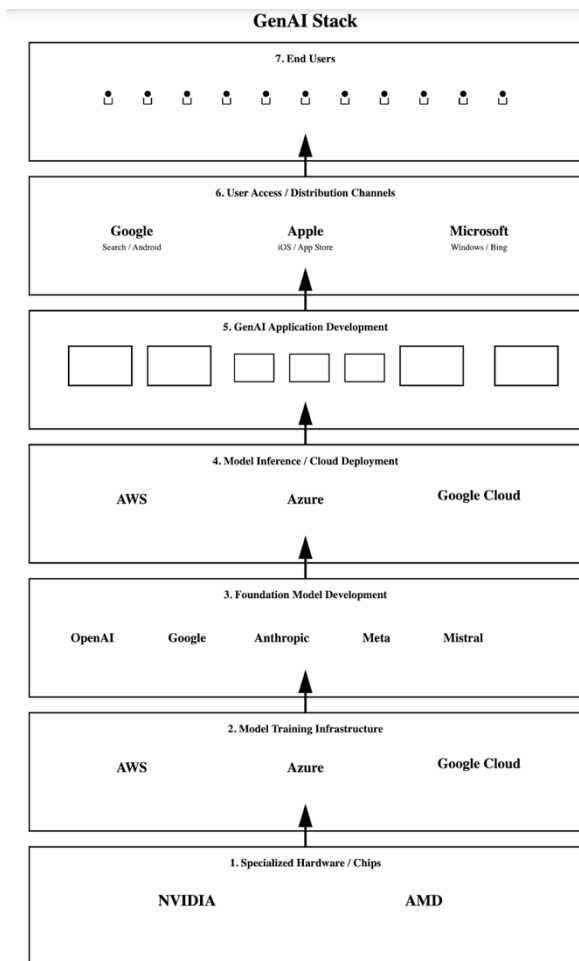
³¹ OECD, *AI Principles Overview*, <https://oecd.ai/en/principles>, 2026, (consulté le 3 mars 2026).

³² *Ibid.*

³³ Alek Tarkowski et al., *Public AI: Policies for democratic and sustainable AI infrastructures*, <https://oecd.ai/en/wonk/public-ai-policies-for-democratic-and-sustainable-ai-infrastructures>, 5 décembre 2025, (consulté le 8 mars 2026).

proposant des services d'IA (5). Cet empilement constitue, avec les données et les compétences, l'espace stratégique où se pose la question de la souveraineté.

Figure 3: L'empilement de fonctions dans un système de GenAI avec des exemples des firmes qui y contribuent³⁴



L'IA doit être comprise comme un **système sociotechnique doté d'un cycle de vie**. Un tel système ne se réduit pas à un algorithme ou à un modèle isolé. Il repose sur un **empilement matériel et logiciel** (les modèles, les infrastructures et les interfaces numériques), se fonde sur **des données** et exige **des compétences individuelles, processus organisationnels et un cadre institutionnel** (culturel, économique, juridique...) pour se déployer.

Les systèmes d'IA forment donc des systèmes sociotechniques complexes dont les effets émergent de l'interaction entre ces diverses composantes. C'est à l'aune de cette complexité socio-technique que se pose la question de la souveraineté.

³⁴ Mihir Kshirsagar, *Lifespan of AI Chips: The \$300 Billion Question*, <https://blog.citp.princeton.edu/2025/10/15/lifespan-of-ai-chips-the-300-billion-question/>, 15 octobre 2025, (consulté le 3 mars 2026).

1.2. Souveraineté numérique et marges de manœuvre

Fin novembre 2025, le Conseil fédéral a approuvé un rapport intitulé « Souveraineté numérique de la Suisse » dans lequel la souveraineté numérique est définie comme « le fait de disposer d'une capacité de contrôle et d'action nécessaire dans l'espace numérique afin de garantir l'exécution des tâches publiques »³⁵. Le terme « espace numérique » désigne « l'ensemble des infrastructures d'information et de communication (matériel et logiciels) qui échangent, collectent, stockent et traitent des données ou les transforment en actions (physiques), ainsi que les interactions entre personnes, organisations et États qui en résultent »³⁶. Cette définition fait de la souveraineté numérique un problème de pilotage stratégique de l'action publique. Il s'agit d'une question de gouvernance technologique visant la maîtrise durable des dépendances numériques.

La Swiss Data Alliance (SDA) a proposé de concevoir la souveraineté numérique comme « la capacité d'un État, dans l'espace numérique, à définir sa propre juridiction au niveau international (en tenant compte de la souveraineté reconnue des autres États), à définir ses propres affaires intérieures et à défendre les deux »³⁷. Si elle rejoint le Conseil fédéral en soulignant la capacité de l'État à se positionner de manière autonome, elle insiste aussi sur l'importance de défendre ses intérêts face à d'autres acteurs et de clarifier les responsabilités et les délimitations dans un environnement numérique globalisé.

Comme le Conseil fédéral, la Conférence latine des directeurs du numérique (CLDN) insiste sur la dimension multidimensionnelle et stratégique lorsqu'elle indique que la souveraineté numérique « désigne la capacité des autorités à maintenir leur autonomie stratégique, soit à pouvoir utiliser et contrôler de manière autonome les biens matériels et immatériels et les services numériques qui impactent l'économie, la société et la démocratie »³⁸.

Ces trois définitions convergent sur un point essentiel : la souveraineté numérique repose sur une capacité effective de décision, d'arbitrage et d'action, autrement dit ce qui est en jeu c'est une autonomie stratégique. Le Conseil fédéral adopte la perspective de l'action administrative, la SDA met l'accent sur la dimension internationale du problème et la CLDN insiste sur les finalités politiques — économie, société, démocratie — qui justifient cette volonté d'autonomie.

En résumé, dans le contexte helvétique, la souveraineté numérique peut être comprise comme un enjeu de pilotage stratégique dans l'espace numérique de manière à préserver l'intégrité de l'action publique conformément au mandat démocratique qui la fonde. Dans un environnement très internationalisé et fortement contraint sur le plan technologique, la souveraineté numérique soulève la question des marges de manœuvre que se donnent les autorités en matière de réglementation, d'orientation des investissements, d'encadrement des usages et de gestion des dépendances et des capacités technologiques.

³⁵ Le Conseil fédéral, *Souveraineté numérique de la Suisse*, Berne, 2025, p. 6.

³⁶ *Ibid.*, p. 5.

³⁷ Swiss Data Alliance, *Souveraineté numérique : façonner l'avenir numérique de la Suisse (livre blanc)*, s.l., 2025, p. 14.

³⁸ <https://cldn.ch/wp-content/uploads/2023/05/Souverainete-numerique-Etude-pluridisciplinaire.pdf>

1.3. Une approche holistique de l'IA

Compte tenu de la complexité et de la nature multidimensionnelle de l'IA, il est indispensable de disposer d'un cadre conceptuel permettant de prendre en compte l'ensemble des aspects pertinents. C'est ce que propose de faire le modèle présenté ci-après, qui vise à clarifier les enjeux de l'IA du point de vue de la souveraineté, notamment, mais pas exclusivement, en ce qui concerne l'usage de cet outil au sein de l'administration publique.

Les huit dimensions définies constituent une grille de lecture fonctionnelle de l'utilisation de l'IA dans l'administration.³⁹ Dans une logique de pilotage stratégique, chacune de ces dimensions constitue un champ où se définissent les marges de manœuvre pour l'action des autorités politiques et de l'administration.

- a. **Transformation numérique de l'administration (processus et services)** — L'IA n'est pas une fin en soi, mais peut être un levier d'amélioration des processus et des prestations, notamment grâce à l'automatisation de certains processus métiers et de support. Elle peut à ce titre jouer un rôle dans le renforcement et l'amélioration des services publics et de l'action administrative. (*Éléments illustratifs : automatisation des processus, services centrés sur les usagers et/ou citoyens.*)
- b. **Stratégie** — Le déploiement maîtrisé de l'IA exige des choix stratégiques cohérents. Cela comprend l'identification des cas d'usage pertinents et des situations où l'utilisation est inappropriée, la définition d'objectifs, de mesures et d'investissements, ainsi que le suivi et l'évaluation continus des résultats obtenus. L'alignement avec les stratégies existantes de l'administration est déterminant. (*Éléments illustratifs : vision, mission, ambition, objectifs stratégiques, feuille de route, plan de mise en œuvre.*)
- c. **Gouvernance et régulation** — La mise en œuvre de cette stratégie repose sur un cadre juridique et organisationnel solide. Celui-ci définit notamment les conditions d'usage d'outils d'IA et leurs limites, en particulier pour la prise de décision administrative (p. ex. octroi d'une autorisation, attribution d'une subvention, priorisation de dossiers...) ainsi que les mécanismes de contrôle et de supervision. Les rôles, structures et processus doivent être clairement définis et rendus transparents. (*Éléments illustratifs : législation, directives, conformité, supervision, audit.*)

³⁹ Ces dimensions d'analyse de l'IA correspondent à celles qui ont été utilisées ces dernières années au sein de l'administration fédérale dans le cadre des travaux visant à développer davantage la coordination pour l'utilisation de l'IA dans l'administration fédérale: voir par exemple l'annexe de la Stratégie partielle pour l'utilisation de systèmes d'IA dans l'administration fédérale (Mars 2025 ; <https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben/sb021-strategie-einsatz-von-ki-systemen-in-der-bundesverwaltung.html>) et le concept visant à développer la coordination pour l'utilisation de l'IA dans l'administration fédérale (Décembre 2025 ; <https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/kuenstliche-intelligenz.html>).

- d. **Données** — Les données constituent le fondement de l'IA. Leur qualité, leur intégrité et leur disponibilité sont déterminantes. Cela implique un management efficace des données, le respect de la protection des données, l'assurance de la qualité, ainsi que leur interopérabilité. (*Éléments illustratifs : stratégie des données, gouvernance des données, sécurité et qualité des données.*)
- e. **Éthique** — L'utilisation de l'IA doit respecter des principes éthiques de protection de la personnalité, ne pas interférer avec l'intégrité des processus démocratiques et juridiques, ne pas générer de biais discriminatoires et permettre la pérennité et la soutenabilité écologique des services mis en place. La protection des droits et de la dignité des individus, la qualité des relations sociales et politiques, ainsi que le métabolisme écologique ne doivent pas être dégradés du fait de décisions automatisées. (*Éléments illustratifs : lignes directrices, codes de conduite, codes de bonnes pratiques*⁴⁰.)
- f. **Algorithmes** — Le développement, la mise en œuvre et l'évaluation des performances des systèmes d'IA nécessitent une expertise spécialisée ainsi qu'un contrôle rigoureux. La validation, les tests, le monitoring continu et l'amélioration des modèles constituent des éléments essentiels. (*Éléments illustratifs : développement de solutions, validation, monitoring, assurance qualité.*)
- g. **Compétences et culture** — Le déploiement réussi de l'IA suppose le développement de compétences organisationnelles et d'une culture favorable. Cela inclut la formation, le recrutement ciblé, la sensibilisation aux opportunités et aux risques de l'IA, la gestion du changement et une communication transparente. (*Éléments illustratifs : formation, leadership, profils de rôles, recrutement, gestion du changement.*)
- h. **Outils et plateformes** — L'utilisation de l'IA repose sur des solutions logicielles, des plateformes et des infrastructures qui doivent être adaptées à l'action administrative. Il convient d'assurer la cybersécurité, la conformité, l'interopérabilité ainsi que la viabilité financière et opérationnelle des solutions retenues. Il importe de gérer la tension entre, d'une part, les attentes des usagers familiers d'outils commerciaux très performants et, d'autre part, l'importance d'assurer le déploiement d'outils « maison » parfois moins performants mais seuls garants de l'intégrité du processus administratif. Une autre tension concerne la temporalité. Dans un contexte d'évolution technologique très rapide et d'instabilité du cadre juridique, les outils ne doivent pas empêcher une action administrative qui s'inscrit dans le temps long. Enfin, un dilemme puissance/fiabilité peut surgir dès lors que des critères d'intégrité de l'action publique questionnent la légitimité de recourir aux services des acteurs dominants.

⁴⁰ Par exemple, le Code de bonnes pratiques de la Confédération pour une science des données (et IA) centrée sur l'être humain et digne de confiance (<https://www.bfs.admin.ch/asset/fr/29325685>).

(Éléments illustratifs : architecture, applications, infrastructure IT, stockage et capacités de calcul.)

Plusieurs thématiques transversales traversent l'ensemble de ces dimensions et influencent directement les marges de manœuvre stratégiques :

- **Approvisionnement** : acquisition stratégique et conforme des technologies, données et services, gestion des dépendances fournisseurs.
- **Standards** : respect de normes garantissant qualité, sécurité, interopérabilité et compatibilité.
- **Confiance** : transparence, respect des droits fondamentaux et usage responsable des données.
- **Collaboration** : coopération entre entités administratives, autres niveaux étatiques, milieux académiques, société civile et économie.
- **(Cyber)sécurité** : gestion des risques techniques, juridiques et organisationnels.

Afin d'opérationnaliser cette approche holistique, il convient de structurer les différentes dimensions de l'IA sous l'angle du pilotage stratégique, tout en gardant à l'esprit les thématiques transversales susmentionnées. Bien que la question de la souveraineté se pose dans sa globalité, les dimensions identifiées constituent des champs d'action dans lesquels l'administration doit être en mesure d'apprécier des choix éclairés, d'arbitrer des priorités et de maîtriser des interdépendances.

Le Tableau 1 synthétise ces dimensions en mettant en évidence, pour chacune d'elles, la finalité de pilotage, les questions stratégiques et les leviers d'action correspondants. Il permet de relier les principes conceptuels présentés ci-dessus à des mécanismes concrets de gouvernance et de mise en œuvre.

Tableau 1: Approche holistique du pilotage stratégique de l'IA

DIMENSION	FINALITÉ	QUESTIONS STRATÉGIQUES	LEVIERS D'ACTION
Transformation numérique	Créer de la valeur publique tangible	Quels processus optimiser ? Quel impact pour les usagers ?	Automatisation ciblée, redesign des processus, intégration dans l'architecture d'entreprise
Stratégie⁴¹	Orienter les priorités et les investissements	Pourquoi utiliser l'IA ? Pour quels objectifs publics ? Avec quels indicateurs de succès ?	Vision, objectifs stratégiques, feuille de route, allocation des ressources
Gouvernance et régulation	Garantir un cadre légitime, maîtrisé et contrôlable	Qui décide ? Qui supervise ? Quels usages sont autorisés ou interdits ?	Cadre légal, directives internes, mécanismes d'audit, clarification des rôles
Données	Assurer la qualité et la maîtrise du socle informationnel	Les données sont-elles fiables, interopérables et protégées ?	Gouvernance des données, stratégie des données, assurance qualité, sécurité
Éthique et comportement	Garantir la légitimité et la confiance	Les droits fondamentaux sont-ils respectés ? Les décisions sont-elles explicables ?	Lignes directrices éthiques, évaluations d'impact, transparence
Algorithmes	Assurer robustesse et performance	Les modèles sont-ils validés, surveillés et documentés ?	Validation, tests, monitoring continu, assurance qualité
Compétences et culture	Développer la capacité organisationnelle	L'administration dispose-t-elle des compétences nécessaires ?	Formation, recrutement, leadership, gestion du changement
Outils et plateformes	Garantir sécurité et soutenabilité technique	Les infrastructures sont-elles sûres, interopérables et durables ?	Architecture IT, cybersécurité, gestion des fournisseurs, choix technologiques

Ce cadre d'analyse de l'IA indique que la souveraineté numérique ne relève pas d'un objectif déclaratif, mais se concrétise dans les marges de manœuvre que se donnent les autorités publiques pour orienter, arbitrer et maîtriser ces différentes dimensions⁴². La question est donc celle des degrés de souveraineté auxquels parvient une société donnée, compte tenu de ses préférences et des relations de dépendance technologique existantes vis-à-vis du reste du monde, mais aussi, plus précisément, de ses rapports géopolitiques avec les autres États et de l'empreinte et de l'influence des firmes dominantes dans le domaine de l'IA. En ce sens, la souveraineté renvoie fondamentalement à une question d'agence et de choix : la capacité d'une autorité politique ou d'une administration à prendre des décisions délibérées et orientées vers

⁴¹ L'Administration numérique suisse a publié, en février 2026, un document présentant la liste des tâches nécessaires à l'élaboration d'une stratégie en matière d'IA (https://www.administration-numerique-suisse.ch/application/files/6217/7131/6338/ANS_-_Liste_des_taches_pour_l_elaboration_d_une_strategie_en_matiere_d_ia.pdf).

⁴² Le rapport de janvier 2026 du Tony Blair Institute for Global Change «*Sovereignty in the Age of AI: Strategic Choices, Structural Dependencies and the Long Game Ahead*» souligne également que la souveraineté ne dépend pas d'un facteur isolé, mais de la capacité à agir sur les différentes dimensions de manière coordonnée, à préserver des capacités de repli et à maintenir des options stratégiques ouvertes dans un environnement structuré par de fortes asymétries et de puissantes interdépendances. Hilda Barasa et al., *Sovereignty in the Age of AI: Strategic Choices, Structural Dependencies and the Long Game Ahead*, London, Tony Blair Institute for Global Change, 2026.

l'avenir quant à la manière dont l'IA est intégrée, gouvernée et utilisée en cohérence avec ses objectifs nationaux.

1.4. Acteurs et champs d'application

Si l'IA constitue un système sociotechnique structuré par différentes couches interdépendantes, et si la souveraineté numérique renvoie à la capacité d'exercer un pilotage stratégique sur ces couches, alors la question centrale devient celle des acteurs qui portent, influencent ou contraignent ce pilotage.

La gouvernance de l'IA implique une pluralité d'acteurs aux intérêts divergents et se déploie dans une variété d'espaces socioéconomiques, ce qui appelle des mécanismes de coordination adaptés.

L'IA mobilise simultanément des autorités publiques, des entreprises nationales et étrangères, des infrastructures critiques, des milieux académiques, des organisations de la société civile ainsi que des usagers et/ou citoyens directement concernés par les applications d'IA mises en œuvre. Ces acteurs disposent de ressources, de compétences et de capacités d'influence très inégales. Leurs objectifs — innovation, efficacité, compétitivité, protection des droits fondamentaux, sécurité ou rentabilité — ne convergent pas nécessairement.

Par ailleurs, les champs d'application de l'IA dans l'administration sont multiples : automatisation de processus internes, aide à la décision, prestations numériques aux citoyens, analyse prédictive, cybersécurité ou encore soutien à l'élaboration des politiques publiques. Chaque domaine soulève des enjeux spécifiques en matière de responsabilité, de transparence et de gestion des risques.

Dans un tel environnement, la gouvernance de l'IA ne se limite pas à la seule mise en œuvre de normes. Elle consiste à organiser les interactions entre acteurs aux intérêts parfois divergents, à arbitrer des tensions structurelles et à préserver des marges de manœuvre stratégiques pour la puissance publique qui agit au nom du peuple. C'est à celle-ci que revient de mettre en œuvre les mécanismes de gouvernance de l'IA en associant les différents acteurs afin d'évaluer et d'arbitrer la manière dont les décisions en matière d'IA affectent la souveraineté dans ses différentes dimensions.

1.5. Le contexte helvétique

La Suisse, par son fédéralisme et son ouverture internationale, constitue un cas d'étude particulièrement pertinent pour analyser les tensions entre innovation, régulation et souveraineté numérique.

Les travaux du Conseil fédéral sur la souveraineté numérique constituent un point de référence central dans ce contexte. En novembre 2025, le Conseil fédéral a approuvé un

rapport définissant la souveraineté numérique comme la capacité de contrôle et d'action nécessaire pour garantir l'exécution des tâches de l'État dans l'espace numérique (voir la section 1.2). Cette définition met l'accent sur la capacité d'agir, d'orienter et de maîtriser les dépendances dans un environnement technologique interdépendant.

Dans le prolongement de ces travaux, des lignes directrices pour la souveraineté numérique de l'administration fédérale ont été adoptées par le Conseil fédéral lors de sa séance du 12 décembre 2025, afin d'assurer une compréhension uniforme du concept et d'en renforcer la mise en œuvre opérationnelle. Ces lignes directrices visent notamment à clarifier les responsabilités, à renforcer la résilience des infrastructures critiques, à encadrer les dépendances technologiques et à garantir la protection des données et des droits fondamentaux dans les projets numériques stratégiques.

Parallèlement, la Stratégie « Suisse numérique » identifie la souveraineté numérique comme un thème prioritaire pour 2026 et souligne la nécessité de préserver la capacité d'action de l'État dans un environnement numérique globalisé. Elle met en évidence l'importance de la coordination entre la Confédération, les cantons et les communes, ainsi que l'ouverture internationale de la Suisse, qui implique une gestion stratégique des interdépendances technologiques et économiques.

Le fédéralisme suisse constitue à cet égard à la fois une force et un défi. Il favorise l'expérimentation, l'innovation locale et la proximité avec les usagers et/ou citoyens, mais il complexifie également la coordination multiniveaux, l'harmonisation des standards et la mutualisation des capacités critiques. La capacité à exercer un pilotage stratégique cohérent dépend ainsi de mécanismes d'alignement efficaces entre les différents niveaux institutionnels.

Le contexte helvétique illustre ainsi de manière concrète les tensions identifiées dans les sections précédentes : nécessité d'un langage commun dans un système multiniveau, arbitrage entre contrôle et dépendance dans un environnement international ouvert, et recherche d'un pilotage stratégique cohérent à travers des compétences institutionnellement fragmentées.

Dans un système fédéral ouvert comme celui de la Suisse, la souveraineté numérique n'est pas un état donné, mais un équilibre à construire en permanence entre coordination interne, interdépendance internationale et capacité d'action stratégique.

1.6. Conclusion

Ce chapitre a établi les fondements conceptuels de l'IA et de la souveraineté numérique. Il a montré que le pilotage stratégique exige une compréhension systémique de l'IA comme système sociotechnique, une approche holistique intégrant ses différentes dimensions et une conscience de la diversité des acteurs et des champs concernés.

Autrement dit, si l'IA constitue un système sociotechnique et si la souveraineté renvoie à la capacité de pilotage stratégique dans un monde interdépendant, alors son analyse ne

peut être sectorielle ou fragmentée. Elle exige une approche intégrée, prenant en compte l'ensemble des dimensions et les différents niveaux auxquels se situent son développement, son déploiement et ses effets.

Dans un tel contexte, la souveraineté numérique ne s'apparente pas à une quête illusoire d'autarcie, mais pose la question de la faculté pour les autorités publiques d'orienter les interdépendances inhérentes à l'écosystème de l'IA en fonction d'une appréciation des risques ou des préjudices économiques, sociaux, politiques, géopolitiques et écologiques que la société est prête à accepter dans ses manières d'utiliser et de rendre accessible cet outil. Autrement dit, la souveraineté numérique concerne la capacité à exercer un pilotage stratégique sur l'ensemble du système sociotechnique IA — données, infrastructures, compétences, usages et cadres institutionnels — en mobilisant les leviers d'action que constituent la réglementation, les investissements technologiques, les formes de déploiement des outils dans l'administration, la politique contractuelle, et le développement des capacités à travers la formation. Elle suppose des arbitrages explicites et une coordination cohérente entre niveaux institutionnels.

À l'ère de l'IA, la souveraineté numérique se construit par des choix stratégiques cohérents, assumés et continuellement réévalués face aux interdépendances technologiques et géopolitiques. Elle n'est pas l'absence de dépendance, ou d'exposition aux risques mais la maîtrise de celles-ci par des mesures d'anticipation, de prévention, de protection et de réduction des vulnérabilités et des préjudices associés.

Cette conception stratégique de la souveraineté numérique montre que les marges de manœuvre de la puissance publique ne peuvent être appréciées uniquement sous l'angle technologique. Elles résultent d'un ensemble d'actes délibérés au niveau institutionnel, juridique, économique, organisationnel et géopolitique de manière à structurer un environnement numérique conforme aux attentes de la population.

2. Enjeux juridiques de la souveraineté numérique à l'ère de l'IA

2.1. Remarques préalables

Stratégie de la Confédération en matière de souveraineté numérique, d'IA et de régulation

À l'échelle fédérale, la Confédération prévoit plusieurs mesures en matière de **souveraineté numérique**, dont la mise en place d'un groupe de travail interdépartemental destiné à évaluer les risques et les mesures à prendre sur le plan légal et technique⁴³. En **matière d'IA**, la Confédération prévoit le déploiement de systèmes d'IA en vue *“d’optimiser les processus et les services de l’administration fédérale, d’aider les cadres et les collaborateurs et de découvrir de nouvelles solutions”*⁴⁴. Plus spécifiquement, **en matière de souveraineté numérique relative à l'IA**, la Confédération prévoit notamment : (i) le développement de solutions internes (alternative à des outils tiers) et la capacité d'adapter, intégrer et gouverner des modèles⁴⁵ en interne ; (ii) une traçabilité des données (transparence, contrôle humain et responsabilité des décisions algorithmiques). **En matière de régulation de l'IA**, la Confédération élabore actuellement un projet de loi (AP-IA⁴⁶). L'AP-IA vise à assurer la mise en œuvre de la Convention du Conseil de l'Europe, avec une régulation suivant trois objectifs : (i) le renforcement de la Suisse en tant que pôle d'innovation ; (ii) le renforcement de la confiance de la population en l'IA (ex. transparence, de traçabilité et de légitimité des processus et des décisions recourant à l'IA)⁴⁷.

L'AP-IA privilégie des adaptations juridiques aussi sectorielles que possible, avec une régulation transversale limitée aux domaines centraux (ex. protection des données, transparence). Il prévoit aussi une combinaison de normes contraignantes (*hard-law*) et non contraignantes (*soft-law*) pour garder une flexibilité face à l'évolution rapide de l'IA⁴⁸. Par comparaison avec l'étranger, la régulation de l'IA fait l'objet de multiples approches⁴⁹. Par exemple, les **Etats-Unis** ont une approche sectorielle avec peu de lois fédérales générales, des interventions étatiques ciblées (FTC, sécurité nationale) et un *leadership* du marché privé. L'**UE** a une approche basée sur les risques et les droits fondamentaux, matérialisée dans une régulation horizontale (IA Act). La **Chine** a une approche centralisée et étatique avec une régulation rapide et prescriptive (ex.

⁴³ Rapport du Conseil fédéral, Souveraineté numérique de la Suisse, 26 novembre 2025, notamment 1 et 23.

⁴⁴ Chancellerie fédérale ChF, Stratégie Utilisation de systèmes d'IA dans l'administration fédérale, 21 mars 2025, 3.

⁴⁵ CHf, Plan de mise en œuvre Sous-stratégie en matière d'IA. La Confédération parle de développer des modèles maîtrisés et réutilisables (notamment en Open Source via les exigences LMeta), de mettre à disposition une IA générative interne comme service standard, le renforcement du CNAI et le « marché d'IA ». Toutefois, il n'y a pas d'objectif explicite de développer des modèles fondamentaux souverains à grande échelle. L'approche reste orientée vers l'intégration et l'adaptation plutôt que l'autonomie technologique.

⁴⁶ L'un des auteurs du présent rapport, Yaniv Benhamou, est membre du groupe d'accompagnement de la Confédération Régulation de l'IA. Les propos contenus dans ce rapport n'engagent pas le groupe d'accompagnement mais uniquement les auteurs de ce présent rapport.

⁴⁷ Conseil fédéral, Réglementation de l'IA : le Conseil fédéral veut ratifier la Convention du Conseil de l'Europe, 12 février 2025; OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificielle, 31 août 2024; OFCOM, Etat des lieux sur la réglementation de l'intelligence artificielle, 19.

⁴⁸ Conseil fédéral, Réglementation de l'IA : le Conseil fédéral veut ratifier la Convention du Conseil de l'Europe.

⁴⁹ Certains des pays (Royaume-Uni et Israël) privilégient une approche sectorielle, car elle paraît plus adaptée à l'évolution dynamique des technologies d'IA. D'autres (Etats membres de l'UE, Canada, Brésil, Corée du Sud) choisissent une approche horizontale, soit des lois horizontales applicables à tous les secteurs pour relever les défis principaux de manière uniforme. Cf. OFCOM, Etat des lieux sur la réglementation de l'intelligence artificielle.

algorithmes, GenAI), une forte supervision gouvernementale, et un objectif de contrôle social et de leadership technologique⁵⁰. Pour le surplus, les réglementations dans différents pays et régions sont synthétisées en annexe (voir Annexe A) et l'AP-IA commenté ci-dessous (2.4).

Mise en œuvre et fédéralisme

Plusieurs mesures sont envisageables pour renforcer la souveraineté numérique en matière d'IA, dont la mise en œuvre dépend de leurs **destinataires**. Les mesures peuvent s'adresser aux autorités (capacités de l'État de contrôler et d'agir pour accomplir ses tâches publiques) ou à la société dans son ensemble (capacités des personnes et entreprises à décider par elles-mêmes de leurs actes dans le numérique)⁵¹. Les mesures peuvent être par ailleurs du ressort des **différents niveaux de l'État**, de la Confédération, des cantons ou des deux niveaux de l'État simultanément (fédéralisme)⁵². Lorsque le domaine relève de la Confédération, certains domaines sont du ressort de différents départements (ex. littératie des données et d'IA, durabilité, énergie), ce qui suppose une collaboration entre départements. Cette collaboration sera facilitée grâce au pilotage centralisé du déploiement de l'IA dans l'administration aux mains de la Chancellerie fédérale. En effet, la Chancellerie fédérale, en collaboration avec les départements, a élaboré des lignes directrices pour l'ensemble de l'administration fédérale centrale, qui concernent notamment le déploiement de l'IA. Au sein des cantons, dès lors qu'il s'agit de domaines les concernant, les stratégies en matière d'IA et de souveraineté numérique peuvent varier d'un canton à l'autre.

Types de modèles d'IA et d'hébergements

L'administration ou l'entreprise qui souhaite déployer un modèle d'IA (ci-après "déployeur") doit s'assurer du respect du cadre légal. À cette fin, il doit choisir un type de modèle et d'architecture d'hébergement adapté, sachant qu'il en existe une grande variété et que chaque type présente des avantages et des limites.

À titre d'**exemples de modèles**, on songe aux systèmes d'IA pour aider à la prise de décision, à GenAI pour la génération de contenus ou à l'IA agentique à travers des agents IA pour effectuer des tâches sans supervision humaine⁵³.

À titre d'**exemples d'hébergement**, on songe à : une *IA locale (on-premises)* installée sur les serveurs internes de l'utilisateur, une *IA en cloud encadré* hébergée chez un prestataire tiers, mais avec des garanties sur la confidentialité et la localisation des données, et une *IA en cloud public* fonctionnant via une infrastructure entièrement externalisée (ex. ChatGPT ou Gemini). L'IA locale peut être adaptée pour l'administration et les acteurs privés qui disposent des ressources nécessaires, tandis que l'IA en cloud encadré ou public semble plus adaptée pour les acteurs privés qui ne disposent pas de ressources nécessaires pour opérer de tels modèles. À noter que l'IA en cloud public

⁵⁰ Cf. OFCOM, Analyse des réglementations dans différents pays et régions du monde ; OFCOM, Etat des lieux.

⁵¹ Conseil fédéral, Souveraineté numérique de la Suisse, 26 novembre 2025.

⁵² BENHAMOU/BERNARD/DURAND.

⁵³ Avec la GenAI, on distingue souvent entre *large language models (LLM)* basés sur un vaste ensemble de données (*datasets*) et *small language models (SML)* plus petites et optimisées pour des tâches spécifiques, souvent entraînées avec les propres *datasets* de l'utilisateur. On distingue aussi souvent entre modèles propriétaires ou *open source*, ce qui permet de connaître et de réutiliser tout ou partie des composants du modèles (données d'entraînement, poids, architecture). Cf. BENHAMOU 2026.

fonctionne sans contrôle direct sur la localisation ou l'usage des données saisies, et sans garanties contractuelles personnalisées, si bien qu'elle ne garantit pas la protection des données personnelles ni celles soumises à un devoir de confidentialité, sauf à disposer d'un consentement éclairé ou d'une levée valable du secret. A noter aussi que l'IA en cloud encadrée n'offre pas tout le temps les garanties requises (protection des données et confidentialité), en particulier lorsque l'architecture sous-jacente repose sur une IA en cloud public (ex. fonctionnalité intégrée à un environnement plus global de l'utilisateur, tel que suite bureautique ou outil de gestion des contacts). Il incombe dès lors à l'utilisateur de procéder à une évaluation au cas par cas, afin de déterminer si l'outil utilisé respecte les exigences applicables, et, le cas échéant, quel type de modèle et d'hébergement choisir⁵⁴.

Conclusion intermédiaire

Sur cette base, on peut établir que les principaux enjeux juridiques en lien avec la souveraineté numérique en matière d'IA concernent le cadre légal relatif au déploiement de solutions IA au sein de l'administration et des acteurs privés suisses, soit celui relatif à **l'utilisation** (ci-dessous 2.2) et au **développement des modèles d'IA** (ci-dessous 2.3).

Il convient aussi d'examiner quelles mesures sont envisageables pour renforcer la Suisse en tant que pôle d'innovation, tout en assurant le respect des **droits fondamentaux** et la confiance de la population dans l'utilisation et le développement de modèles d'IA (ci-dessous 2.4).

Il convient enfin d'examiner quelles mesures sont envisageables face à la **concentration du pouvoir** des grandes entreprises technologiques (ci-dessous 2.4).

Enfin, pour comprendre le niveau de l'Etat et les destinataires concernés par les mesures, on distinguera suivant que les mesures s'adressent aux acteurs privés ou aux autorités fédérales ou cantonales (ci-dessous 2.5).

2.2. Utilisation de modèles d'IA de fournisseurs IA par l'administration et les acteurs privés : transfert des données

Déployer des modèles d'IA au sein de l'administration et des entreprises et développer des modèles et des infrastructures autonomes supposent généralement un transfert de données d'une entité à une autre, généralement de l'entité utilisatrice du modèle au fournisseur d'IA⁵⁵. Il convient donc de clarifier quelles sont les règles en matière de transfert des données, ou, plus généralement, le cadre légal de l'utilisation des modèles par l'administration et les acteurs privés.

⁵⁴ Pour une présentation des solutions d'hébergement, cf. Lignes directrices FSA concernant l'utilisation de l'IA ; MEHMETAJ, 30.

⁵⁵ On distingue généralement le transfert d'une administration à une autre (G2G), d'une administration à une entreprise privée (G2B) ou d'une entreprise privée à une autre (B2B). Cf. IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2021, 6-7.

Données anonymisées, cryptées ou pseudonymisées

L'administration ou l'entreprise recourant à un modèle d'IA ("déployeur") devra s'assurer des règles en matière de protection des données et de confidentialité. Ces règles ne se poseront que si le fournisseur d'IA a accès au contenu des données, par exemple parce que les données lui sont envoyées en clair ou parce qu'il a accès à la clé de cryptage ou au tableau de correspondance. Elles ne se poseront en revanche pas si le fournisseur d'IA n'a pas accès au contenu des données, par exemple parce qu'elles lui sont envoyées sous forme **anonymisée, cryptée ou pseudonymisée**, que la clé de cryptage, respectivement le tableau de correspondance, reste sous le contrôle de l'utilisateur et qu'il n'existe pas de possibilité d'identification par recoupement des données. Il est ainsi intéressant, voire préférable, de recourir à ce type de solution pour éviter les considérations relatives à la protection des données et la confidentialité qui suivent⁵⁶.

Ces solutions ne sont toutefois **admissibles** que si elles sont réalisées de manière rigoureuse et techniquement effective. Une attention particulière doit être portée à la manière dont les données sont saisies ou transmises à un système d'IA⁵⁷.

Protection des données et confidentialité

Lorsque le déployeur transmet des données à l'outil d'IA, un tel transfert est admissible selon des règles strictes en matière de protection des données. Lorsque le déployeur est un acteur privé ou l'administration fédérale, la **sous-traitance** est admissible lorsque la loi ou une base légale le prévoit⁵⁸, la sous-traitance est encadrée (instructions, contrôles, mesures techniques et organisationnelles dites "TOMs") et aucune obligation de garder le secret ne s'y oppose (art. 9 LPD)⁵⁹. Lorsque le déployeur est une administration cantonale, les lois cantonales sur la protection des données prévoient des règles identiques ou similaires à celles de la LPD, sous réserve de quelques spécificités (ex. exigences contractuelles et/ou de localisation en Suisse)⁶⁰.

En présence d'informations protégées par un **secret de fonction ou professionnel** (ex. art. 320-321 CP ; art. 47 al. 1 let. a LB ; art. 13 al. 2 LLCA)⁶¹, le déployeur doit s'assurer du respect du secret lors de l'utilisation de l'outil d'IA. Si le déployeur recourt à un prestataire IT qui est qualifié d'auxiliaire et soumis au secret professionnel, le consentement du client n'est pas nécessaire⁶². Si le prestataire IT n'est pas qualifié

⁵⁶ BENHAMOU/ERARD/KRAUS.

⁵⁷ MEHMETAJ, 31, recommandant de ne transmettre à l'outil que les informations strictement nécessaires à la tâche attendue, y compris lors du préchargement de documents et de ne jamais effectuer d'anonymisation ou de suppression d'éléments sensibles dans l'interface d'IA en cloud public.

⁵⁸ En droit privé, la sous-traitance est généralement permise et nécessite un contrat. En revanche, la sous-traitance par un organe fédéral nécessite généralement une base légale, en particulier en cas de délégation d'une tâche publique. Cf. ATF 138 II 134, c. 5.1 ; BELLANGER, p. 57.

⁵⁹ EMILIE JACOT-GUILLARMOD, Art. 9 LPD N 4 ss, in LPD : loi fédérale sur la protection des données [Benhamou, Yaniv ; Cottier, Bertil, édit.], Bâle (Helbing Lichtenhahn) 2023.

⁶⁰ MÉTILLE, smetille.ch/2025/11/04.

⁶¹ Le secret de fonction couvre toute information dont un agent public a connaissance dans l'exercice de ses fonctions et qui n'est pas publique. Le secret professionnel couvre toute information dont un professionnel a connaissance dans l'exercice de sa profession (ex. médecins, avocats, ecclésiastiques).

⁶² La notion d'auxiliaire peut être définie comme la personne qui soutient le professionnel l'accomplissement de ses tâches. Son étendue est encore floue. Les prestataires de services d'hébergement en nuage (*Cloud Service Providers*) remplissent en principe cette exigence (ATF 145 II 229, c. 7.3), mais pas nécessairement les fournisseurs d'IA, notamment d'IA *en cloud public* en tant qu'ils ne jouent pas un rôle clair et fonctionnel dans l'accomplissement des tâches du professionnel et n'assurent pas une confidentialité des données suffisantes. Cf. BENHAMOU/ERARD/KRAUS, p. 124 ; CHAPPUIS/ALBERINI, p. 337, 338.

d'auxiliaire, le déployeur devra obtenir l'accord préalable du maître du secret⁶³. La situation est similaire en présence d'informations protégées par un devoir de confidentialité (ex. secrets d'affaires)⁶⁴. L'utilisateur devra obtenir une levée préalable de la confidentialité fondée sur le consentement du client⁶⁵.

En cas de sous-traitance impliquant un **transfert des données hors de Suisse** (p. ex. parce que le sous-traitant est domicilié à l'étranger, utilise des sous-traitants ultérieurs à l'étranger ou fait partie d'un groupe étranger qui pourrait avoir accès aux données depuis l'étranger)⁶⁶, le déployeur devra s'assurer du respect des règles en matière de transfert à l'étranger. À l'égard de l'administration fédérale et des acteurs privés, un tel transfert à l'étranger sera possible dans un pays à niveau de protection adéquat ou, en l'absence d'un niveau de protection adéquat, à la condition de mettre en place des garanties contractuelles avec le prestataire (art. 9 et 16 LPD)⁶⁷. Au sein de l'administration fédérale, sur la base de la **LSI** toutefois, les **données classifiées "secret"** peuvent uniquement être stockées dans le nuage privé sécurisé de la Confédération, tandis que les **données classifiées "interne" ou "confidentiel"** peuvent être stockées dans un nuage public si des mesures contractuelles, techniques et organisationnelles de protection adéquates garantissant le respect du droit applicable sont mises en place⁶⁸. Dans les cantons, le transfert à l'étranger dépend des lois cantonales de protection des données. Certains cantons imposent des conditions strictes (lieu de traitement, contenu du contrat, chiffrement, ou contrôle préalable), tandis que d'autres sont plus souples et n'ajoutent que peu, voire aucune exigence supplémentaire par rapport à la LPD⁶⁹.

Transparence et responsabilité

Au-delà de ces règles en matière de sous-traitance et de confidentialité, les principes de la LPD doivent aussi être respectés, tels que la licéité, la sécurité et le devoir d'information⁷⁰. Par exemple, la personne concernée dont les données sont traitées

⁶³ Sur la levée du secret, cf. notamment BENHAMOU/ERHARD/KRAUS, 122 ss ; MEHMETAJ, 30 s.

⁶⁴ Une telle confidentialité est souvent prévue par les parties à travers des restrictions contractuelles (géographiques, techniques et/ou organisationnelles). Cela est habituel pour des données protégées par des secrets d'affaires, des logiciels propriétaires ou codes sources sensibles, telles que des infrastructures IT critiques, des projets publics ou para-publics ou des secteurs régulés (banque, santé, défense). Cela est en revanche inhabituel pour les contenus peu sensibles, les projets open source et l'hébergement cloud standard grand public. Contractuellement, le titulaire conclut avec le tiers des clauses contractuelles contenant des obligations, telles que des exigences d'hébergement en Suisse ou l'EEE, l'interdiction de transfert hors pays ou à d'autres sous-traitants de 2^{ème} degré sans l'accord écrit ou sur la base d'une liste blanche de pays ou sous-traitants de 2^{ème} degré autorisés.

⁶⁵ MEHMETAJ, 30, notant qu'une telle renonciation doit être formulée de manière claire et spécifique à la situation, soit que le client ait été préalablement informé des risques associés, notamment en cas de recours à une IA en cloud public.

⁶⁶ Un prestataire basé en Suisse mais partie à un groupe étranger (ex. Microsoft) pourrait être amené à communiquer les données qui lui sont confiées aux autorités de la juridiction de la maison-mère en raison des lois applicables à la maison-mère. Les exemples courants sont le US Cloud Act et le règlement E-Evidence, deux réglementations permettant aux autorités de poursuite pénale d'avoir un accès facilité aux données stockées à l'étranger (cf. note de bas de page suivante).

⁶⁷ Conseil fédéral, Souveraineté numérique de la Suisse, 26 novembre 2025, n. 2-3, citant le US Cloud Act et le règlement E-Evidence. Ces deux réglementations permettent aux autorités de poursuite pénale d'avoir un accès facilité aux données stockées à l'étranger ayant une utilité dans le cadre de procédures pénales. Sur cette base, l'arrêt Schrems II repris en substance par le PFPDT, a mis en lumière que dans certains cas, le droit du pays de destination des données met en péril l'efficacité de garanties contractuelles comme les clauses contractuelles types (ex. en raison de droits d'accès étendus des autorités locales qui ne sont pas liées par les garanties contractuelles). Le PFPDT recommande ainsi de clarifier le cadre légal du pays de destination avant d'utiliser des clauses contractuelles standards pour un pays donné (PFPDT, Guide pour l'examen de la licéité, p. 3). Le Swiss-U.S. Data Privacy Framework a réduit la portée pratique des controverses liées aux lois américaines (CLOUD Act/FISA) pour les organisations certifiées. Il n'y a donc plus besoin de mettre en place des clauses contractuelles types et de réaliser une « Analyse d'impact des transferts des données » (AITD) avant un transfert aux États-Unis. Cf. Métille.

⁶⁸ Cf. art. 10 et 12 LSI ; OSI ; Ordonnance Geve ; OCSP ; TF 1C_598/2016.

⁶⁹ MÉTILLE, smetille.ch/2025/11/04.

⁷⁰ Cf. arrêt TAF, 11.7.2011, A-6242/2010, c. 10.3 rappelant que les principes de la LPD doivent être aussi respectés, tels que la licéité, la sécurité et le devoir d'information.

devra pouvoir reconnaître que ses données sont transférées à l'étranger (principe de reconnaissabilité, art. 6 LPD) et, en cas de transfert de pays à niveau de protection non équivalent, être informée des garanties appropriées et des pays dans lesquels les données sont envoyées.

Au-delà des règles en matière de protection des données, les utilisateurs sont aussi tenus de respecter les règles et bonnes pratiques en matière de transparence (ex. dans la recherche, les règles déontologiques en matière d'intégrité scientifique). Dans un contexte d'utilisation publique, chaque contenu principalement généré ou modifié par une IA générative devrait être clairement identifié comme tel. Les utilisateurs sont tenus de signaler à leur hiérarchie l'utilisation d'outils d'IA dans le cadre de leurs fonctions⁷¹.

Au-delà des règles en matière de protection des données, le déployeur restera responsable de l'usage de l'IA (cf. aussi ci-dessous 2.4). En effet, les utilisateurs sont personnellement responsables de l'usage de l'IA, ce qui suppose qu'ils ont une compréhension de base des caractéristiques et des risques inhérents à l'IA avant d'en faire usage (ex. dépendance, biais, hallucinations, données erronées ou incomplètes, protection des données, droit d'auteur, cas échéant, spécificités des clauses contractuelles). La validation finale des contenus ou des décisions générés ou assistés par un outil de GenAI incombe à l'utilisateur.

Conclusion intermédiaire

On observe aujourd'hui deux dynamiques contradictoires. D'un côté, le cadre légal semble assez souple pour permettre une utilisation accrue des modèles d'IA. On observe donc une adoption croissante de l'IA, de manière plus ou moins maîtrisée au sein des entreprises et de l'administration. D'un autre côté, on observe une volonté politique de rapatrier davantage de traitements de données sur le territoire national pour des raisons de sécurité et d'indépendance.

Au-delà du cadre légal souple, l'État peut prendre des mesures politiques afin de renforcer des solutions indigènes plutôt qu'étrangères. Cette tendance s'observe en France et plus récemment en Suisse, où la Confédération souhaite réduire progressivement sa dépendance vis-à-vis de Microsoft, le cas échéant, pour se tourner vers des alternatives *open source* et/ou des acteurs locaux.

Ces décisions pour réduire la dépendance de la Suisse vis-à-vis des prestataires étrangers tels que Microsoft sont toutefois du ressort du politique. Si l'État veut avoir davantage de souveraineté numérique, il serait souhaitable qu'il adopte une approche plus claire et assumée politiquement : si l'on considère que certaines données traitées par l'administration doivent impérativement l'être en Suisse, il faudrait l'inscrire explicitement dans la loi et en assumer les conséquences budgétaires et organisationnelles⁷². Afin de favoriser l'émergence d'acteurs locaux, l'Etat pourrait être tenté de recourir aux appels d'offres. Cela pourrait toutefois être contraire aux règles en

⁷¹ Par exemple les hautes écoles demandent souvent une transparence quant à l'utilisation de GenAI. Cf. par exemple UNIGE, IA générative, guide à l'intention de la communauté universitaire.

⁷² CHAVANNE, ictjournal.ch/interviews/2026-03-05, notant qu'un marché trop fermé privilégiant les fournisseurs suisses poserait en outre des questions de compétitivité pour les entreprises suisses actives à l'international si les autres pays font de même.

matière de marché public, si bien qu'il est recommandé de conduire une analyse juridique complémentaire sur ces règles (ci-dessous 2.5).

2.3. Développement de modèles souverains par l'administration et les acteurs privés : accès aux données

Développer un marché de l'IA, avec des modèles internes et maîtrisés, suppose que l'administration et les acteurs privés aient un accès suffisant à des données d'entraînement de qualité (y compris pour les phases de test et de validation)⁷³.

L'importance de l'accès aux données explique qu'il y ait de nombreux développements législatifs en Suisse et à l'étranger.⁷⁴ Le cadre légal est toutefois fragmenté du fait de la variété des données utilisées pour les systèmes d'IA et du fait que les données peuvent provenir d'une multitude d'acteurs et être soumises à une multitude de régimes légaux différents parfois en tension (p.ex. droit d'auteur, protection des données et des secrets d'affaires)⁷⁵. Cela conduit à une sous-exploitation des données, si bien qu'il est recommandé de prévoir des mécanismes d'accès aux données.

Cela étant, la sous-exploitation des données varie fortement d'un secteur à un autre, si bien qu'une solution unique adaptée à tous les marchés des données n'existe probablement pas⁷⁶. Par ailleurs, faciliter l'accès aux données, par exemple sous forme d'accès gratuit aux données publiques, peut interroger, sachant que cela peut conduire à des risques de responsabilité et que les données publiques sont souvent récupérées par de grandes entreprises technologiques (ex. les données ouvertes de l'Office fédéral de topographie sont réutilisées par Apple et Google pour leur application "Plan" et Google Maps). Il est donc recommandé d'être prudent quant aux modalités et au degré d'ouverture des données publiques, ce qui est développé ci-dessous.

Protection des données

Lorsque l'accès aux données porte sur des **données personnelles**, celles-ci font l'objet d'un régime strict de protection. La protection des données peut apparaître comme un frein à l'innovation, puisque le traitement porte régulièrement atteinte à un ou plusieurs principes de protection des données (notamment reconnaissabilité, proportionnalité, limitation)⁷⁷. Il est rappelé ici que les données personnelles rendues accessibles publiquement (ex. données des réseaux sociaux) continuent à être protégées (art. 5 let. c LPD), seules certaines dérogations sont prévues (ex. art. 17 al. 1 let. d LPD; 30 al. 3 LPD)⁷⁸.

⁷³ Lorsqu'il est question d'accès aux données, on distingue généralement suivant le type de données concernées (données personnelles et non personnelles), suivant le type d'entités concernées (ex. B2B, B2G, G2B) et suivant que l'accès est volontaire ou qu'il est obligatoire. IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2021.

⁷⁴ En droit suisse, il existe plusieurs initiatives qui visent à favoriser l'accès aux données personnelles et non personnelles, notamment la motion CSEC-E 22.3890 "Élaboration d'une loi-cadre sur la réutilisation des données" ; IPI, accès aux données non personnelles dans le secteur privé, 4. Cf. aussi, Alexandre Jotterand, (Non-Personal) Data Sharing in Switzerland: Legal Landscape and Practical Implications, sic! 2025, 441 ss; Jacques de Werra, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non-personnelles (par des licences obligatoires ou des licences « FRAND ») ? In: RSDA 2020, 365 ss.

⁷⁵ BENHAMOU 2020.

⁷⁶ IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2021.

⁷⁷ THOUVENIN, 17.

⁷⁸ FRANCEY, ART. 17 N 1 SS ET ART. 30 N 1 SS, in LPD : loi fédérale sur la protection des données [Benhamou, Yaniv ; Cottier, Bertil, édit.], Bâle (Helbing Lichtenhahn) 2023.

Se pose donc la question de savoir si, du point de vue du principe de licéité, ces traitements peuvent être justifiés par un motif justificatif. A l'égard de traitements effectués par l'administration fédérale et des acteurs privés, la LPD prévoit en effet plusieurs exceptions et motifs justificatifs. Dans le **secteur privé**, le traitement peut être justifié par un intérêt prépondérant, en particulier lorsque les données d'entraînement sont généralement traitées *“à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, si les conditions suivantes sont réunies”* (art. 31 al. 2 let. e LPD)⁷⁹. Dans le **secteur public**, le traitement peut être aussi justifié lorsque ses fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique et que certaines conditions sont réunies (données anonymisées dès que la finalité le permet, non-communication de données sensibles à des privés, consentement de l'organe avant que le destinataire ne communique à des tiers et publication des résultats sans que l'identification des personnes ne soit possible) (art. 39 LPD)⁸⁰. Le traitement de données personnelles automatisé dans le cadre d'essais pilotes peut être aussi autorisé à certaines conditions (art. 35 LPD). Ces motifs justificatifs nécessiteraient toutefois une analyse approfondie afin de voir lesquels pourraient s'appliquer à quelles étapes du développement du modèle d'IA, pour quels usages et à quelles conditions.

Dans les **cantons**, les lois cantonales sur la protection des données prévoient aussi des motifs justificatifs au traitement identiques ou similaires à ceux de la LPD. Les principaux motifs justificatifs sont la base légale. Autrement dit, le traitement de données personnelles par une autorité cantonale est licite s'il repose sur une base légale, une base légale générale étant suffisante pour les données ordinaires, une base légale formelle étant exigée pour les données sensibles (ex. fiscalité, police, santé publique) (art. 35 LIPAD; art. 4-5 LPrD). L'intérêt public prépondérant est aussi parfois prévu comme motif justificatif, en particulier si le traitement est nécessaire à l'accomplissement d'une tâche publique et proportionné au but poursuivi (ex. sécurité publique, santé publique, gestion administrative) (art. 39 LIPAD ; art. 15 LPrD)⁸¹. Ces motifs justificatifs nécessiteraient aussi une analyse approfondie pour chaque canton, afin de voir quelle est sa marge de manœuvre pour développer des modèles d'IA dans le respect de la protection des données.

Au-delà du principe de licéité, les traitements doivent aussi respecter les autres principes (ex. transparence, proportionnalité et finalité), les obligations du responsable du traitement (ex. registre des activités et analyse d'impact) et les droits de contrôle des personnes concernées (ex. droit d'accès)⁸².

⁷⁹ Pour les détails quant au périmètre de cet intérêt prépondérant, cf. THOUVENIN, 17. Par comparaison, en droit européen, le RGPD n'est pas aussi souple que la LPD et fait actuellement l'objet d'une révision dans le cadre du “Digital Omnibus” afin de faciliter la réutilisation des données sensibles à des fins d'entraînement. Cf. Digital Omnibus Regulation Proposal, 19 novembre 2025.

⁸⁰ ROSENTHAL/VERALDI, notant que les exigences sont moins élevées du point de vue de la licéité.

⁸¹ Le consentement de la personne concernée est en effet difficile à invoquer en raison du rapport d'autorité qui ne le rend pas libre. Cf. EDPB, Lignes directrices, Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679, 4 mai 2020, N 16 ss.

⁸² Ces garanties en matière de protection des données ont conduit l'autorité italienne à suspendre temporairement le déploiement de ChatGPT sur territoire italien, en attendant des garanties suffisantes.

Autres mécanismes de protection (ex. contractuels, droit d'auteur, secrets d'affaires)

Lorsque l'accès aux données porte sur des **données non personnelles** (ex. données anonymisées, techniques, originales ou secrètes), il existe plusieurs freins à leur partage. Les données protégées par le **droit d'auteur** supposent en principe l'autorisation de l'ayant droit. Le partage des **données techniques**, ou de données originales dont la protection par le droit d'auteur a expiré, peut aussi être limité dans certaines situations. Les producteurs de données peuvent en effet imposer des restrictions contractuelles ou des mesures techniques de protection⁸³ et, dans certains cas, invoquer la protection des secrets d'affaires⁸⁴ et/ou la protection contre la concurrence déloyale⁸⁵. Ces mécanismes créent ainsi une sorte d'exclusivité des données

Nonobstant ces mécanismes, plusieurs solutions permettent ou facilitent l'accès aux données. En termes de mécanismes **d'accès obligatoire**, on songe aux mécanismes suivants :

- Les **exceptions du droit d'auteur**, en particulier l'exception à des fins de recherche scientifique (art. 24d LDA). Cette exception est toutefois limitée : (i) à la recherche scientifique (ce qui exclut des finalités principalement commerciales)⁸⁶ ; (ii) les données doivent être accessibles (ce qui exclut les données protégées par des mesures contractuelles ou techniques) ; et (iii) elle est limitée au regard du droit de reproduction (ce qui exclut la communication des résultats, au moins lorsque l'*input* est reproduit dans l'*output*)⁸⁷.
- Les **licences obligatoires ou licences FRAND** en droit de la propriété intellectuelle et en droit de la concurrence, consistant pour une autorité administrative ou judiciaire à autoriser des tiers à accéder à certaines données dans certaines circonstances et à certaines modalités⁸⁸. La licence obligatoire

⁸³ De telles restrictions contractuelles ont été considérées comme valables par la Cour de Justice de l'Union Européenne (CJUE) dans l'affaire CJUE, arrêt du 15 janvier 2015, C-30/14, *Ryanair c. PR Aviation*, [2015] ECLI:EU:C:2015:10), § 39 : « [L]es droits revêtant un caractère impératif en faveur des utilisateurs légitimes d'une base de données [de la Directive 96/9] ne sont pas applicables à une base de données qui n'est protégée ni par le droit d'auteur ni par le droit sui generis en vertu de ladite directive, de sorte que celle-ci ne fait pas obstacle à l'adoption de clauses contractuelles ayant pour objet les conditions d'utilisation d'une telle base de données. ». Cette jurisprudence doit être revue à la lumière du nouveau *Data Act* européen qui prévoit de nouvelles règles en matière de contrat de transfert, ce qui dépasse le cadre du présent rapport. Cf. Benhamou, *Big Data*.

⁸⁴ Il faut que les données aient une valeur commerciale et aient fait l'objet de mesures raisonnables de la part du détenteur légitime de l'information pour la garder secrète (ex. accords de confidentialité et/ou des restrictions physiques et techniques d'accès). En droit international, voir l'article 39 de l'Accord ADPIC qui identifie les normes généralement applicables. En droit suisse, voir DE WERRA 2015, p. 164. En droit de l'UE, voir l'article 2 al. 1 de la Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites. De même, les données qui n'ont pas encore été divulguées peuvent être protégées par des accords confidentiels ou, en l'absence de clause spécifique, par des engagements de confidentialité prévus par des règles spécifiques (par exemple, le droit du travail prévoit parfois une obligation de garder des informations secrètes), voir BENHAMOU 2020, p. 399.

⁸⁵ En Suisse, les bases de données peuvent être protégées dans certaines circonstances par la Loi fédérale contre la concurrence déloyale (LCD) du 19 décembre 1986 (Etat le 1^{er} décembre 2022), en particulier l'article 5 let. c LCD interdisant la réutilisation d'œuvres de tiers par des procédés techniques sans investissements correspondants ; voir DE WERRA/BENHAMOU 2017.

⁸⁶ La doctrine discute de savoir dans quelle mesure la recherche peut aussi poursuivre un but commercial (p. ex. commercialiser les résultats de la recherche et conclure des partenariats publics-privés) en référence au Message LDA qui définit la recherche scientifique comme toute « *recherche systématique de nouvelles connaissances* » et qu'il ne faut faire « *aucune distinction entre recherche à but commercial et [...] non commercial [car la recherche ne poursuit] souvent pas un but unique* » (Message LDA, p. 595). Cf. ISLER, p. 111.

⁸⁷ Ce cas de figure (l'*input* reproduit dans l'*output*) se produit, par exemple avec GenAI, en cas de mémorisation des données d'entraînement (*input*) dans les résultats (*output*). Cf. BENHAMOU 2026.

⁸⁸ IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2021.

peut cependant avoir des conséquences négatives pour le fournisseur de données, en particulier en le conduisant à révéler des secrets des affaires et/ou à supporter des coûts élevés d'interopérabilité de ses données ainsi que le dissuadant de collecter et de traiter des données. Une intervention étatique pourrait donc s'avérer contre-productive. Le caractère dynamique et évolutif des jeux de données rend par ailleurs le concept de "données essentielles" également assez incertain. Ce type d'intervention repose par ailleurs sur une évaluation *ex post* de la situation, par le biais de l'examen d'un cas antérieur de position dominante sur le marché. Par comparaison dans l'UE, l'approche *ex post* du droit de la concurrence est désormais complétée par le Digital Markets Act (DMA). Celui-ci instaure une régulation *ex ante* en qualifiant de "gatekeepers" les grandes plateformes structurantes (désignées selon des critères de taille, de contrôle d'un service essentiel et d'accès à un vaste public) et en leur imposant notamment de garantir l'interopérabilité, l'accès et la portabilité des données des utilisateurs professionnels et finaux à des conditions équitables, raisonnables et non discriminatoires. Ainsi, en droit suisse, sauf à prévoir une loi similaire au DMA, les mécanismes de licences obligatoires ou de licences FRAND en droit de la propriété intellectuelle et en droit de la concurrence ne constituent pas des mesures opportunes afin de faciliter l'accès aux données. Tout au plus, elles pourraient présenter une utilité dans un secteur ou un marché particulier⁸⁹.

- Les **réglementations sectorielles** accordant un accès obligatoire aux données. Un tel droit d'accès aux données ne devrait être accordé que de manière sectorielle, en cas de défaillance du marché dans un secteur concerné, s'il est impossible de remédier à cette défaillance par le seul droit de la concurrence en tenant compte des intérêts légitimes du titulaire des données⁹⁰. Dans plusieurs domaines, les lois sectorielles prévoient que l'administration doit obligatoirement donner accès à ses données publiques.

Dans le domaine statistique, l'administration fédérale doit permettre aux tiers la réutilisation des données statistiques, moyennant l'indication de la source (LSF 20). Dans le domaine de l'énergie, les exploitants de réseaux électriques sont tenus de fournir aux tiers (ex. fournisseurs en énergie, consommateurs finaux) les données de comptage (OApEI 8 al.3). Une difficulté tient toutefois au fait que ces données publiques bénéficient souvent aux acteurs privés qui peuvent les réutiliser sans compensation. Pour surmonter cette difficulté, une solution est de conditionner l'accès obligatoire à des modalités en cas de réutilisation commerciale. Par exemple, dans le domaine des géodonnées, l'administration fédérale doit permettre aux tiers la réutilisation des géodonnées (à moins que des intérêts publics ou privés prépondérants ne s'y opposent) (LGéo 10). En cas d'utilisation commerciale, la réutilisation des données peut donner lieu à la perception d'une rétribution (LGéo 19 ss, LGéo-GE 44).

Comme autre exemple, la **LMETA** prévoit que l'administration fédérale doit publier le code source des logiciels qu'elle développe ou fait développer pour

⁸⁹ IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2025, 25; DE WERRA.

⁹⁰ IPI, Accès aux données non personnelles dans le secteur privé, 1.03.2021, 17; DE WERRA.

exécuter ses tâches (art. 9 LMETA) et publier leurs données sous forme de données ouvertes (art. 10 LMETA, art. 14 ONUM). Cela a pour conséquence que, si une autorité fait développer un logiciel spécifique par un prestataire externe, elle devra tenir compte de cette exigence⁹¹. Les unités décentralisées de l'administration fédérale (ex. CFF, EPF) ne sont toutefois pas tenues de publier le code source des logiciels qui ont été développés sans contributions financières de la Confédération ou dans le cadre de la recherche (ONUM). Cela permet de tenir compte d'une logique de marché et de permettre à ces entités décentralisées de décider des modalités d'accès à leurs données.

Un autre type d'intervention sectorielle consiste, pour l'autorité compétente dans ce domaine, à fournir l'infrastructure technique nécessaire à l'échange de données entre les différents acteurs du marché. Par exemple, dans le domaine de la mobilité, "*l'infrastructure nationale de données mobilitaires*" (NaDIM) va être mise en place pour l'échange de données non personnelles sur la mobilité (horaires, disponibilité, localisation, tarifs, etc.)⁹².

- **Le Règlement UE sur les données (Data Act)**, applicable aussi à certaines entreprises suisses, en particulier celles exportant vers l'UE ou faisant du commerce dans l'UE⁹³, exige des contrats clairs sur l'accès aux données et leur utilisation dans les relations B2B, à des conditions équitables, raisonnables et non discriminatoires (cf. principe FRAND). Le but est d'empêcher que les "grands prestataires" de services d'IA, souvent basés à l'étranger, ne déterminent unilatéralement l'accès aux données et entravent ainsi le développement de modèles commerciaux innovants, en particulier ceux des petites entreprises et des start-ups. Cela a pour conséquence que les entreprises suisses soumises au Data Act doivent revoir leurs contrats B2B, les utilisateurs de données pouvant réclamer un accès équitable aux données, les entreprises productrices de données devant rendre leurs données accessibles à des conditions FRANDs⁹⁴.
- **Les règles sur la transparence**, fédérales et cantonales. Tel est le cas de la LTrans, garantissant l'accès aux documents officiels de l'administration fédérale, mais fonctionne surtout comme un droit d'accès sur demande et non comme un véritable régime de réutilisation des données publiques. Tel est aussi le cas de la stratégie Open Government Data Suisse, mise en œuvre notamment via le portail opendata.swiss. Cette politique vise la mise à disposition proactive de données publiques librement réutilisables (*open by default*). Toutefois, il s'agit principalement de *soft law* et non d'une obligation légale aussi forte que dans l'UE⁹⁵.

⁹¹ En particulier, elle devra vérifier suffisamment tôt qu'elle détient bien les droits nécessaires sur le logiciel pour publier son code source (FF 2022 804 p. 39)

⁹² IPI, Accès aux données non personnelles dans le secteur privé, 1.03.2021, 17.

⁹³ En plus de cette application extra-territoriale, le Data Act prévoit des assouplissements. Les petites entreprises (moins de 10/50 employés et moins de 2/10 millions d'euros de chiffre d'affaires annuel, cf. 2003/361/CE) sont exemptées des exigences du Data Act, à moins qu'elles ne fassent partie d'une plus grande entreprise ou qu'elles agissent en tant que sous-traitants.

⁹⁴ European Commission, Final Report of the Expert Group on B2B Data Sharing and Cloud Computing Contracts, dans lequel sont proposées des clauses contractuelles types (« Model Contractual Terms », MCT).

⁹⁵ IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2025.

En termes d'accès volontaire aux données, on songe aux mécanismes suivants :

- Les **données ouvertes** (*Open Data*) ou les **données partagées** (*Shared Data*), soumises à des licences libres (cf. ci-dessous “données sous licences libres”). À l'égard des données publiques, l'ouverture des données peut être commandée par des politiques publiques, voire des réglementations sectorielles. À l'égard des données du secteur privé, l'ouverture ou le partage peut être stimulé par des exigences réglementaires (données commerciales d'une société cotée en bourse), la réputation (données sur les émissions de CO2 ou la durabilité sociale), la communication (données sur les produits alimentaires pour les clients), la visibilité (données et contenu sur les points d'intérêt touristiques, données liées à la mobilité) ou l'externalisation des tâches opérationnelles (les horaires des entreprises de transport)⁹⁶. En revanche, ces données ne sont souvent pas proposées sous une forme lisible par une machine avec une licence ouverte correspondante ni en tant qu'ensemble de données. Par ailleurs, de nombreux acteurs sont réticents à partager pour des raisons économiques (garder un avantage concurrentiel) et légales (protection des données, les droits d'auteur, les secrets commerciaux)⁹⁷.
- Des **espaces communs de données**, soit une structure technique et organisationnelle permettant et régissant l'accès et l'échange de données provenant de différentes sources et de différents acteurs, souvent dans un secteur donné⁹⁸.

En Europe, la stratégie européenne pour les données de 2020 prévoyait initialement la création de neuf espaces européens communs de données⁹⁹. Cette ambition s'est depuis traduite par le développement progressif de plusieurs espaces sectoriels (ex. santé, patrimoine culturel, énergie, mobilité, agriculture, administration publique, compétences), désormais intégrés dans une stratégie plus large de construction d'un marché européen des données, récemment renforcée par la *Data Union Strategy*¹⁰⁰.

⁹⁶ IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2021.

⁹⁷ IPI, accès aux données non personnelles dans le secteur privé, 1 mars 2021.

⁹⁸ Datenraum Referenzarchitektur 2025, 18 décembre 2025.

⁹⁹ Commission européenne, Une stratégie européenne pour les données.

¹⁰⁰ Pour l'état d'avancement des travaux dans l'UE, cf. European Commission, *Common European Data Spaces*, 2022.

En Suisse, plusieurs espaces de données ont vu le jour ponctuellement par secteurs et par thématiques (ex. dans les domaines de la mobilité, de l'énergie ou de la santé). A ce jour, il manque toutefois une orientation commune et coordonnée entre les différents espaces de données, afin de garantir une interopérabilité entre les espaces de données et d'éviter la création de nouveaux silos de données. A cette fin, la Confédération travaille sur plusieurs mesures en vue de promouvoir un écosystème de données, allant de : (i) des rapports et **documents relatifs à la gouvernance et à l'architecture**, (ii) l'adoption du **"Code de conduite pour l'exploitation des espaces de données fiables"** (élaboré par l'OFCOM) ayant valeur de recommandation pour l'administration fédérale ainsi que, cas échéant, pour d'autres acteurs du secteur privé, (iii) l'élaboration d'une **loi-cadre** sur la réutilisation des données (responsable DFJP, d'ici 2026), (iv) la mise en place d'un **point de contact** central en vue de coordonner la mise en place d'espaces de données sectoriels (santé et agriculture) (rattaché à la Chancellerie fédérale, opérationnel depuis 2025). Ces mesures jettent les bases pour un cadre de référence permettant de promouvoir des espaces de données fiables en Suisse.

- Cependant, si la voie de créer des espaces de données semble prometteuse et importante à l'échelle suisse et européenne, plusieurs questions juridiques restent encore ouvertes, telles que le droit applicable en cas de partenariats publics-privés et/ou d'espaces de données internationaux. Cette voie mérite donc d'être soutenue par les administrations, mais nécessite aussi une analyse approfondie et continue. Il s'agit en effet d'un processus de développement continu qui repose sur les besoins des acteurs concernés, dont plusieurs questions juridiques doivent être encore à clarifiées.
- Pour compléter ces mesures, on peut songer à des **mesures de soutien complémentaires** promouvant l'échange de données, telles que des modèles de contrats, des guides de bonnes pratiques, permettant d'accroître l'information de tous les acteurs, de renforcer la sécurité juridique et de diminuer les coûts de transaction. Ces prestations pourraient être fournies par des institutions publiques, privées ou sous la forme de "partenariats public-privé" qui bénéficient d'un vaste soutien et sont légitimés à agir.

Données sous licences libres

Dans l'économie des données et de l'IA, les données sont parfois rendues accessibles sous une licence libre, soit une licence qui donne accès au contenu et qui respecte généralement les "quatre libertés fondamentales" d'exécuter, étudier, modifier et redistribuer (connues sous le nom de FOSS). Tel est le cas des données ouvertes (*Open Data*) ou des données partagées (*Shared Data*) évoquées ci-dessus.

D'emblée, précisons qu'en matière d'IA, l'ouverture des données peut porter sur différents éléments composant l'IA (ex. données d'entraînement, poids et architecture du modèle). Précisons aussi qu'il existe différents types de licences libres, allant des

licences permissives (ex. licence MIT ou Apache) aux licences moins permissives (ex. licence GNU GPL ou CC-BY-NC-SA 4.0)¹⁰¹.

Ces licences libres posent de **nombreuses questions**, telles que la **compatibilité entre les licences** (ex. OpenRAIL et Llama 2b) et l'**effet propagateur** des termes contractuels sur l'ensemble du modèle, en particulier lorsque l'élément sous licence libre contient une clause de partage à l'identique pour tous les éléments qualifiés de "dérivés" (Share-Alike)¹⁰². Lorsque l'élément sous licence libre est intégré dans des données d'entraînement, il est probable que ses termes contractuels se propagent à toutes les données d'entraînement. En revanche, les termes contractuels ne se propageront en principe pas à l'ensemble du modèle (ex. poids ou architecture du modèle) ou à ses résultats (*outputs*) car la chaîne du droit d'auteur est rompue entre la donnée d'entraînement et le résultat¹⁰³.

Vu le peu d'effet propagateur des licences libres, certains fournisseurs d'IA sont incités à utiliser des ressources sous licence libre pour entraîner leurs modèles tout en les gardant propriétaires, ce qui revient à une certaine réappropriation commerciale des données libres (appelées parfois *data commons*). Pour favoriser la libre circulation des *data commons*, tout en évitant leur réappropriation commerciale, une solution serait de redéfinir les "dérivés" dans le contexte de l'IA afin d'étendre les termes contractuels aux autres éléments de l'IA¹⁰⁴. Une autre solution est de prévoir que, en cas d'utilisation commerciale, la réutilisation des données peut donner lieu à la perception d'une rétribution (*dual licence*).

Conclusion intermédiaire

Vu les différents régimes de protection et malgré les flexibilités permettant d'y déroger, le droit suisse prévoit peu de mécanismes d'accès aux données (obligatoires ou volontaires), ce qui risque de freiner le développement de projets de l'administration ou du secteur privé.

Il est donc recommandé de prévoir des adaptations légales ou réglementaires visant à faciliter l'accès aux données (obligatoires ou volontaires).

On pourrait envisager une **réglementation horizontale** similaire au *Data Act* afin d'éviter une dépendance excessive à l'égard des prestataires de services d'IA étrangers.

On pourrait aussi envisager une réglementation horizontale ou sectorielle dans certains domaines octroyant un **droit d'accès et d'utilisation des données (*statutory right of access*)**, en particulier les données d'entraînement utilisées dans le développement de modèles d'IA par les entités publiques et privées entretenant des relations contractuelles avec des fournisseurs de technologies étrangers. Un tel droit renforcerait non seulement

¹⁰¹ BENHAMOU/DULONG DE ROSNAY ET LES NOMBREUSES RÉFÉRENCES CITÉES.

¹⁰² Cf. MIT licence: "copies or substantial portions of the software"; Apache License v2: "Derivative Works" meaning any work [...] based on (or derived from) the Work and for which [...] modifications represent, as a whole, an original work of authorship. [...] Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof."

¹⁰³ Sauf dans les cas de mémorisation. De plus, le résultat n'est pas susceptible d'être protégée par le droit d'auteur en raison de l'absence d'auteur humain. Cf. BENHAMOU 2024 et les nombreuses références citées.

¹⁰⁴ BENHAMOU 2026.

la transparence, mais pourrait également réduire la dépendance vis-à-vis de ces fournisseurs de technologies. Ce droit pourrait être **couplé à des mécanismes de rémunération** afin de reconnaître la valeur des données (ex. secteurs, tels que la santé, la finance et les services publics) et de garantir que les entités basées en Suisse soient rémunérées équitablement lorsque leurs ensembles de données alimentent le développement commercial de l'IA (principe du partage équitable des avantages)¹⁰⁵.

On pourrait envisager un nouveau type de licence libre, dont les termes contractuels s'étendraient à tous les éléments des modèles d'IA et, dont l'utilisation commerciale donnerait lieu à une compensation (*dual licence*)¹⁰⁶. Afin de rendre effectif ce type de licence libre, celle-ci pourrait être mise en œuvre par des coopératives de données qui auraient pour mission de gérer les licences et les conditions d'utilisation au nom et pour le compte des ayants droit¹⁰⁷.

2.4. Protection des droits fondamentaux et confiance

Dans le déploiement de l'IA, les autorités doivent s'assurer du respect des droits fondamentaux et de la confiance de la population (ex. transparence, traçabilité, encadrement des décisions automatisées, notamment les décisions administratives). Par ailleurs, les autorités doivent garantir un minimum de souveraineté numérique¹⁰⁸, tout en assurant la mise en œuvre de la Convention du Conseil de l'Europe¹⁰⁹.

La mise en œuvre de ces garanties incombe, selon l'obligation concernée, à la Confédération, aux cantons ou aux deux niveaux de l'État simultanément¹¹⁰. Par exemple, en matière de protection des données, la Confédération est compétente pour les acteurs privés et les organes fédéraux (Cst 95 al. 1 97 al. 1, 122 al. 1), tandis que les cantons restent compétents pour le traitement de données effectué par des organes cantonaux ou communaux.

Projet de loi fédérale : régulation de l'IA

A l'échelle fédérale, un **acte normatif** est en cours d'élaboration afin de mettre en œuvre la convention sur l'IA, à l'exclusion du droit cantonal et communal ("**AP-IA**"). L'AP-IA prévoit une série d'obligations, telles que la transparence, la responsabilité et des flexibilités en faveur de la recherche et du développement. Ces obligations sont applicables à la fois à l'administration fédérale et aux acteurs privés. Les cantons restent responsables de la mise en œuvre dans leurs domaines de compétence.

¹⁰⁵ BENHAMOU 2026 ; Pour des considérations similaires, voir par exemple l'article 44 de la loi genevoise sur l'information territoriale (RS GE E 1 46), qui prévoit que l'utilisation commerciale de certaines données – en particulier celles issues du catalogue des données d'intérêt cantonal – fournies par l'État de Genève nécessite la conclusion d'une convention de rémunération entre l'utilisateur potentiel et le détenteur des données.

¹⁰⁶ BENHAMOU 2024.

¹⁰⁷ Cf. Benhamou Yaniv, Mélanie Dulong de Rosney, Open Licensing and Data Trust for Personal and Non-Personal Data: A Blueprint to Support the Commons and Privacy. In: *IIC*, 2025 et les nombreuses références citées.

¹⁰⁸ A l'échelle fédérale, cf. Conseil fédéral, Stratégie Suisse numérique, 1er janvier 2026. A l'échelle cantonale, p.ex. Art. 21A Cst-GE.

¹⁰⁹ Art. 5 al. 4 Cst, le Conseil fédéral souhaitant ratifier la Convention du Conseil de l'Europe (cf. ci-dessus).

¹¹⁰ OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificiel; WYTENBACH, p.299.

Si l'AP-IA n'est pas encore publique, les travaux en cours permettent d'en comprendre les contours¹¹¹. Il semble se distancer de l'IA Act. Il ne vise pas à encadrer les systèmes d'IA en tant que produits, d'autant que la LSPro (en cours de révision) assurera un niveau de sécurité comparable à celui de l'UE pour la mise sur le marché¹¹² de produits. Il vise à prévenir et atténuer les impacts liés au recours à des systèmes d'IA, tout en étant suffisamment souple pour éviter une charge réglementaire trop lourde. Cette question d'équilibre entre régulation et innovation est courante et occupe tous les régulateurs. La confédération et les cantons devront ainsi trouver le bon dosage entre une régulation précise et protectrice des droits fondamentaux, tout en s'assurant de renforcer la Suisse comme lieu d'innovation. Certains comportements risquent d'être interdits mais de façon plus souple que l'IA Act, soit après une analyse de cadre de gestion des risques et sous réserve d'exceptions (cf. art. 16 par. 4 Convention)¹¹³. Les mesures peuvent viser par ailleurs à la fois les déployeurs et les fournisseurs. Les déployeurs sont généralement les plus proches de la phase d'utilisation des systèmes d'IA et à mêmes d'évaluer les risques, tandis que les fournisseurs sont à la base de la conception des modèles et donc à mêmes d'anticiper les risques. En termes d'obligations, on peut songer aux mesures suivantes :

Obligation de mettre en place un **cadre de gestion des risques**. Cela inclut une obligation de contrôle humain lors de la prise de décisions automatisées et/ou toute autre utilisation de modèles d'IA ("*humain in the loop*"), une obligation de documentation technique imposée aux fournisseurs (notamment de qualité des données) et une obligation d'analyse d'impact (en cas de risque élevé) imposée aux déployeurs d'IA. Cette charge réglementaire peut être accompagnée d'allègements pour le secteur privé de façon analogue à l'analyse d'impact LPD (art. 22 LPD). Par exemple, le déployeur privé pourrait renoncer à une analyse d'impact s'il doit utiliser le système d'IA en raison d'une obligation légale (cf. art. 22 al. 4 LPD) ou à consulter l'autorité de surveillance s'il respecte un code de conduite approuvé par ladite autorité ou a consulté un conseiller interne en matière d'IA (art. 22 al. 5 LPD).

Obligations en **matière de transparence**. La transparence, qui devrait être le socle minimal permettant de renforcer la confiance, peut inclure plusieurs dimensions : (i) introduire un devoir d'informer en cas d'interaction avec un système d'IA et en présence de contenus synthétiques (ex. marquage des contenus générés par GenAI, type *watermarking*)¹¹⁴ ; (ii) renforcer le devoir d'informer en droit du travail avant le déploiement d'un système d'IA ; (iii) élargir le devoir d'informer aux décisions "fondées essentiellement" sur un traitement automatisé de données, afin de mieux couvrir les

¹¹¹ Les éléments ci-dessous reposent principalement sur OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificielle, 31 août 2024 et OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificielle, 31 août 2024.

¹¹² Le SECO travaille actuellement sur la révision partielle de la LSPro afin de l'adapter aux nouvelles règles européennes en matière de sécurité des produits (GPSR et MSR). La consultation externe sur ce projet est prévue pour le mois de juin 2026, (voir à ce propos : https://fedlex.data.admin.ch/eli/dl/proj/2025/10/cons_1)(consulté le 18.02.2026).

¹¹³ Les exemples fréquents incluent: (i) techniques subliminales pour altérer le comportement, génération de contenus synthétiques visant à tromper le public ou à influencer les processus démocratiques, (ii) systèmes de notation sociale ("*social scoring*"), (iii) détection des émotions (sauf exceptions, telles que thérapeutique, but scientifique ou sécurité), (iv) surveillance biométrique en temps réel dans l'espace public (sauf exceptions, telles que poursuite d'activités de police), (v) prédiction de la commission d'infractions futures sur la base de données comportementales, sociales ou démographiques (sauf exceptions, telles qu'activité criminelle déterminée et moyennant une appréciation humaine préalable).

¹¹⁴ Cf. Art. 5 AI Act: imposée aux fournisseurs (ex. qui devraient permettre le marquage des contenus pouvant être générés grâce à leur modèle) et aux déployeurs (ex. qui devraient indiquer toute génération de texte, audio ou vidéo).

systèmes d'IA influençant fortement les décisions. (iv) S'agissant des décisions prises par les autorités, en cas de décisions automatisées, on pourrait renforcer les exigences en matière de base légale formelle et, en cas d'utilisation d'IA à haut risque, introduire une obligation d'annonce dans un registre¹¹⁵.

Obligation en matière **d'égalité et de non-discrimination**. Au-delà du cadre de gestion des risques qui permet d'encadrer certaines de ces questions, on peut songer à la possibilité de dénoncer à l'autorité de surveillance des enjeux d'égalité et de non-discrimination. On songe aussi à prévoir un allègement du fardeau de la preuve vu les difficultés à prouver des discriminations, par exemple en cas de discrimination indirecte ou sur la base d'une seule décision individuelle (ex. si des postes sont proposés systématiquement)¹¹⁶.

Obligations en matière de **démocratie**. Cela est traité non seulement à travers le cadre existant¹¹⁷ et l'AP-IA¹¹⁸ mais aussi la LPSCom¹¹⁹.

En termes de mesures pour favoriser la **recherche et l'innovation**, on peut songer aux mesures suivantes : (i) Au-delà des lois sectorielles prévoyant la possibilité d'adopter des projets pilotes ou des législations expérimentales et de mettre à disposition des centres d'innovation en tant qu'interfaces entre la recherche, l'économie et l'administration, on peut songer à (ii) exclure la recherche et le développement du champ de l'AP-IA. En cas d'introduction d'une telle exception, celle-ci ne porterait toutefois que sur les systèmes d'IA encore indisponibles à l'utilisation et, en cas de mise sur le marché, les obligations légales s'appliqueraient rétroactivement à tous les cycles de développement du modèle. La démarcation sera toutefois difficile entre le développement d'outils (hors champ de l'AP-IA) et la commercialisation d'outils (dans le champ de l'AP-IA), par exemple en cas de partenariats publics-privés entre hautes écoles et secteur privé¹²⁰. On songe aussi à (iii) la création d'environnements contrôlés et de **bacs à sables réglementaires** ou, alternativement pour éviter une bureaucratie additionnelle, une **approche sectorielle**¹²¹; (iv) permettre aux acteurs de soumettre des idées à l'autorité de surveillance sans crainte d'être sanctionnés ensuite (p. ex. *chinese walls*) ; (v) inciter l'entraînement à travers un accès facilité aux données, en particulier les données des "grands" fournisseurs au profit des "petits" acteurs et/ou les données publiques à certaines conditions pour éviter leur réappropriation par le secteur privé (cf. ci-dessus).

¹¹⁵ A l'image du registre des activités LPD (art. 12 LPD), le registre public des modèles d'IA pourrait inclure l'unité responsable, le domaine d'utilisation, la base légale, le type d'algorithmes, la catégorie de données personnelles traitées.

¹¹⁶ On peut songer à étendre l'allègement du fardeau de la preuve de la LEg, par exemple dans le processus d'embauche. On notera que l'IA peut conduire à des discriminations directes ou indirectes, soit basées sur des critères d'apparence neutre mais dont les effets peuvent désavantager un groupe (ex. temps de travail ou formation, sans lien avec le sexe). Cf. BRAUN BINDER/ BURRI/ LOHMANN/ SIMMLER/ THOUVENIN/ VOKINGER, Künstliche Intelligenz : Handlungsbedarf im Schweizer Recht).

¹¹⁷ Cf. protection civile et pénale de la personnalité (CP/CC); art. 34 LDP, permettant d'annuler un scrutin si la volonté libre n'a pas été exprimée de manière fiable et non faussée ; art. 5 et 22 LPD, exigeant une transparence accrue en cas de profilage politique.

¹¹⁸ Par exemple, à travers l'interdiction de certains comportements, cadre de gestion des risques, transparence et étiquetage de contenus synthétiques), obliger les plateformes à identifier les contenus synthétiques (ex. marquage de contenu « inauthentique »).

¹¹⁹ Par exemple, à travers l'évaluation des risques systémiques, dont les effets négatifs sur les processus démocratiques, la transparence de leurs systèmes de recommandation (*recommender systems*).

¹²⁰ Cette difficulté est bien connue en droit d'auteur avec l'exception de text and data mining (TDM) limitée à la recherche (cf. ci-dessus).

¹²¹ Cf. art. 23a LApEI; art. 25h LCR. En cas d'introduction de tels mécanismes, il est nécessaire de clarifier les concepts tels que projets pilotes, bacs à sables réglementaires et leur champ d'application.

En termes de recours à l'**autorégulation** et à la **corégulation** – deux modèles à ne pas confondre le 1^{er} (ex. normes techniques) étant volontaire et non contraignant, le 2^{ème} étant encadré et surveillé par l'État – on peut songer aux mesures suivantes : (i) **normes techniques** par les acteurs concernés pour interpréter la loi, par renvoi général via une disposition générale, ou renvoi ponctuel à certaines obligations spécifiques (ex. l'analyse d'impact ou la gestion des risques dès la conception)¹²² ; (ii) **Codes de conduite (CoC)**, qui seraient élaborés par les acteurs privés et soumis à l'approbation préalable de l'autorité de surveillance ainsi que les **certifications**, qui seraient élaborés et surveillés par les organismes d'autorégulation (OAR), étant précisé que la certification LPD n'a pas eu le succès escompté en raison en des coûts qu'elle représente (cf. art. 13 LPD et 6 al. 2 OCPD). Les CoC et les certifications permettraient d'alléger la charge réglementaire (ex. le cadre de gestion des risques), tout en étant encadrés par l'autorité de surveillance. Cela renforcerait ainsi la sécurité juridique et la légitimité démocratique. (iii) encourager les acteurs privés à participer aux processus de **normalisation internationale** en matière d'IA (ex. normes ISO).

En termes de **responsabilité**, le droit actuel prévoit déjà une responsabilité pour risque, suivant les cas, une couverture obligatoire d'assurance (circulation routière, aviation, responsabilité du fait des produits) et, à l'égard de l'administration fédérale, une responsabilité de la Confédération sans faute du fonctionnaire responsable (art. 3 al. 1 LRCP)¹²³. On pourrait songer à réviser la loi sur la responsabilité du fait des produits (LRFP) afin d'inclure l'IA, étant précisé que cela irait au-delà de l'IA (car la LRFP inclurait aussi les logiciels).

En termes de **surveillance**, on peut songer à trois modèles de surveillance : autorités sectorielles existantes (ex. FINMA, PFPDT, ComCom), autorité transversale unique ou modèle mixte combinant les autorités sectorielles et une autorité transversale, étant précisé que le modèle choisi devra être fonctionnellement indépendant des pouvoirs exécutif et législatif¹²⁴.

En termes de **voies de droit**, le droit actuel prévoit que la résolution de cas individuels revient aux tribunaux civils en droit privé et aux autorités de recours traditionnelles en droit public. On peut penser à compléter le droit actuel avec les mesures suivantes : (i) des voies de droit extraordinaire sous la forme d'une plainte ou d'une dénonciation¹²⁵ ; (iii) mesures administratives et sanctions pénales sur le même modèle que la LPD¹²⁶. Relevons que les mécanismes d'actions collectives (à l'image des *class actions* américaines) ont été rejetés encore récemment par le législateur, au motif que les instruments actuels seraient suffisants, en particulier à travers l'action des organisations et le cumul subjectif et objectif d'actions individuelles¹²⁷.

¹²² Par exemple dans le domaine de la construction. Cf. Guide de législation OFJ, N 726 ; ODIV 65 al. 1.

¹²³ A noter que la réparation morale suppose une faute (art. 6 LRCP) et qu'il faut pouvoir attribuer le dommage à un agent (ce qui est difficile avec des agents autonomes).

¹²⁴ Conseil de l'Europe, Rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit.

¹²⁵ Cf. art. 71 PA; art. 49 al. 1 LPD sans offrir la qualité de partie sauf en cas de rapport étroit et spécial avec la situation litigieuse et d'un intérêt digne de protection à ce que l'autorité de surveillance intervienne.

¹²⁶ Dans la LPD, les mesures administratives sont du ressort du PFDPT (art. 49-52 LPD), les sanctions pénales du ressort des autorités pénales (art. 60-66 LPD).

¹²⁷ Dernier projet (FF 2021 3048 Action des organisations et transaction collective), rejeté par le Conseil national le 17 mars 2025 et le Conseil des Etats le 15 septembre 2025.

L'AP-IA a le mérite d'encadrer l'utilisation et le développement de modèles d'IA en Suisse, en particulier de renforcer le respect des droits fondamentaux et la confiance de la population. Quelques **points d'attention et d'amélioration** peuvent toutefois être formulés :

En matière de **transparence**, le devoir d'informer en cas d'interaction avec un système d'IA et de génération de contenus synthétiques va confronter les destinataires de la mesure à la difficulté de tracer la frontière entre des contenus générés et des contenus assistés. Cette limite est connue du droit d'auteur et échappe précisément aux tribunaux quant à la délimitation entre une œuvre assistée et générée. On voit donc mal le destinataire de la mesure apprécier et savoir quand appliquer le devoir d'information et quand s'en passer.

En matière **d'égalité et de non-discrimination**, une difficulté tient au fait que l'allègement du fardeau de la preuve risque d'être limité au droit du travail, en particulier aux discriminations à l'embauche, alors que de nombreuses discriminations (directes ou indirectes) peuvent apparaître dans de très nombreux autres contextes (ex. octroi ou refus de prestations de l'État).

En matière de **démocratie**, la LPSCom complètera l'AP-IA, notamment avec une obligation de transparence sur les algorithmes de recommandation (*recommender systems*)¹²⁸ et de remettre à l'OFCOM un rapport de transparence et d'évaluation des risques (ex. en cas de présence accrue de désinformation et de risques systémiques). La LPSCom actuelle contient toutefois plusieurs points d'amélioration, notamment quant à son champ d'application et ses obligations¹²⁹.

En matière de **recherche et d'innovation**, les concepts tels que les projets pilotes et les bacs à sable réglementaires doivent être largement clarifiés et implémentés. Ils sont pour l'instant souvent des concepts, peu utilisés et peu connus des administrés. D'éventuelles exceptions en faveur de la recherche et innovation (ex. exclusion du champ d'application)

En matière **d'auto-régulation**, il convient de privilégier autant que possible la co-régulation afin, d'une part, de garantir la légitimité et le contrôle démocratique et, d'autre part, de renforcer la sécurité juridique pour les entités concernées par l'auto-régulation.

Administration cantonale

Les cantons devront évaluer comment se conformer à la Convention du Conseil de l'Europe. Une option serait de reprendre les obligations de l'AP-IA relatives à l'administration fédérale pour l'administration cantonale. L'IA confronte tous les secteurs à de nouveaux défis, qui concernent en priorité la transparence et la protection

¹²⁸ Dans la LPSCom, cette transparence ne porte que sur les "principaux paramètres utilisés dans leurs systèmes de recommandation et leur pondération" et les "possibilités de modifier ou d'influencer les principaux paramètres" (art. 18 LPSCom). La transparence ne porte en revanche pas sur la neutralité des algorithmes. Ainsi, les plateformes pourraient continuer de décider de favoriser et discriminer certains contenus, contrairement aux médias publics encadrés par la LRTV et soumis à des règles strictes telles que l'objectivité et la pluralité d'opinions. Cf. Benhamou, Contrôle judiciaire des commentaires en ligne et de la désinformation : suites de l'ATF 149 I 2. In: La semaine judiciaire, 2024, vol. 146, n° 9, p. 717.

¹²⁹ BENHAMOU/ DE WERRA/ PASCAL/ CHAIX, Prise de position du Digital Law Center.

des données. Toutefois, l'importance des questions soulevées par l'IA diffère en fonction des secteurs. Dès lors, certains défis existants pourraient par exemple être résolus sur une large base dans une logique commune intersectorielle, tandis que d'autres questions, spécifiques à un secteur, continueraient à être réglées de manière sectorielle¹³⁰.

Conclusion intermédiaire

Un acte normatif à l'échelle fédérale est en cours de rédaction et vise à régler les nombreux enjeux relatifs aux droits fondamentaux et à la confiance, tout en favorisant la recherche et le développement en Suisse. Cela étant, on peut formuler des pistes d'amélioration pour l'AP-IA qui pourraient être reprises pour les actes normatifs visant l'administration cantonale. Les cantons devront en effet aussi s'assurer de respecter la Convention du Conseil de l'Europe.

2.5. Concentration des pouvoirs

Le problème principal ne réside pas dans la technologie ou dans des cas d'application individuels, mais dans la concentration du pouvoir des grandes entreprises technologiques. Des mesures structurelles sont nécessaires afin de corriger cette asymétrie de pouvoir¹³¹.

Favoriser l'émergence de solutions locales, émanant des acteurs privés et de l'administration

Afin de favoriser l'émergence de solutions locales émanant des acteurs privés et de l'administration, on peut songer à des **exigences réglementaires sectorielles** qui stimuleraient le développement de solutions locales pour certains secteurs et/ou imposeraient des standards locaux également à des prestataires étrangers désireux d'opérer sur le marché suisse. Par exemple, dans les domaines bancaires et financiers, de la santé et de l'énergie, les exigences en matière de secret et de sécurité ont incité les utilisateurs à privilégier les acteurs locaux ou les prestataires étrangers à développer des solutions locales. On notera toutefois que, même en prévoyant des exigences réglementaires permettant d'imposer des standards de protection à tous les prestataires suisses ou étrangers, cela n'empêche pas les acteurs suisses de se tourner vers de "grands" fournisseurs étrangers soumis à leur tour à d'autres règles étrangères (ex. Microsoft opérant depuis la Suisse mais potentiellement soumis à l'US Cloud Act).

A supposer que les acteurs locaux se développent, leur nationalité et la localisation territoriale ne constituent toutefois pas nécessairement une garantie suffisante, car l'entité résidente en Suisse pourrait être contrôlée depuis l'étranger et être soumise à des décisions contraires aux intérêts du pays par la maison-mère. Ceci est d'autant plus vrai que la question même de la nationalité ne va pas de soi lorsqu'on parle de contrôle économique effectif : s'agit-il de l'adresse du siège, de la majorité de l'actionnariat, de la

¹³⁰ OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificielle, 12 février 2025.

¹³¹ OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificielle, 12 février 2025.

nationalité du *management* ? Face à cette somme d'incertitudes, le droit public pourrait prévoir des **participations publiques** ou **limiter les investissements étrangers** dans des entreprises considérées comme infrastructures critiques. Des lois générales comme la LCart semblent très orientées marché et résister à des réflexions telles que la souveraineté numérique¹³². En revanche, on peut songer à des lois spécifiques comme la LEIA qui vise à empêcher l'acquisition d'entreprises suisses par des investisseurs étrangers lorsqu'une telle acquisition menace ou compromet l'ordre public ou la sécurité publique de la Suisse. Ainsi, il est prévu que certaines acquisitions soient soumises à une approbation obligatoire, en particulier celle portant sur "*les entreprises qui fournissent aux autorités suisses des systèmes ou services informatiques clés liés à la sécurité*" (art. 3 al. 1 let. f LEIA)¹³³. Une telle piste nécessiterait une analyse approfondie afin de voir quels types d'entreprises technologiques peuvent être protégés par cette loi.

L'État pourrait aussi favoriser le développement de **solutions publiques** pouvant être commercialisées ensuite à d'autres institutions publiques ou des acteurs privés, comme cela a été fait avec le dossier patient des HUG (DPI+) mis à disposition des Hôpitaux du Valais. Cette mise à disposition ou vente de solutions institutionnelles pose toutefois des questions de concurrence puisque l'État intervient dans la libre concurrence et pourrait ainsi prendre des mesures qui entraveraient la libre concurrence. Pour surmonter cette difficulté, une solution serait d'interpréter cette approche comme conforme au cadre légal existant, en particulier aux principes constitutionnels (art. 5 al. 2 et 9 Cst permettant à l'État d'expérimenter)¹³⁴.

A l'échelle fédérale, l'administration fédérale décide, sur la base d'analyses de marché et des objectifs d'interopérabilité, de rentabilité et de sécurité, si une prestation doit être fournie à l'interne ou acquise à l'extérieur (ONUM 9). Si elle recourt à un fournisseur externe, elle peut aussi faire appel à **eOperations Suisse SA** pour certaines prestations (acquisition et développement de moyens informatiques) et pour autant que ces prestations soient aussi fournies aux autorités cantonales et communales (ONUM 13 al. 1). EOperations est une société propriété des pouvoirs publics, dans laquelle la Confédération prend des participations dans eOperations Suisse SA par l'achat d'actions (ONUM 13 al. 2) qui facilite la coopération entre la Confédération, les cantons et les communes dans le domaine des prestations électroniques des autorités pour la population et le secteur économique.

Règles en matière de marché public

L'émergence d'acteurs locaux peut être stimulée à travers la commande publique. On songe aux **règles en matière de marchés publics**.

¹³² A l'étranger, le droit de la concurrence permet parfois de protéger des entreprises locales, en tenant de considérations allant au-delà d'une pure régulation du marché. Par exemple, dans l'UE, Traité UE (TFUE) a permis à l'Allemagne de protéger le secteur de l'énergie (EOM) et aux US, le droit antitrust (Sherman Act sur les monopoles et le Clayton Act sur contrôle des concentration) a permis aux US de protéger certains secteurs.

¹³³ Un mécanisme similaire est prévu dans la LFAIE (*Lex Koller*) qui prévoit de limiter les investissements immobiliers par les étrangers. Un projet de révision de la loi est en cours et prévoit notamment l'obligation d'obtenir une autorisation pour acheter des parts de véhicules immobiliers cotés.

¹³⁴ FLÜCKIGER, Légistique.

La piste à laquelle on serait tentés de songer serait de recourir aux appels d'offres pour renforcer la souveraineté numérique, par exemple en privilégiant certains acteurs locaux. Or, cela reviendrait à discriminer certains soumissionnaires au profit d'autres, et serait contraire aux règles en matière de marché public. Une telle piste nécessiterait en tout cas une analyse approfondie afin de voir s'il existe des exceptions en droit des marchés publics.

On devra être en tout cas prudent lors du libellé de l'appel d'offres pour éviter d'écarter des entreprises suisses. Le droit des marchés publics ménage une certaine marge de manœuvre permettant de recourir à des procédures de gré à gré, notamment en cas de solution *in-house* ou de la présence d'une entreprise unique en mesure de fournir le bien ou le service requis. On notera par ailleurs que les États européens s'intéressent aux procédés américains d'attribution des marchés publics (e.g. *Small Business Act*) ayant permis le développement de géants technologiques, en mettant en place des instruments permettant à des petites et moyennes entreprises (PME) de s'appuyer sur la commande publique pour se développer¹³⁵. On pourrait aussi envisager des critères de durabilité dans l'appel d'offre ou l'octroi de subventions (ex. empreinte carbone, efficacité énergétique, emplacement des centres de données).

Cybersécurité et cyberassurance

Les enjeux de cybersécurité sont majeurs pour la société et les entreprises, et se sont amplifiés à l'ère de l'IA. Ils supposent de recourir à des TIC résilientes, notamment à travers une **diversification des fournisseurs** de solutions matérielles et logicielles en vue de réduire les dépendances et une **préparation adéquate** en cas de cyberincident (formation, contrat et TOMs). Au-delà de ces mesures classiques, on peut aussi songer à encourager le recours aux cyberassurances afin de renforcer la prévention et la couverture de risques. A cette fin, plusieurs mesures sont envisageables¹³⁶ :

- (i) Vu la diversité des offres existantes et la difficulté de les comparer, **sensibiliser** les acteurs aux cyberassurances afin de leur permettre de comprendre l'apport de celles-ci, notamment en matière de cybersécurité et de gestion des cyberrisques.
- (ii) favoriser l'émergence de **standards minimaux et homogènes** via des lignes directrices, des bonnes pratiques et modèles de contrats, qui détermineront notamment ce qui doit être inclus dans une couverture minimale afin d'avoir une référence commune et comparable.
- (iii) **moyens d'incitation** à la conclusion de cyberassurances par les PME, par exemple via des codes de conduite ou certifications qui permettraient aux PME d'obtenir des conditions d'assurance plus favorables (ex. primes réduites) dans le cas où elles respecteraient certains standards de sécurité.
- (iv) conditionner la soumission ou l'adjudication de marchés publics à la conclusion préalable d'une cyber-assurances.
- (v) éventuelle introduction d'une **cyberassurance obligatoire** dans certains cas (ex. contrats conclus avec l'Etat présentant des risques pour les données personnelles).

¹³⁵ Ex. le *Small Business Act* a orienté une part de la commande publique vers des petites entreprises, ce qui a permis à des entreprises innovantes de s'appuyer sur des clients solvables pour améliorer leurs produits et services. Pour des experts français, ce type d'instrument pourrait être déployé au niveau français pour les achats publics innovants sans contrevenir au droit européen. Voir BENHAMOU B., Souveraineté numérique. Cf. Benhamou/Durand/Bernard et les références citées.

¹³⁶ DE WERRA/BENHAMOU.

L'Etat pourrait même contribuer à la prise en charge de certains cyberrisques systémiques qui ne se limitent pas à affecter des entreprises individuelles mais portent atteinte à toute la société (ex. terrorisme, cyberguerre).

Renforcement de l'autodétermination numérique

Une solution pour limiter la concentration des pouvoirs et plus généralement pour renforcer la souveraineté numérique individuelle pourrait être de favoriser l'autodétermination numérique. Celle-ci est une nouvelle approche destinée à renforcer le contrôle des particuliers, des entreprises et de la société sur leurs propres données¹³⁷. D'un point de vue dogmatique, l'**autodétermination numérique** pourrait être consacrée à travers l'interprétation des droits fondamentaux¹³⁸ ou à travers la reconnaissance d'un nouveau droit venant combler les lacunes des droits fondamentaux¹³⁹.

Par exemple, plusieurs cantons intègrent progressivement un **nouveau droit à l'intégrité numérique**, visant à mieux protéger les individus dans leur vie numérique¹⁴⁰. A Genève, le nouveau droit à l'intégrité numérique a une composante de souveraineté numérique (Cst-GE 21A al. 4), présentée comme une condition de l'effectivité des droits fondamentaux, surtout face à la dépendance envers de grands fournisseurs technologiques. La portée exacte d'un tel droit doit être encore précisée par la jurisprudence¹⁴¹. Ce nonobstant, l'objectif du Conseil d'État est de se positionner sur les plans symbolique, politique et pratique comme un exemple en matière de développement de solutions ou de services indigènes, tout en évitant l'adoption d'une disposition limitative qui mènerait à l'interdiction de recourir à certains services extérieurs, en l'absence d'alternatives suisses¹⁴². En effet, certaines prestations nécessaires au déploiement des activités de l'administration sont proposées en Suisse, d'autres à l'étranger. Dans ce contexte, l'art. 21A al. 4 requiert de l'État qu'il privilégie des solutions d'hébergement de données maîtrisées au niveau suisse, sans que cela ne constitue un impératif absolu. Il vise également la garantie d'un niveau de protection équivalent pour les données traitées à l'étranger conformément à l'art. 21A al. 3.

Toutefois, l'approche de l'autodétermination numérique pose des problèmes théoriques et pratiques. Sur le plan théorique, les données personnelles ne sont utiles que mises en relation avec celles des autres (concept de "*interpersonal privacy*")¹⁴³. Concevoir la question de l'intégrité des données individuelles ne tient pas compte de cette composante. Sur le plan pratique, il est difficile de demander aux individus de saisir tous les enjeux concernant leurs données, sans ressources cognitives et techniques. Le contrôle des individus sur leurs données repose sur une fiction (Il suffit de penser aux millions de clics que chacun doit faire tous les jours pour prétendument contrôler ses données au sujet cookies pour comprendre le problème) et ne leur donne aucun pouvoir effectif sur leurs données. Cela risque même de déresponsabiliser les entreprises, en

¹³⁷ Ce concept est étroitement lié au droit à l'autodétermination informationnelle, mais il va plus loin : il s'agit non seulement de protéger les personnes, les entreprises et la société dans son ensemble, mais aussi de les encourager, grâce à des concepts innovants en matière d'utilisation des données, à partager leurs données, sans en perdre le contrôle, afin que ces données soient exploitables. Cf. BENHAMOU/BERNARD/DURAND.

¹³⁸ P.ex. droit à la vie et liberté personnelle (art. 10 Cst/CH), dont découle les droits de la personnalité (art. 27ss CC) ; protection de la sphère privée (art. 13 Cst/CH), dont découle l'autodétermination informationnelle. Cf. Benhamou/Durand/Bernard, et les références citées.

¹³⁹ En effet, seul l'État est initialement soumis aux droits fondamentaux, même si ceux-ci doivent se manifester dans l'ensemble de l'ordre juridique et les autorités doivent veiller à ce que les droits fondamentaux prennent également effet entre les particuliers (art. 35 Cst/CH).

¹⁴⁰ RUEGGER/ DIAS.

¹⁴¹ RUEGGER/ DIAS.

¹⁴² PL-12945, 20 et 25.

¹⁴³ BIRNHACK.

transférant la responsabilité du contrôle des données sur les individus. Ainsi, pour rendre effective l'autodétermination numérique, il s'agirait de le faire d'abord au niveau collectif, étant données les limites cognitives des individus pour faire valoir ce principe dans l'espace numérique. Cela peut se faire par exemple au moyen d'une gouvernance collective des données (ex. coopératives de données) et/ou d'exercice collectif des droits individuels (ex. droit d'accès aux données)¹⁴⁴.

Malgré les limites exposées, cette piste d'autodétermination numérique a non seulement le mérite de poursuivre des objectifs légitimes, mais correspond aussi aux législations européennes et suisses en matière de protection des données, en particulier en ce qui concerne les droits de contrôle des individus. Elle pourrait être rendue effective à travers la mise en place de coopératives de données, cas échéant combinée avec des contrats modèles permettant de déterminer les modalités de réutilisation des données.

Conclusion intermédiaire

L'État dispose de plusieurs instruments pour limiter la concentration des pouvoirs. On songe à l'introduction d'exigences réglementaires pour stimuler des solutions locales, voire prévoir des participations publiques ou limiter les investissements étrangers dans des entreprises considérées comme des infrastructures critiques. L'État pourrait aussi favoriser le développement de solutions publiques pouvant être commercialisées ensuite à d'autres institutions publiques ou à des acteurs privés. L'État devrait aussi accorder de l'importance à la commande publique, notamment lorsqu'il rédige les appels d'offres, et encourager le marché des cyberassurances afin de renforcer la cybersécurité des acteurs. Enfin, l'autodétermination numérique est souvent citée par certains, des autorités aux législateurs, comme une approche permettant de renforcer la souveraineté individuelle. Malgré les limites qu'une telle approche comporte, son ancrage dans la loi (ex. art. 21A Cst-GE) donne mandat à l'État d'œuvrer davantage en faveur de la souveraineté numérique. L'Etat pourrait par exemple favoriser la mise en place de coopératives de données, et de contrats modèles.

2.6. Conclusion sur les enjeux juridiques

Le cadre légal semble assez souple pour permettre à la fois le déploiement des modèles d'IA (IA locale, en cloud encadré ou public) et le développement de modèles souverains. Par ailleurs, la protection des droits fondamentaux et la confiance du public devraient être renforcées avec le projet de loi IA ("AP-IA"). Plusieurs points d'amélioration subsistent toutefois. S'agissant de **l'utilisation des modèles d'IA** par des fournisseurs IA, l'administration est souvent confrontée à une dynamique contradictoire, voire à une "injonction" d'adopter des modèles d'IA pour améliorer ses processus, tout en devant assurer le respect d'un cadre légal strict, tel que la protection des données, la confidentialité des données et les droits fondamentaux. Or, ce respect du cadre légal peut être mis en péril, suivant les types de modèles d'IA et d'hébergement choisis. Le

¹⁴⁴ Cf. Yaniv Benhamou / Mélanie Dulong de Rosney, Open Licensing and Data Trust for Personal and Non-Personal Data: A Blueprint to Support the Commons and Privacy. In: *JIC*, 2025, 1553 et les nombreuses références citées; René Mahieu/Jef Ausloos, Harnessing the collective potential of GDPR access rights: towards an ecology of transparency, in: *Internet Policy Review*, 1 ss et les nombreuses références citées.

cadre légal ne prévoit par ailleurs pas, ou peu, de règles en matière de souveraineté numérique, ce qui n'incite pas l'administration et les acteurs privés à plus d'autonomie.

S'agissant du **développement de modèles souverains**, peu de mécanismes existent en droit suisse afin de faciliter l'accès aux données, ce qui risque de freiner le développement de projets de l'administration ou du secteur privé.

S'agissant de la **protection des droits fondamentaux**, celle-ci devrait être assurée avec le projet de loi "AP-IA". L'AP-IA risque toutefois de prendre encore du temps avant d'être adoptée, mérite encore quelques points d'attention et d'amélioration et ne vise que les acteurs privés et l'administration fédérale, à l'exclusion des administrations cantonales et municipales.

Sur cette base, on peut recommander les mesures suivantes :

- (i) à l'échelle fédérale et cantonale, clarifier le cadre légal à l'utilisation de modèles d'IA par des fournisseurs IA, cas échéant, adopter des mesures politiques, voire des exigences légales afin de renforcer des solutions indigènes plutôt qu'étrangères ;
- (ii) à l'échelle fédérale, prévoir des adaptations légales ou réglementaires pour favoriser le partage obligatoire de données détenues par certaines entreprises (ex. les "grands" fournisseurs) afin de développer des modèles souverains ainsi que le partage des données publiques à certaines conditions afin d'éviter leur réappropriation par les acteurs privés sans compensation ;
- (iii) à l'échelle cantonale, vérifier que le droit cantonal assure suffisamment le respect des droits fondamentaux lors de l'utilisation et le développement de modèles d'IA, le cas échéant adopter de nouvelles règles, en s'inspirant du projet de loi fédérale "AP-IA" ;
- (iv) à l'échelle fédérale et cantonale, adopter des mesures structurelles afin de corriger l'asymétrie de pouvoir entre les grandes entreprises technologiques et l'État et les "petits" acteurs.

3. Une croissance fulgurante mais différenciée de l’empreinte de l’IA en Suisse

3.1. Perspective générale

Alors que la Suisse occupe systématiquement les premières places des classements internationaux évaluant son potentiel de déploiement des TIC¹⁴⁵, sa position est moins claire en ce qui concerne spécifiquement le développement de l’IA. Le pays obtient en effet de bons résultats dans les indicateurs évaluant la diffusion de l’IA, les capacités techniques de déploiement ou de financement, mais il accuse un certain retard en matière de gouvernance et d’efforts d’atténuation des risques liés à la diffusion de cette technologie.

Utilisation grand public

L’usage de la GenAI se généralise rapidement en Suisse, qui présente l’un des plus importants taux de diffusion dans la population des pays de l’OCDE.¹⁴⁶ L’Office fédéral de la statistique notait une intensité d’utilisation très forte chez les Suisse·sse·s puisque, au printemps 2025, 43 % des personnes âgées de 15 à 88 ans répondent avoir déjà utilisé l’IA générative. Parmi les utilisateur·trice·s, 34 % en font un usage hebdomadaire et 36 % l’emploient au quotidien. Ces utilisations ont davantage lieu dans le cadre privé (38 % des répondant·e·s) plutôt qu’à des fins professionnelles (31 %) ; elles augmentent fortement chez les jeunes puisque 75 % des étudiant·e·s indiquent utiliser ce type d’applications¹⁴⁷.

Capacités techniques et compétences

Le pays est relativement bien positionné en termes de ressources technologiques, notamment du fait de la présence d’employé·e·s qualifié·e·s et d’importantes capacités de financement privé¹⁴⁸. Ainsi, la région de Zürich est régulièrement présentée comme propice au développement d’un écosystème IA¹⁴⁹. La présence des géants de la tech et l’annonce récente de l’ouverture d’une succursale d’OpenAI renforcent cette image.¹⁵⁰ De fait, la Suisse occupe une position avantageuse en matière d’investissements privés

¹⁴⁵ Y. Benhamou, F. Bernard et C. Durand, *Souveraineté numérique: étude pluridisciplinaire pour la Suisse, 2023, op. cit.*, p. 48.

¹⁴⁶ En 2025, 47 % des individus entre 16 et 74 ans avaient utilisé des outils de GenAI au cours des trois mois précédant l’enquête, contre 36, 8 % en moyenne dans l’OCDE et 56.3 en Norvège, en tête du classement. OCDE. « L’utilisation de l’IA par les individus progresse rapidement dans l’ensemble de l’OCDE, tandis que l’adoption par les entreprises continue de s’étendre », <https://www.oecd.org/fr/about/news/announcements/2026/01/ai-use-by-individuals-surges-across-the-oecd-as-adoption-by-firms-continues-to-expand.html>, 28 janvier 2026, (consulté le 5.03.2026).

¹⁴⁷ Office fédéral de la statistique, « Utilisation d’Internet dans les ménages en 2025 : Une Suisse friande d’IA et toujours plus exposée à la désinformation », communiqué de presse, 5 décembre 2025, https://www.news.admin.ch/fr/newsb/6zpv_pRIse2PU3NnFlv0n (consulté le 19.03.2026).

¹⁴⁸ La Suisse est l’un des pays avec le plus de compétences liées à l’IA Voir Nestor Maslej et al., « The AI Index 2025 Annual Report », AI Index Steering Committee, Institute for Human-Centered AI, Stanford University avril 2025, <https://aiindex.stanford.edu/report/>, (consulté le 27.02.2026).

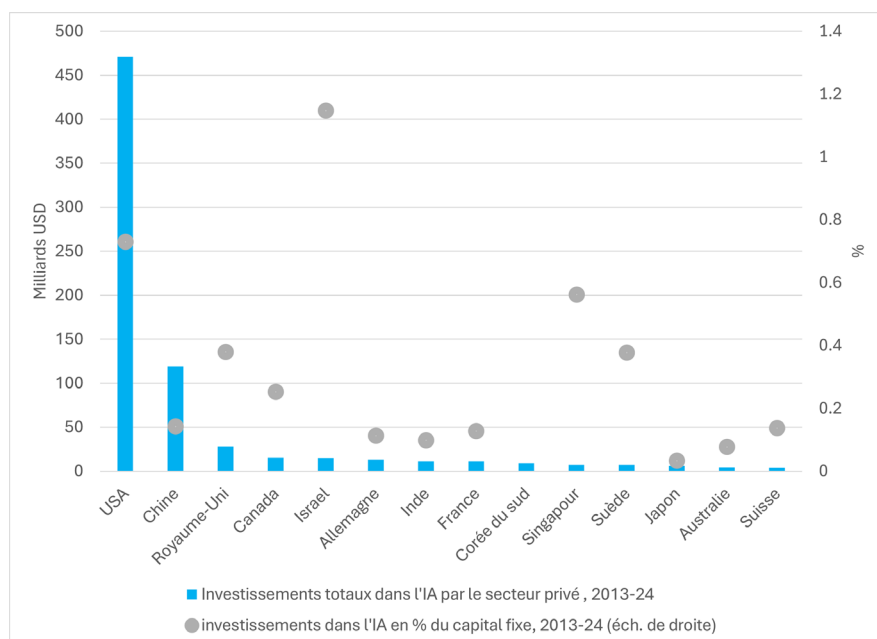
¹⁴⁹ Elio Sottas et Emilie Délétroz, « Zurich, le nouveau hub européen de l’intelligence artificielle », RTS, 9 décembre 2025, <https://www.rts.ch/info/sciences-tech/2025/article/zurich-nouveau-hub-europeen-de-l-ia-entre-innovation-et-defis-29085164.html>, (consulté le 24.02.2026).

¹⁵⁰ « Greater Zurich: Home to top IT companies in Europe », *Greater Zurich Area*, 2024, <https://www.greaterzuricharea.com/en/greater-zurich-home-top-it-companies-europe> (consulté le 27.02.2026). « OpenAI sets up new office in Switzerland », *Swissinfo*, 20 janvier 2025, <https://www.swissinfo.ch/eng/multinational-companies/openai-sets-up-new-office-in-switzerland/88468988>, (consulté le 27.02.2026).

dans les entreprises d'IA ; entre 2013 et 2024, le secteur privé y a investi 3,9 milliards de dollars (

Figure 4). Rapporté à l'investissement total en capital fixe, ce montant la place parmi les économies les plus actives dans ce domaine. Il convient cependant de souligner qu'en termes absolus les montants investis en Suisse sont sans commune mesure avec les sommes engagées aux États-Unis.

Figure 4 : Investissement dans l'IA par le secteur privé rapporté à l'investissement total en capital fixe (2013-2024)¹⁵¹



Capacités gouvernementales

Si la Suisse est bien classée sur le plan technique, plusieurs expert·e·s interrogé·e·s soulignent des lacunes politiques dans la maîtrise du développement de l'IA. Ce sont du reste les indicateurs de capacités gouvernementales qui font chuter la position de la Suisse dans différents classements qui évaluent le développement de l'IA. Dans l'édition 2025 de la Government AI Readiness Index¹⁵², qui note la capacité des États à piloter l'adoption de l'IA conformément au bien-être de sa population, la Suisse se situe en 26^e position. En cause, son faible score dans les piliers « capacités d'action publique » évaluant la présence d'une stratégie et d'un organe d'implémentation de l'IA au niveau national, ainsi que la participation du pays à des efforts de coordination internationale. La Suisse obtient également une note relativement basse dans le critère « politique et

¹⁵¹ Investissements du secteur privé dans l'IA dans Nestor Maslej et al., « The AI Index 2024 Annual Report », *Stanford University, HAI*, avril 2024, <https://aiindex.stanford.edu/report/>, (consulté le 27.02.2026). Investissements en capital fixe et déflateur tirés de de Müller, Karsten, et al. *The Global Macro Database: a New International Macroeconomic Dataset* (Version 2026-01), National Bureau of Economic Research, April 2025, <http://www.nber.org/papers/w33714>.

¹⁵² Oxford Insights, « Government AI Readiness Index 2025 », 2025, <https://oxfordinsights.com/ai-readiness/government-ai-readiness-index-2025/> (consulté le 04.03.2026)

gouvernance » du Stanford HAI Vibrancy Tool, qui mesure la présence d’une législation en matière d’IA et les mentions de l’IA dans les procédures législatives¹⁵³.

Ces indices n’évaluent pas le contenu des stratégies nationales, mais simplement la présence d’annonces et de documents officiels qui témoignent d’une politique en matière d’IA, ainsi que d’un engagement visible dans sa réalisation, comme la présence d’un budget et d’institutions de contrôle dédiées. La position de la Suisse reflète donc surtout un temps de latence dans l’élaboration de politiques publiques en matière d’IA, et son retard pourrait être réduit par la mise en place du projet de réglementation de l’IA en cours d’élaboration annoncé par le Conseil fédéral le 12 février 2025 (cf. 1.2 et 2.1.) Cependant, plusieurs acteurs considèrent que ce projet ne permet pas un encadrement adéquat des conséquences néfastes engendrées par l’IA. Algorithm Watch Switzerland pointe ainsi un « manque la vision qui garantirait également un bénéfice réel pour les personnes, la société et l’environnement »¹⁵⁴. L’organisation souligne également manque d’initiative dans le développement de projets IA déployées pour l’intérêt général.

En conclusion, bien que la Suisse constitue un nœud d’innovation hautement qualifié et connaisse une diffusion rapide de l’IA sur son territoire, l’insuffisance des capacités publiques de coordination constitue une source majeure de fragilité.

3.2. Diffusion dans le secteur des entreprises

Si l’adoption de l’IA par le secteur privé demeure peu documentée par les statistiques officielles, différentes enquêtes montrent que, en Suisse comme à l’international, son déploiement dans les entreprises est loin de suivre une trajectoire linéaire. Au contraire, les études soulignent un processus marqué de différenciation en fonction des secteurs des entreprises, mais aussi de leur tailles et d’autres variables économiques comme leur rentabilité.

En 2023, 34 % des entreprises suisses de plus de 250 employé.e.s utilisaient l’IA, un niveau légèrement supérieur à la moyenne de l’OCDE (30,5 %)¹⁵⁵. Une enquête plus récente de la haute école spécialisée bernoise rapporte qu’en 2024 35,9 % des participants utilisaient l’IA au quotidien dans leur travail, contre 27,2 % l’année précédente. Seuls 14,6 % affirmaient ne jamais s’en servir dans le cadre professionnel. En revanche, les entretiens effectués pour la préparation de ce rapport ont souligné que ces chiffres portent surtout sur des utilisations localisées d’outils d’IA ; un nombre très restreint de grandes entreprises ont entrepris une transformation complète du processus de travail.

¹⁵³ Stanford University Human-Centered Artificial Intelligence, “Global AI Vibrancy Tool”, <https://hai.stanford.edu/ai-index/global-vibrancy-tool> (consulté le 21.04.2026). La Suisse obtient la 11^{ème} place du classement général qui inclut des critères techniques et politiques, mais elle chute à la 21^{ème} place lorsque seuls l’indicateur « politique et gouvernance » est pris en compte.

¹⁵⁴ Algorithm Watch Switzerland, « Réglementation de l’IA: un Conseil fédéral timide », Communiqué de presse, 12 février 2025, <https://algorithmwatch.ch/fr/prise-position-etat-des-lieux-ia/#:~:text=Le%20Conseil%20f%C3%A9d%C3%A9ral%20veut%20r%C3%A9glementer%20l'Intelligence%20artificielle.,la%20concentration%20du%20pouvoir%20au%20sein%20des> (consulté le 5.04.2026).

¹⁵⁵ OCDE, « ICT Access and Usage Database », 2025 <https://goingdigital.oecd.org/datakitchen/#/cover/5/ict/indicator/explore/en>, (consulté le 17.02.2026).

Par ailleurs, il est important de souligner que le recours à l'IA dans un contexte professionnel ne s'inscrit pas toujours, loin s'en faut, dans le cadre d'une stratégie d'entreprise. 31,6 % des répondant·e·s ne se sentaient pas ainsi encouragés par leur employeur¹⁵⁶. Il existe ainsi en Suisse un phénomène d'« IA fantôme » (*shadow AI*) qui renvoie à la banalisation de l'adoption individuelle au travail, hors de tout cadre maîtrisé¹⁵⁷.

L'ampleur et les formes de l'utilisation de l'IA dans les entreprises sont difficiles à indiquer en raison de biais de sélection dans les enquêtes existantes et de la taille limitée des échantillons. Dans l'ensemble, l'absence de données publiques sur l'utilisation et la diffusion de l'IA constitue un problème majeur de gouvernance technologique, qui joue à tous les niveaux, y compris en termes de maîtrise de l'empreinte écologique (voir la section 4.4). Voici cependant les éléments dont on dispose :

- L'adoption de l'IA dans les entreprises dépend fortement de leur taille. Plus celles-ci sont grandes, plus importantes sont les chances qu'elles aient implémenté l'IA dans leur processus de travail. Ce phénomène a été mis en évidence aux États-Unis, où l'adoption de l'IA est significativement plus importante dans les entreprises de plus de 250 employé·e·s¹⁵⁸. En Suisse, cette même conclusion a été tirée d'un rapport sur l'adoption de l'IA par les membres de SwissMem¹⁵⁹. Celui-ci montre également un écart significatif entre l'adoption par les firmes les plus profitables de l'échantillon, où 18 % étaient dans une phase pilote de l'IA, contre seulement 2 % pour le segment des firmes les moins profitables¹⁶⁰.
- Au-delà du nombre d'employé·e·s et de la profitabilité, une étude portant sur l'Allemagne, l'Autriche et la Suisse conclut que des effets de réseaux sont déterminants pour l'adoption de cette technologie. De ce fait, l'emplacement d'une entreprise et son inclusion dans un réseau de connaissances sociotechniques jouent un rôle décisif pour sa mise en place, accentuant les disparités au sein des secteurs¹⁶¹.
- Des différences sectorielles importantes existent également. Selon un rapport d'AXA sur les PME suisses, le pourcentage d'entre-elles ayant implémenté l'intelligence artificielle dans le processus de travail est passée de 22 % en 2024 à 34 % en 2025¹⁶². En 2025, 37 % étaient en phase de test. L'utilisation était plus répandue dans le secteur des services (37 %) que dans l'industrie (20 %), et se faisait principalement dans les grandes PME (entre 50 et 250 employé·e·s). Les principales tâches concernées étaient les traductions, la correspondance et les textes publicitaires. Une autre enquête menée par PwC dans le canton de

¹⁵⁶ Yannis Valentin Schmutz et al., « The Corporate Adoption of Generative AI in Switzerland: A Survey Study », *Bern University of Applied Sciences*, août 2025, <https://www.bfh.ch/dam/jcr:dbdda5f8-3db0-4b5e-9a85-48f54fef24da/gen-ai-survey-2024.pdf> (consulté le 19.03.2026).

¹⁵⁷ Mario Silic, et al., « From shadow it to shadow AI—threats, risks and opportunities for organizations », *Strategic Change*, 2025.

¹⁵⁸ Kathryn Bonney et al., « Tracking firm use of AI in real time: A snapshot from the Business Trends and Outlook Survey », Working Paper 32319, National Bureau of Economic Research, 2024, <https://www.nber.org/papers/w32319>, (consulté le 02.03.2026).

¹⁵⁹ Oliver von Dzengelevski et al., « The state of AI in the Swiss tech industry: Results from a survey by ETH Zurich in cooperation with Swissmem and Next Industries », Rapport, ETH Zurich, 25 juin 2024, p. 9.

¹⁶⁰ *Ibid.*, p. 9.

¹⁶¹ Dahlke, Johannes, et al. "Epidemic effects in the diffusion of emerging digital technologies: evidence from artificial intelligence adoption." *Research Policy* 53.2 (2024): 104917.

¹⁶² AXA Suisse et Sotomo, « AXA KMU-Arbeitsmarktstudie 2025 », *Étude de marché*, juillet 2025.

Genève en 2024¹⁶³ indique que 54 % des PME interrogées affirmaient avoir opérationnalisé des systèmes IA. Les secteurs principaux ayant intégré l'IA étaient des services : les services financiers (76 % des entreprises interrogées indiquent avoir adopté l'IA), l'informatique (71 %), la communication (67 %) et les services immobiliers (67 %). En revanche, seules 14 % des PME du secteur de la construction indiquaient avoir opérationnalisé ces outils.

Le déploiement de l'IA dans le secteur privé est donc modulé par les caractéristiques économiques des entreprises. Leur nombre d'employé·e·s, leur rentabilité, et leur insertion dans des réseaux sociotechniques et leur secteur apparaissent comme des éléments déterminants de cette différenciation. Par ailleurs, deux modalités distinctes de diffusion de cette technologie apparaissent : une diffusion planifiée par les entreprises elles-mêmes côtoie une diffusion spontanée dépendante de l'adoption individuelle des outils par les travailleur·euse·s.

3.3. Diffusion dans les administrations

En 2023, 67 % des pays de l'OCDE avaient intégré l'IA dans le secteur public¹⁶⁴. Des projets similaires sont également progressivement mis en place en Suisse, notamment aux échelons fédéraux avec la formation du Réseau de compétences en intelligence artificielle (CNAI)¹⁶⁵. Cette diffusion reste toutefois différenciée selon les administrations et leurs échelles.

Après une première phase de pilotage, les administrations fédérales dans une période de systématisation. En janvier 2026, 103 projets liés à l'IA dans les administrations avaient été déclarés au CNAI, dont environ 13 % en phase avancée (opérationnels ou en cours de déploiement) (Figure 5). En revanche, la mise en place de l'IA est moins importante dans les plus petites entités comme les communes. Le rapport « l'IA au sein de l'administration publique » publié en 2025 par l'Administration numérique suisse indique que des mesures sont prises dans la formation des employé·e·s à l'utilisation et la mise en place de l'IA sont moins présentes dans les communes, où seules 34% des personnes interrogées affirment avoir suivi une formation, contre 78% au niveau fédéral et 87% dans les cantons¹⁶⁶.

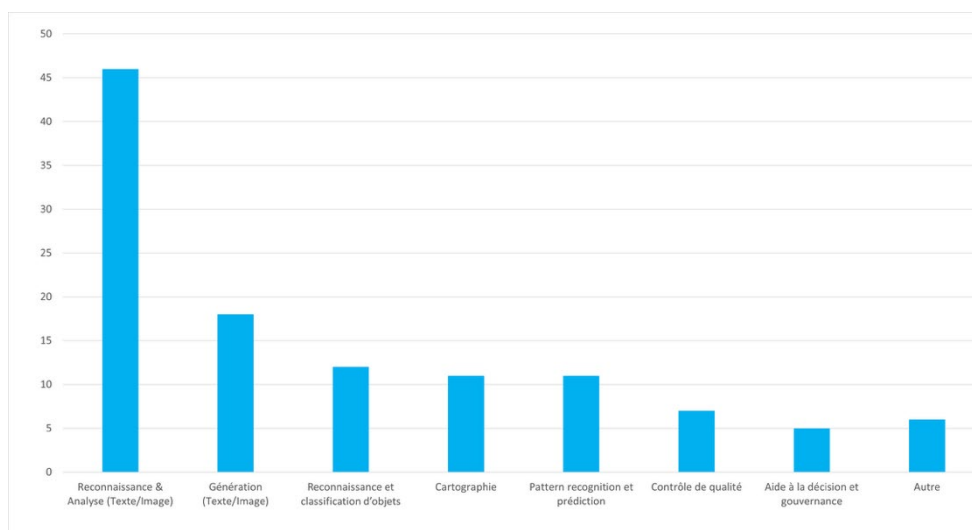
¹⁶³ PwC et OCEI, « Analyse de l'impact de l'intelligence artificielle sur l'économie genevoise : Rapport élaboré sur la base d'une enquête auprès des PME du canton de Genève », Rapport, 2024, <https://www.pwc.ch/fr/insights/secteur-public/impact-de-l-intelligence-artificielle-sur-l-economie-genevoise.html> (consulté le 19.03.2026).

¹⁶⁴ OECD, « AI in public service design and delivery », *Governing with Artificial Intelligence*, juin 2025, https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/ai-in-public-service-design-and-delivery_09704c1a.html (consulté le 24.02.2026).

¹⁶⁵ Chancellerie fédérale, « Réseau de compétences en intelligence artificielle (CNAI) », 12 décembre 2025, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/kuenstliche_intelligenz/kinetzwirk.html (consulté le 24.02.2026).

¹⁶⁶ Administration numérique suisse, « L'IA au sein de l'administration publique : Rapport ciblé sur l'intelligence artificielle dans le cadre de l'étude nationale sur la cyberadministration 2025 », 2025, <https://www.administration-numerique-suisse.ch/application/files/2417/5559/7196/Rapport-cible-IA-2025.pdf> (consulté le 24.02.2026).

Figure 5 : Catégories des projets IA reportés au CNAI¹⁶⁷



Les projets se multiplient, mais, si des lieux de coordination existent, comme le CNAI dans l'administration fédérale ainsi que certains échanges intercantonaux¹⁶⁸, certains experts regrettent l'absence d'une vision générale dans la mise en place de l'IA aux différents échelons administratifs. Dans ce sens, un rapport de Algorithm Watch Switzerland souligne que, en 2023, la plupart des cantons ne sont pas en mesure de transmettre une liste exhaustive des systèmes d'IA utilisés dans leurs administrations¹⁶⁹. Pour l'ONG, ce manque de transparence soulève des problèmes de traçabilité et de contrôle démocratique des décisions faites par les algorithmes.

Ces éléments résonnent avec les résultats d'une enquête sur l'utilisation de l'IA dans l'administration suisse, qui conclut qu'en 2024 le moteur principal de la diffusion des outils d'IA dans l'administration suisse est la curiosité et la motivation personnelle¹⁷⁰. Plus de la moitié des personnes interrogées soulignent une absence de cadre sur l'application de l'IA, et des inquiétudes liées à la protection des données. Ces utilisations individuelles reflètent également l'étendue du phénomène d'IA fantôme précédemment évoqué et également relevé dans les organisations publiques au niveau européen.¹⁷¹ Elles entraînent des risques pour la sécurité des données, la fiabilité des outils de GenAI et la gouvernance de cette technologie.

¹⁶⁷ Chancellerie fédérale, « Réseau de compétences en intelligence artificielle (CNAI): Banque de données de projets 2026 », 26 janvier 2026 <https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/kuenstliche-intelligenz/kinetzwerk.html> (consulté le 24.02.2026). Le recensement des projets se fait sur base volontaire, les données ne sont donc pas exhaustives. Notre classification a été effectuée en fonction des mots clefs déclarés sous "domaines thématiques" puis regroupés par catégorie. Un projet peut donc comporter plusieurs domaines thématiques. Les projets sans indications de domaines thématiques ont été exclus.

¹⁶⁸ Deloitte, « L'intelligence artificielle dans l'administration publique en Suisse », 2024, <https://www.deloitte.com/ch/fr/Industries/government-public/perspectives/kuenstliche-intelligenz-in-der-oeffentlichen-verwaltung-in-der-schweiz.html> (consulté le 24.02.2026).

¹⁶⁹ Algorithm Watch Switzerland, « Un patchwork algorithmique dans les administrations suisses », 25 septembre 2023, <https://algorithmwatch.ch/fr/analyse-algorithmes-dans-les-administrations/> (consulté le 21.04.2026).

¹⁷⁰ Ali Asker Gündüz, *et al.*, « Innovation & Generative Künstliche Intelligenz. Ergebnisse aus der Schweizer Verwaltungspraxis », HSG Publications, août 2025, <https://www.alexandria.unisg.ch/handle/20.500.14171/123251>, (consulté le 20.02.2026).

¹⁷¹ Luca Tangi, *et al.*, « A Silent Partner: The Shadow Presence of Generative Artificial Intelligence in Public Administrations ». In: Hofmann, S., *et al.* Electronic Participation. ePart 2025. Lecture Notes in Computer Science, vol 15978.

Conclusion

Si l'IA est déjà une réalité dans les secteurs privé et public en Suisse, sa diffusion est loin d'être linéaire puisqu'elle varie en fonction du secteur et du type d'organisation. Par ailleurs, l'étendue du phénomène d'IA fantôme dans les entreprises et l'administration indique qu'elle n'obéit pas toujours à stratégie coordonnée. Sa trajectoire de diffusion dépend donc des leviers institutionnels qui l'orientent. Or, les capacités gouvernementales de la Suisse semblent encore insuffisantes pour influencer durablement ce déploiement dans les entreprises et dans les administrations. La Suisse dispose donc d'une certaine marge de manœuvre dans la mise en place de dispositifs de gouvernance de l'IA.

4. Les défis socioéconomiques de l'IA

Le Rapport de l'Assemblée citoyenne publié en février 2026 par l'EPFL AI Center rend compte des préoccupations et attentes d'un panel composé de suisses romand.e.s qui met en évidence l'inquiétude de la population vis-à-vis de la généralisation de cette technologie en termes notamment d'enjeux de sécurité (81 % des répondant.e.s), de désinformation (77 %), de non-respect de la vie privée (65 %) et de pertes d'emplois (59 %) ¹⁷².

Ces préoccupations socio-économiques liées à la diffusion de l'IA sont largement documentées dans la littérature spécialisée et concernent, au sens large, la capacité du peuple souverain à maîtriser son destin. Cette section propose d'examiner ces défis de manière transversale en nous tournant d'abord vers la question des dépendances technologiques, avant de présenter l'état des connaissances en ce qui concerne les risques associés à cette technologie, puis de nous concentrer sur les conséquences sur le travail.

4.1. Des dépendances technologiques marquées mais différenciées

La question des dépendances technologiques en matière d'IA se pose aux différents niveaux de la chaîne de valeur qui contribuent au développement et au fonctionnement des systèmes d'IA. Comme le résume un article scientifique récent, les données, les algorithmes, le calcul et le capital humain jouent chacun un rôle essentiel dans le développement et le déploiement de l'IA :

Les données sont la matière première traitée par le calcul ; en d'autres termes, le calcul est le « moteur » alimenté par de grandes quantités de données. Il existe un secteur en pleine croissance qui se concentre sur la production de ces données, et des investissements importants sont réalisés dans de nouvelles méthodes permettant de générer des données d'entraînement précieuses avec moins d'intervention humaine. Les algorithmes dictent les opérations effectuées sur les données pour produire des capacités d'IA. Les algorithmes englobent le code source qui définit tout, de l'architecture des modèles d'IA aux méthodologies spécifiques utilisées dans leur calibrage. La puissance de calcul (et le matériel et les logiciels associés) est utilisée pour exécuter les algorithmes et sert de « substrat » au traitement de l'information impliqué dans l'IA. Enfin, le capital humain est important pour produire des données, des algorithmes et des calculs, et pour faire fonctionner le processus de formation lui-même. ¹⁷³

Les questions du travail et des compétences seront discutées plus loin (voir la section 4.3) ; nous nous focaliserons ici sur trois niveaux : celui des données, en lien avec le caractère de technologie sociale et culturelle des systèmes d'IA ; celui des algorithmes, et plus spécifiquement le niveau des modèles d'IA ; et des centres de données où sont déployées des puces électroniques avancées pour entraîner les systèmes d'IA et traiter

¹⁷² Mélissa Anchisi, *Assemblée citoyenne sur l'intelligence artificielle*, s.l., EPFL AI Center, 2026.

¹⁷³ Girish Sastry et al., « Computing power and the governance of artificial intelligence », *arXiv preprint arXiv:2402.08797*, 2024, p. 7-8.

les requêtes des utilisateurs finaux. Dans ces trois domaines, les firmes basées aux États-Unis exercent une domination très nette, dont il est important de saisir la mesure dans le contexte helvétique.

Les traits sociaux, culturels et cognitifs charriés par les données dans les systèmes d'IA

Les modèles de langage ne sont pas en tant que tels des agents intelligents mais plutôt une nouvelle forme de technologie culturelle et sociale, permettant aux humains de tirer profit des informations accumulées par d'autres humains. Cependant, dans un grand nombre de cas, en particulier avec les agents conversationnels, cette technologie est déployée de telle sorte qu'elle prend des traits humains (anthropomorphisme) tels que la création de liens émotionnels (par exemple, l'empathie et la reconnaissance) avec les utilisateurs et l'emploi du pronom à la première personne¹⁷⁴. Ainsi, cet artefact puissant - d'apparence omnisciente et toujours disponible - prend la forme d'une personne extraordinaire digne de confiance. Les explications des systèmes d'IA synthétiquement fluides, numériquement précises et visuellement formatées se présentent comme des outputs faisant autorité, supprimant le scepticisme des individus auxquels elles s'adressent¹⁷⁵. Au-delà des enjeux de sécurité, des biais générant des discriminations (4.2) et des risques de perte de compétences (voir la section 4.3), cela soulève la question de l'adéquation socio-culturelle au contexte de leur utilisation.

Les grands modèles de langage (LLM) et les grands modèles multimodaux sont des modèles statistiques qui traitent d'énormes masses de données produites par les humains, qu'il s'agisse de texte, de sons, d'images, de vidéos. Les LLMs compilent des masses considérables de textes, les décomposent en mots distincts et estiment la distribution de probabilité de longues séquences de mots. Comme le note un article récent paru dans la revue *Science*, « il s'agit d'une représentation imparfaite du langage, mais elle contient une quantité étonnamment importante d'informations sur les schémas qu'elle résume. Cela permet au LLM de prédire quels mots viennent ensuite dans une séquence et ainsi de générer un texte de type humain »¹⁷⁶. La puissance de ces modèles tient au fait qu'ils sont non seulement capables de puiser dans un vaste corpus de la culture humaine, mais également d'y effectuer une grande variété de nouvelles opérations. En d'autres termes, ils ne se contentent pas de répertorier, résumer ou condenser de l'information, mais ils la réorganisent de manière à produire de nouvelles représentations qui contribuent à l'évolution socio-culturelle.

Ce sont des machines conçues pour fonctionner efficacement et reproduire fidèlement, en fonction de la requête, les probabilités estimées des séquences de texte, d'images et de vidéo — en moyenne. Les données sur lesquelles elles sont entraînées constituent donc le centre de gravité du type de vérité qu'elles produisent. Or, les données sur lesquelles se fondent les modèles les plus populaires en Occident sont des données

¹⁷⁴ Lujain Ibrahim et al., « Multi-turn evaluation of anthropomorphic behaviours in large language models », *arXiv preprint arXiv:2502.07077*, 2025.

¹⁷⁵ Ikram Chraïbi Kaadoud, *IA et métacognition : savoir quand on peut faire confiance, ou non, à la machine n'est pas toujours évident*, <https://theconversation.com/ia-et-metacognition-savoir-quand-on-peut-faire-confiance-ou-non-a-la-machine-nest-pas-toujours-evident-279348>, 29 mars 2026, (consulté le 22 avril 2026).

¹⁷⁶ Henry Farrell et al., « Large AI models are cultural and social technologies », *Science*, 2025, vol. 387, n° 6739, p. 1154.

majoritairement de langue anglaise et provenant de manière dominante des États-Unis¹⁷⁷. Cette génétique des modèles a des implications pour le type de tendance culturelle qu'ils véhiculent¹⁷⁸, ce qui pose deux types de problèmes. D'une part, les modèles ont « une tendance intrinsèque à être les plus précis dans les situations les plus courantes de leurs données d'apprentissage et les moins précis dans les situations qui étaient rares dans ces données ou totalement nouvelles »¹⁷⁹, ce qui a pour conséquence une moindre adéquation des réponses au contexte minoritaire, par exemple en termes de style de raisonnement cognitif ou de système de valeurs. D'autre part, il y a un risque d'homogénéisation culturelle. Les modèles peuvent accélérer la diffusion de la culture dominante et ce de manière d'autant plus puissante que les traits socioculturels sont directement véhiculés dans des interactions anthropomorphes avec les individus.

Les chatbots et les systèmes multiagents d'IA: un espace concurrentiel et hétérogène

A l'échelle mondiale, un nombre important de chatbots et de systèmes multiagents d'IA sont utilisés. ChatGPT, qui a été le premier produit grand public lancé en octobre 2022, reste dominant avec presque 60 % du trafic début 2026, mais il existe désormais de nombreux autres outils dont certains comme Google Gemini, Gork adossé à X ou Claude d'Anthropic connaissent une croissance très rapide (Figure 6).

La situation se caractérise donc par une domination très nette des entreprises étasuniennes. Si les dépendances sont certaines, elles ne sont cependant pas figées. La courte histoire de l'IA de masse est déjà jalonnée de moments dramatiques comme lors du lancement de DeepSeek R1, en janvier 2025, dont le caractère économe en calcul pour des performances proches de celles des leaders avait surpris. Un an plus tard, ce sont les performances de Claude qui secouent l'industrie¹⁸⁰. Au-delà de ces divers épisodes, une tendance apparaît. Les outils d'IA sont en voie de « commodification ». D'une part, l'écart entre les outils chinois et les leaders états-uniens se réduit très sensiblement¹⁸¹ et, d'autre part, à mesure que les modèles d'IA sous-jacents progressent, des améliorations marginales ne sont plus décisives pour la plupart des utilisateurs. Ces deux éléments augurent d'un déplacement de la qualité vers les coûts dans la dynamique concurrentielle qui va probablement conduire à une forte restructuration du marché en faveur des modèles d'IA sous-jacents chinois¹⁸² ou européens moins coûteux. Dans tous les cas, il est significatif que, si la domination de ChatGPT est nette, la part des outils d'IA varie notablement d'un pays à l'autre (Figure 7). Cette diversité atteste de l'instabilité de la situation et fait apparaître une forme de

¹⁷⁷ Vered Shwartz, *Artificial intelligence needs to be trained on culturally diverse datasets to avoid bias*, <https://theconversation.com/artificial-intelligence-needs-to-be-trained-on-culturally-diverse-datasets-to-avoid-bias-222811>, 13 février 2024, (consulté le 22 avril 2026).

¹⁷⁸ Jackson G. Lu, Lesley Luyang Song et Lu Doris Zhang, « Cultural tendencies in generative AI », *Nature Human Behaviour*, 20 juin 2025, vol. 9, n° 11, p. 2360-2369.

¹⁷⁹ H. Farrell et al., « Large AI models are cultural and social technologies », art cit, p. 1155.

¹⁸⁰ George Hammond, « Anthropic's breakout moment: how Claude won business and shook markets », *Financial Times*, 6 févr. 2026p.

¹⁸¹ Nestor Maslej et al., « Artificial Intelligence Index Report 2025 ».

¹⁸² June Yoon, « Is an AI price war about to begin? », *Financial Times*, 19 févr. 2026p.

divergence entre les pays occidentaux et le monde chinois (ici Hong-Kong) qui pourrait se prolonger dans d'autres pays en développement.

L'existence en Suisse d'un LLM public, Apertus, est un point d'appui important. Si celui-ci n'est pas destiné à concurrencer les leaders auprès du grand public, il donne cependant la possibilité aux acteurs suisses de développer une alternative sûre adaptable à des fonctions stratégiques. En effet, les modèles plus petits peuvent être efficaces, plus accessibles aux petites et moyennes entreprises (PME) et moins gourmands en énergie¹⁸³. À mesure que la technologie se développe, l'espace s'élargit pour des options dont l'intérêt n'est pas d'être à la frontière, mais d'être robustes et sûres.

Néanmoins, il est évident que du fait de la taille réduite de la Suisse, les mécanismes de marché seuls ne peuvent suffire à faire émerger des solutions alternatives locales aux leaders sur l'ensemble des segments des systèmes d'IA, ce qui implique qu'un mix d'intervention publique (réglementation, commande publique, investissements...) de coopération internationale et de diversification doit être envisagé.

Figure 6 : Trafic mondial sur les principaux chatbots d'IA en janvier 2026 (Similarweb)

¹⁸³ Anouch Seydtaghia, « Apertus, projet suisse majeur en IA, aura une nouvelle version au printemps », *Le Temps*, 10 févr. 2026p.

Figure 7 : Répartition du trafic sur les principaux chatbots d'IA en Suisse et pour une sélection d'autres pays en janvier 2026 (Similarweb)

Les capacités de calcul : la localisation

Le second enjeu, en termes de dépendance, concerne les capacités de stockage et de traitement des données. Du fait de la centralité des capacités de calcul dans le développement de l'IA et de son déploiement, celle-ci devient un enjeu de souveraineté pour les États, au même titre, par exemple, que les câbles de communication sous-marins concernant l'accès à internet¹⁸⁴. L'accès aux ressources informatiques fournies par des centres de données situés à l'étranger et/ou détenus par des entités étrangères est une question particulièrement sensible car elle comporte des risques d'espionnage, de sabotage, d'augmentation des prix, d'ingérence politique ou de contraintes géopolitiques. Les conditions d'accès aux ressources cloud nécessaires à la mise en œuvre des processus d'IA constituent ainsi l'une des dimensions décisives de la souveraineté numérique dans le contexte de l'IA, appelée *AI Compute Sovereignty*¹⁸⁵.

Une première manière de concevoir cette dimension de la souveraineté renvoie à la disponibilité, sur une juridiction territoriale donnée, de centres de données capables d'entraîner des modèles d'IA ou, de manière plus réduite, d'inférer des réponses d'IA pour donner suite aux requêtes des utilisateurs. À l'aune de ce critère-là, selon une étude préliminaire de l'OCDE, la Suisse dispose de seulement une partie des ressources informatiques nécessaires à l'IA ; les centres de données qu'elle héberge permettent de traiter des requêtes, mais seraient insuffisants pour entraîner des modèles, à la différence des principaux pays de l'OCDE ainsi que de la Chine et de rares pays en développement (Inde, Brésil, Afrique du Sud, Émirats arabes unis). Cependant, grâce aux investissements publics réalisés, ses compétences ont été acquises, comme en témoigne le lancement du LLM public Apertus, développé par la Swiss AI Initiative, en co-

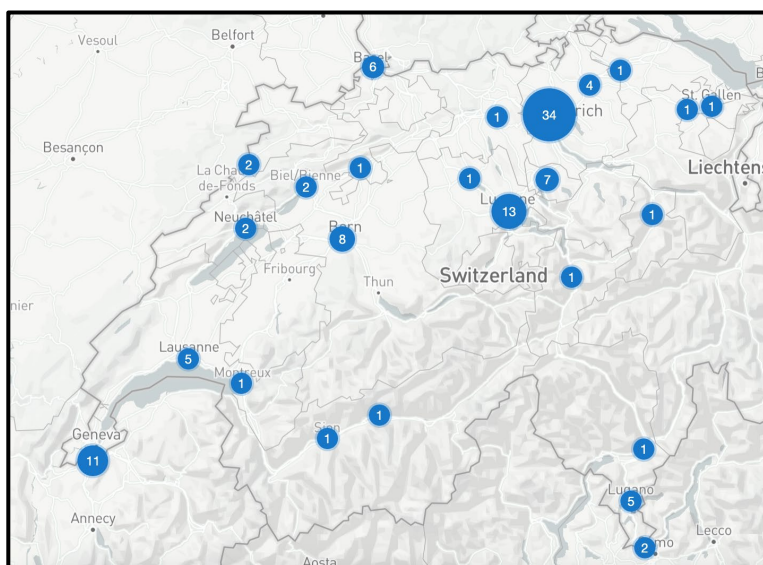
¹⁸⁴ G. Sastry et al., « Computing power and the governance of artificial intelligence », art cit ; Lars Gjesvik, « Private infrastructure in weaponized interdependence », *Review of International Political Economy*, 2 mai 2022, p. 1-25.

¹⁸⁵ Zoe Hawkins, Vili Lehdonvirta et Boxi Wu, « AI compute sovereignty: Infrastructure control across territories, cloud providers, and accelerators », *Cloud Providers, and Accelerators* (June 20, 2025), 2025.

développement avec l'École polytechnique fédérale de Lausanne, l'École polytechnique fédérale de Zurich et le Centre suisse de calcul scientifique¹⁸⁶.

En Suisse même, les capacités se concentrent principalement dans la région de Zurich, même si d'autres cantons et en particulier Genève accueillent aussi des centres de données (Figure 8), y compris dédiés à l'IA¹⁸⁷. Néanmoins, il est important d'avoir à l'esprit qu'une large part des requêtes associées à l'IA mobilise des ressources informatiques situées dans un autre pays. Dans le cas de la France, pour l'année 2024, 58% des consommations d'énergie associées à l'utilisation des centres de données avaient lieu à l'étranger¹⁸⁸, ce qui souligne les dépendances internationales en la matière.

Figure 8 : Localisation et nombre des centres de données en Suisse (<https://www.datacentermap.com/switzerland/>, consulté le 25 février 2025)



Les capacités de calcul : la distribution du contrôle

Une deuxième manière de concevoir la souveraineté sur les centres de données consiste à regarder la nationalité des entreprises qui fournissent des services de cloud d'IA. Plus encore que pour les chatbots, la domination des firmes états-uniennes sur le cloud en général est écrasante et concentrée, puisque les trois géants états-uniens (Amazon Microsoft et Google) captent à eux seuls les deux tiers des revenus cloud (Figure 9). Ce marché en très forte croissance est évalué à 107 milliards de dollars au troisième trimestre 2025, contre 68 milliards deux ans plus tôt. Cette dynamique laisse la possibilité à un grand nombre d'acteurs hors du trio de tête de se développer, notamment

¹⁸⁶ ETHZ, *Apertus: a fully open, transparent, multilingual language model*, <https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a-fully-open-transparent-multilingual-language-model.html>, 2 septembre 2025, (consulté le 18 mars 2026).

¹⁸⁷ Microsoft Switzerland, *Microsoft Deepens Switzerland's Digital Future with Strategic Investment in Cloud and AI Infrastructure, Startups, Skilling and Innovation*, <https://news.microsoft.com/de-ch/2025/06/02/microsoft-deepens-switzerlands-digital-future-with-strategic-investment-in-cloud-and-ai-infrastructure-startups-skilling-and-innovation/>, 2 juin 2025, (consulté le 25 février 2026).

¹⁸⁸ Lorraine De Montenay et al., *Prospective d'évolution des consommations des data centers à court, moyen et long terme de 2024 à 2060*, <https://librairie.ademe.fr/energies/8910-prospective-d-evolution-des-consommations-des-data-centers-a-court-moyen-et-long-terme-de-2024-a-2060.html>, janvier 2026, (consulté le 25 février 2026).

mais pas seulement en Chine avec Alibaba, Tencent et Huawei¹⁸⁹. En ce qui concerne la Suisse, le risque de militarisation de cette dépendance est aggravé par le fait que les grandes infrastructures cloud, y compris pour l'IA, sont dans leur totalité dominées les firmes états-uniennes, contrairement à un certain nombre de pays comme l'Allemagne, la France, la Grande Bretagne, le Canada ou la Corée qui abritent également des cluster dominés par des firmes chinoises et/ou européennes de manière à se prémunir des risques que fait peser un alignement complet sur des fournisseurs venus d'un seul pays¹⁹⁰. Il faut cependant souligner qu'outre l'infrastructure publique ALPS, la présence d'Exoscale, une entreprise de Cloud dont le siège est à Lausanne, peut constituer un point d'appui à une politique de souveraineté, et que d'autres fournisseurs de services existent en Europe tels que OVHcloud basé en France et Hetchner basé en Allemagne.

Une dernière manière de concevoir les relations de dépendance en matière de calcul renvoie aux capacités technologiques associées aux puces électroniques nécessaires au fonctionnement de l'IA. Là encore, la domination des États-Unis est écrasante avec, au premier chef, la place de NVIDIA pour la conception en association avec TSMC basé principalement à Taiwan. La Chine est le seul autre pays capable de concevoir et de produire des puces avancées pour l'IA. La situation de dépendance de la Suisse aux États-Unis est donc conforme à celle des autres pays à haut revenu. En Europe seul STMicroelectronics produit des puces, mais pas au niveau le plus avancé, et Amazon est en passe d'entrer au capital de l'entreprise¹⁹¹.

La demande pour ces puces très sophistiquées est telle qu'elle conduit les fabricants à reconfigurer leurs lignes de production, entraînant des hausses de prix et des difficultés d'approvisionnement sur d'autres types de puces électroniques, ce qui affecte de nombreux secteurs, y compris bien sûr le matériel informatique, la téléphonie ou l'automobile¹⁹².

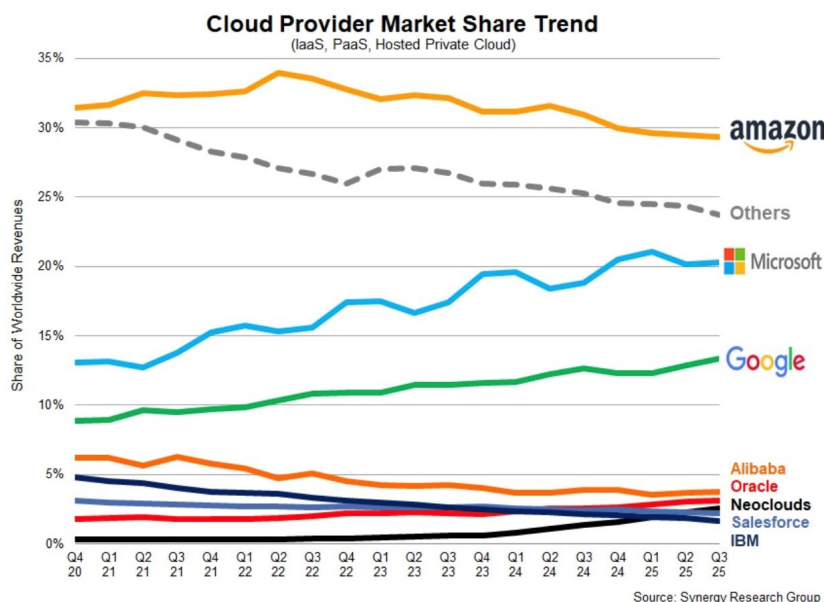
¹⁸⁹ Synergy Research Group, *Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher*, <https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher>, 19 novembre 2025, (consulté le 25 février 2026).

¹⁹⁰ Z. Hawkins, V. Lehdonvirta et B. Wu, « AI compute sovereignty: Infrastructure control across territories, cloud providers, and accelerators », art cit.

¹⁹¹ Laghrari, *STMicroelectronics s'envole en Bourse après un contrat à plusieurs milliards avec Amazon*, <https://www.lesechos.fr/tech-medias/hightech/stmicroelectronics-senvole-en-bourse-apres-un-contrat-a-plusieurs-milliards-avec-amazon-2214854>, 9 février 2026, (consulté le 25 février 2026).

¹⁹² Ian King et al., « Why the AI Boom Will Make Phones, Cars and Electronics More Expensive », *Bloomberg.com*, 8 mars 2026p.

Figure 9 : Évolution de la répartition mondiale des revenus tirés des services d'infrastructure cloud aux entreprises (Synergy Group, 2025)



4.2. Des risques mal maîtrisés

Les événements mettant en évidence des risques ou des préjudices effectifs liés à l'IA se multiplient à un rythme qui s'accélère à l'échelle mondiale, comme en Suisse (Figure 10) ce qui pose à la fois la question de la sécurité de l'IA et celle des torts déjà causés.

Figure 10 : Nombres d'incidents et de situations dangereuses recensés dans le monde et en Suisse depuis 2022 (OCDE)¹⁹³

¹⁹³ OCDE, *OECD AI Incidents Monitor, an evidence base for trustworthy AI*, <https://oecd.ai/en/incidents>, 2026, (consulté le 27 février 2026). Un événement où le développement ou l'utilisation d'un système d'IA entraîne un préjudice *réel* est qualifié d'« incident lié à l'IA », tandis qu'un événement où le développement ou l'utilisation d'un système d'IA est *potentiellement* préjudiciable est qualifié de « risque lié à l'IA ». OECD, *Defining AI incidents and related terms*, s.l., 2024, vol.16.

Incertitudes sur la sécurité

Le déploiement à grande échelle des systèmes d'IA pose des problèmes de sécurité majeurs¹⁹⁴. L'amélioration des capacités en matière d'IA, plus rapide que ne le prévoyaient de nombreux experts, a pour conséquence que le nombre et la criticité des risques identifiés ont considérablement augmenté ces derniers mois, sans que les techniques de prévention ne parviennent à suivre¹⁹⁵. Une évaluation récente du Future of Life Institute (FLI) portant sur 8 des principaux modèles d'IA note que les progrès réalisés par les firmes ne comblent pas le fossé structurel qui se creuse entre le développement des capacités et la préparation en matière de sécurité, si bien que, dans l'ensemble, les mesures de sécurité sont très insuffisantes¹⁹⁶.

Dans le détail, ce rapport du FLI remarque notamment que l'évaluation des risques et les mesures de sécurité prises se concentrent sur les menaces graves pour la santé publique, la sécurité et l'environnement (CBRN **C**hemical, **B**iological, **R**adiological, or **N**uclear materials). En revanche, les dégradations écologiques associées au développement des centres de données ne sont pas prises en compte tandis que les risques sociétaux et systémiques sont laissés dans le flou. Le rapport parle à cet égard d'une « hypocrisie fondamentale » quant au risque existentiel. Bien que les dirigeants d'entreprises telles qu'Anthropic, Google DeepMind, OpenAI, xAI et Z.ai aient publiquement exprimé leurs inquiétudes à ce sujet, ces firmes ne déploient pas de stratégies concrètes en la matière et, pour la plupart, fournissent un effort de lobbying intense contre le renforcement de la réglementation.

En l'état actuel, parmi les entreprises basées aux États-Unis et au Royaume-Uni, seule Anthropic inclut des engagements explicites en matière de transparence, tels que solliciter l'avis d'experts et informer les autorités américaines en cas d'incident au-delà du niveau ASL-2¹⁹⁷. Pourtant, les résultats des recherches récentes sont très préoccupants quant au risque de perte d'alignement¹⁹⁸. Le phénomène connu sous le nom de « jailbreaking » consiste à manipuler les LLM afin de contourner leurs mesures de sécurité intégrées, ce qui peut les amener à générer des résultats nuisibles, toxiques ou contraires à l'éthique. Auparavant, c'était un processus long et intensif en travail, désormais, un seul modèle à haute capacité peut planifier et mener de manière autonome des attaques persuasives à plusieurs tours. Cette évolution « laisse présager une dynamique de « régression de l'alignement », c'est-à-dire une dynamique dans laquelle des générations successives de modèles de langage de plus en plus performants pourraient, paradoxalement, affaiblir plutôt que renforcer l'alignement, car leurs capacités de raisonnement avancées pourraient être détournées pour

¹⁹⁴ Diego Kuonen et Gérard Vernez, « Sécurité en mutation : l'effet IA. », *Cybersecurity trends*, 2025p. 31-34p.

¹⁹⁵ L'examen le plus exhaustif des risques à notre connaissance se trouve ici : Yoshua Bengio et al., « Rapport international sur la sécurité de l'IA 2026 », *arXiv preprint arXiv:2602.21012*, 2026.

¹⁹⁶ Future of Life, *FLI AI Safety Index*, Campbell, California, 2025.

¹⁹⁷ AI Safety Level 2 désigne les systèmes qui présentent des signes précurseurs de capacités dangereuses, par exemple la capacité de donner des instructions sur la fabrication d'armes biologiques.

¹⁹⁸ Le risque d'alignement désigne la menace potentielle qui survient lorsque les objectifs visés par les systèmes technologiques et leurs résultats réels entraînent des conséquences imprévues et potentiellement indésirables.

compromettre les mécanismes de sécurité des modèles antérieurs, moins performants »¹⁹⁹.

Une illustration de ces inquiétudes croissantes est la décision de l'armée suisse d'écarter l'adoption des logiciels de Palantir pour deux raisons. La première, la possibilité que le gouvernement ou les services de renseignements des États-Unis puissent accéder par ce biais à des données sensibles ; la seconde concerne les atteintes à la vie privée et le risque d'erreur, le rapport concluant qu'il ne pouvait être exclu « que certaines personnes puissent être ciblées involontairement sur la base de corrélations statistiques »²⁰⁰. Les lignes rouges mises par l'entreprise Anthropic sur l'emploi de ses systèmes d'IA qui ont conduit le Pentagone à classer l'entreprise comme un risque pour la sécurité ne sont guère rassurantes. Au refus d'armes complètement autonomes en raison du manque de fiabilité de l'IA actuelle, Anthropic ajoute que « l'utilisation de ces systèmes à des fins de surveillance *domestique* massive est incompatible avec les valeurs démocratiques »²⁰¹. L'insistance sur le caractère domestique de la surveillance de masse implique que l'entreprise n'a pas d'objection à ce que celle-ci soit déployée dans d'autres pays.

Des préjudices déjà tangibles

Une question essentielle est celle des données transmises lors de l'utilisation de l'IA puisque par défaut « tous les modèles d'IA s'entraînent sur les données issues des interactions » avec les utilisateurs, les informations sensibles partagées lors des interactions peuvent être récupérées ultérieurement²⁰². C'est un problème pour les libertés individuelles mais aussi pour les organisations, firmes et administrations, pour lesquelles l'utilisation non encadrée des chatbots par les travailleurs·ses constitue une brèche de sécurité sérieuse.

Un autre type de préjudice provient des usages malveillants, lorsque des contenus générés par IA sont utilisés à des fins criminelles telles que la fraude, l'usurpation d'identité et le chantage (Tableau 2). Le risque d'escroquerie n'est pas cantonné à des individus, puisque, dans certains cas, l'identité de dirigeants d'entreprise a été compromise, conduisant à des virements de dizaines de millions de dollars au bénéfice de fraudeurs, incitant des administrateurs de systèmes techniques à fournir des informations telles que des identifiants de connexion. D'autres fois, des *deepfakes* sont utilisés pour nuire à la réputation de personnes ou exercer un chantage, ce qui là aussi peut créer des vulnérabilités pour des organisations. Enfin, la grande majorité des *deepfakes* est constituée de contenus sexuels ciblant de manière disproportionnée les femmes et les jeunes filles, et comprend également la production de contenus pédopornographiques.

¹⁹⁹ Thilo Hagendorff, Erik Derner et Nuria Oliver, « Large reasoning models are autonomous jailbreak agents », *Nature Communications*, 5 février 2026, vol. 17, n° 1, p. 1435.

²⁰⁰ Marguerite Meyer et al., « How tenaciously Palantir courted Switzerland », *Republik*, 8 décembre 2025 ; Schweizer Armee, *Palantir Technologies Inc.*, Bern, 2024. Rafe Rosner-Uddin et Mercedes Ruehl, « Palantir sues magazine that revealed Switzerland rejected its approaches », *Financial Times*, 22 févr. 2026p.

²⁰¹ Dario Amodei, *Statement on our discussions with the Department of War*, <https://www.anthropic.com/news/statement-department-of-war>, février 2026, (consulté le 28 février 2026).

²⁰² Future of Life, *FLI AI Safety Index*, op. cit., p. 4.

Tableau 2 : Types d'usages malveillants de faux contenus générés par IA contre les personnes ²⁰³

Diffamation	Génération d'un faux contenu qui présente une personne se livrant à des activités compromettantes telles qu'une activité sexuelle ou la consommation de drogue, puis diffusion de ce contenu afin d'entacher sa réputation, de nuire à sa carrière et/ou de la forcer à se retirer des activités publiques (par exemple de la politique, du journalisme ou des divertissements)
Abus psychologiques/intimidation	Génération de représentations nuisibles d'un individu dans le but principal de le harceler et de lui causer un traumatisme psychologique . Les victimes sont souvent des enfants.
Escroquerie/fraude	Utilisation de l'IA pour générer du contenu (tel qu'un clip audio usurpant la voix d'une victime), par exemple pour autoriser une transaction financière .
Chantage/extorsion	Production de faux contenus sur une personne tels que des images intimes, sans son consentement, et menace de les divulguer si les demandes financières ne sont pas satisfaites .

Un troisième type de problème résulte des biais sexistes et racistes incorporés dans les modèles²⁰⁴. Il a ainsi été montré que les chatbots suggéraient aux femmes des prétentions salariales plus faibles que celles des hommes à un niveau de compétence équivalent, que leur accès au crédit était entravé, que les diagnostics médicaux étaient de moindre qualité pour les femmes que pour les hommes. La littérature indique également que les outils d'IA utilisés dans le recrutement peuvent discriminer activement les candidates féminines, ainsi que les candidates portant un foulard et les personnes dont le nom « sonne noir ». Alors que se pose la question de l'automatisation d'un certain nombre de procédures, ces biais constituent un obstacle important, à la fois du point de vue de l'exigence de traitement égalitaire entre les personnes et du point de vue de la qualité de la décision, puisque les biais impliquent que des options plus favorables – par exemple des candidates plus compétentes – risquent d'être écartées.

Enfin, sans que cette liste ne soit exhaustive, deux derniers points doivent être soulevés. Le premier concerne les cyberattaques : les systèmes d'IA sont déjà mobilisés pour élaborer des attaques, identifier des failles de sécurité et, à l'avenir, les systèmes d'IA pourraient eux-mêmes être vulnérables à des attaques qui les orienteraient vers des objectifs cachés²⁰⁵. De plus, une course est engagée entre l'automatisation de la fabrication et de la diffusion de fausses nouvelles et le développement de modèles censés les identifier²⁰⁶. Le second porte sur le pouvoir de persuasion des dispositifs d'IA. S'il existe peu de preuves systématiques que la manipulation par IA dans le monde réel soit actuellement répandue ou efficace par rapport au contenu généré par des

²⁰³ Y. Bengio et al., « Rapport international sur la sécurité de l'IA 2026 », art cit, p. 52.

²⁰⁴ Laura Bates, « How tech turned against women », *Financial Times*, 21 févr. 2026p. *When AI gets it wrong: the problem of bias in data*, <https://www.supsi.ch/quando-l-ia-sbaglia-il-problema-degli-stereotipi-nei-dati>, 15 septembre 2023, (consulté le 22 avril 2026).

²⁰⁵ Y. Bengio et al., « Rapport international sur la sécurité de l'IA 2026 », art cit, p. 64-72.

²⁰⁶ Ehtesham Hashmi et al., « Advancing fake news detection: Hybrid deep learning with fasttext and explainable ai », *IEEE access*, 2024, vol. 12, p. 44462-44480 ; Pranshu Verma, « The rise of AI fake news is creating a 'misinformation superspreader' », *The Washington Post*, 2023, December 17 2023.

personnes, les recherches expérimentales indiquent que les chatbots ont une force de persuasion qui augmente avec la puissance des modèles, atteignant des niveaux similaires voire surpassant ceux des humains²⁰⁷. Cet aspect est particulièrement pertinent dans un contexte où l'usage quotidien de l'IA est massifié en Suisse, où l'importance de la démocratie directe multiplie les opportunités d'influer sur la décision publique. Mais le problème est aussi que les firmes apprennent à manipuler à des fins commerciales les recommandations fournies par les IA²⁰⁸, ce qui risque d'altérer les décisions d'achat des organisations comme des individus.

Déplacement des capacités administratives, vulnérabilités techniques et coût économique croissant

Au-delà des incertitudes sur la fiabilité et des préjudices déjà observables associés au déploiement des systèmes d'IA, la manière dont ces systèmes sont contrôlés par un petit nombre d'entreprises pose des risques associés au pouvoir infrastructurel qu'elles en retirent. De manière non exhaustive, trois principaux enjeux peuvent être identifiés.

Le premier concerne les capacités administratives. Jusqu'au début du siècle, les statistiques collectées par les États dépassaient de loin celles dont disposaient les entreprises. Avec l'essor des Big Tech en général et des systèmes d'IA plus récemment, un basculement fondamental a lieu. Les grandes firmes du numérique disposent désormais des capacités statistiques les plus puissantes et déploient de multiples façons les pouvoirs quasi-politiques de conformation des comportements qui en découlent²⁰⁹. Ainsi, il y a déjà une dizaine d'années, les sociologues Marion Fourcade et Kieran Healy notaient que « de nombreuses entreprises optimisent la visibilité des utilisateurs en regroupant leurs services sous un profil utilisateur unique. Autrefois, l'État était la seule entité disposant des ressources nécessaires pour identifier et suivre les individus dans de nombreux contextes et environnements. Ce n'est plus le cas aujourd'hui. »²¹⁰. Depuis, le phénomène n'a fait que s'accroître. Les firmes privées disposent de davantage de capacités de calcul et de davantage de données que les États, elles sont en outre moins entravées que ceux-ci pour croiser leurs données, ce qui leur donne des capacités administratives accrues. Les solutions qu'elles proposent aux administrations et les exigences de mise en place de standards d'accès aux données publiques (API) renforcent ce phénomène et des entreprises comme Palantir, se présentent désormais comme des auxiliaires intégrés de l'ensemble des processus administratifs. La question posée est donc celle de l'intégrité dans la durée de l'action de la puissance publique dès lors que les capacités logistiques à mettre en œuvre des décisions politiques²¹¹ s'érodent tandis que croissent celles des grandes firmes numériques.

²⁰⁷ Y. Bengio et al., « Rapport international sur la sécurité de l'IA 2026 », art cit, p. 57-62.

²⁰⁸ Christopher Mims, « How Businesses Are Manipulating ChatGPT Results », *Wall Street Journal*, 30 janv. 2026p.

²⁰⁹ Shoshana Zuboff, *The age of surveillance capitalism: the fight for the future at the new frontier of power*, London, Profile Books, 2019, 691 p ; Antoinette Rouvroy et Thomas Berns, « Gouvernamentalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, 2013, vol. 177, n° 1, p. 163-196.

²¹⁰ Marion Fourcade et Kieran Healy, « Seeing like a market », *Socio-Economic Review*, 23 décembre 2016, p. 19.

²¹¹ Michael Mann parle à ce sujet de pouvoir infrastructurel. Michael Mann, « The autonomous power of the state: its origins, mechanisms and results », *European Journal of Sociology/Archives européennes de sociologie*, 1984, vol. 25, n° 2, p. 185-213.

Le second enjeu associé au déploiement de l'IA sur le territoire suisse concerne les incertitudes sur la disponibilité technique des produits à moyen et long terme. Cette question comporte de multiples dimensions. Nous évoquerons ici seulement le phénomène de bulle de l'IA qui renvoie à des investissements colossaux et financés par endettement alors que les pertes ne cessent de croître²¹². La promesse est celle d'une rentabilité à venir, mais il est important d'avoir conscience qu'une part essentielle des investissements réalisés concerne des puces électroniques qui deviennent rapidement obsolètes. Autrement dit, maintenir des infrastructures de calcul dans la durée risque de coûter très cher. Si la rentabilité se fait trop attendre, des faillites pourraient déstabiliser l'offre et conduire à des ruptures de service et à une réduction de la puissance de calcul disponible pour les requêtes d'IA ordinaires.

L'envers de cette rentabilité, c'est bien sûr l'augmentation des coûts des services d'IA pour les utilisateurs. Pour l'instant, les services sont mis à disposition à un coût bien inférieur à leur coût effectif. Comme l'explique Bloomberg, « La stratégie à long terme du secteur repose sur l'offre de logiciels d'IA plus avancés, notamment des agents capables d'automatiser les tâches à plus forte valeur ajoutée et ainsi inciter les entreprises à consacrer une part plus importante de leurs budgets à ces outils. »²¹³ Si les gains d'efficacité se concrétisent, les entreprises et les administrations auront les moyens d'assumer les coûts. Mais même si leur impact est moindre, les investisseurs en IA pourraient tout de même réaliser d'importants bénéfices. Si, d'ici quelques années, les systèmes d'IA, à la faveur de prix artificiellement bas, ont tellement intégré les processus de travail que les coûts de sortie sont devenus prohibitifs, les clients ne pourront plus s'en passer et seront contraints de payer. Dans un monde accro à l'IA, les entreprises technologiques engrangeront des profits considérables, sans nécessairement que les gains attendus du côté des clients soient effectivement au rendez-vous.

Tant du point de vue des capacités administratives, de la robustesse des services ou du risque de voir la facture croître de manière incontrôlée, la dépendance à quelques acteurs pour la fourniture de systèmes d'IA risque de conduire à l'établissement de relations de subordination économico-politiques. Ce problème concerne plus largement l'infrastructure publique numérique et fait écho à la question classique en économie du développement des rapports structurellement inégaux entre pays à haut revenu et pays de la périphérie²¹⁴.

4.3. Le travail en danger

Du point de vue des investisseurs, les objectifs du déploiement de l'IA par les entreprises visent principalement à économiser le travail en le remplaçant par des processus complets, ce qui pourrait affecter des secteurs entiers. C'est ce qu'explique par exemple Sebastian Duesterhoeft du fonds de capital-risque Lightspeed : « Nous avons estimé que l'IA n'était pas un logiciel « d'entreprise » au sens traditionnel du terme, qui vise les

²¹² Cédric Durand, « After AI », *NLR/Sidecar*, 15 janvier 2026.

²¹³ Agnee Ghosh, « Bonanza or Bubble? Where AI Goes From Here », *Bloomberg.com*, 18 mars 2026p.

²¹⁴ Cecilia Rikap, *Teoría de la Dependencia Digital*, Caja Negra., s.l., 2026, 240 p.

budgets informatiques : elle permet de réduire les coûts de main-d'œuvre, et à un certain moment, vous prenez en charge l'ensemble des flux de travail humains »²¹⁵. Les économistes sont plus mesurés²¹⁶, de même que les cabinets de conseil qui accompagnent les entreprises et dont les témoignages convergent sur une idée simple : il est facile d'automatiser un processus une fois ; en revanche, installer l'automatisation dans la durée avec des agents IA en conservant les compétences qui permettent d'évoluer et de s'adapter à des circonstances changeantes, c'est autrement plus complexe.

Du point de vue des processus de travail, la persistance de problèmes de fiabilité, d'une part, et les transformations de l'activité, d'autre part, soulèvent des inquiétudes croissantes.

Une fiabilité incertaine

Les systèmes de GenAI connaissent des défaillances qui ont déjà causé des dommages dans la pratique, qu'il s'agisse de citations juridiques inventées ou de diagnostics médicaux erronés, mais ce n'est qu'un des aspects de problèmes de fiabilité récurrents (Tableau 3). Si les professionnels humains commettent eux aussi des erreurs, les défaillances de l'IA suscitent des inquiétudes particulières en raison de leur nouveauté, de leur ampleur potentielle, de la difficulté à prévoir quand elles se produiront et de la tendance des utilisateurs à se fier sans discernement à des résultats qui se présentent comme certains.

Le rapport international sur la sécurité de l'IA 2026 insiste sur ce point. Des progrès importants ont permis de réduire la fréquence des hallucinations, mais même les meilleurs agents d'IA ne sont pas vraiment fiables : ils continuent de donner des réponses incorrectes sur un ton assuré, et l'écriture de code par la GenAI comporte toujours des bugs. Par exemple, Amazon, qui a récemment licencié 30 000 personnes, en partie en raison de l'automatisation permise par les LLMs, a fait face à plusieurs pannes d'ampleur suite au codage par la GenAI²¹⁷. Autre cas, un cabinet d'avocat états-unien de premier plan a dû reconnaître devant un tribunal fédéral qu'un mémoire important qu'il avait déposé dans une affaire très médiatisée contenait de nombreuses « erreurs » générées par un logiciel d'intelligence artificielle²¹⁸. De plus, les performances en situation réelle sont nettement moins bonnes que dans des contextes formels, tels que des examens : par exemple, dans le domaine de la médecine, les LLMs réussissent assez largement les examens, mais fournissent régulièrement des réponses potentiellement dangereuses à des questions médicales concrètes.

Ce qui rend particulièrement difficile la résolution de ce problème de fiabilité tient au fait qu'on ne les comprend pas bien. Les concepteurs ne savent pas prévoir ces erreurs et donc les prévenir. L'acuité de cette question de la fiabilité est accentuée par le

²¹⁵ George Hammond, « Anthropic's breakout moment: how Claude won business and shook markets », *Financial Times*, 6 févr. 2026p.

²¹⁶ M. Baily et al., « Generative AI at the Crossroads: Light Bulb, Dynamo, or Microscope? », art cit.

²¹⁷ Rafe Rosner-Uddin, Philip Georgiadis et Melissa Heikkilä, « Amazon to axe another 16,000 corporate jobs », *Financial Times*, 28 janv. 2026p. ; Rafe Rosner-Uddin, « Amazon holds engineering meeting following AI-related outages », *Financial Times*, 10 mars 2026p.

²¹⁸ Kaye Wiggins et Sujeet Indap, « Elite law firm Sullivan & Cromwell admits to AI 'hallucinations' », *Financial Times*, 21 avr. 2026p.

développement des agents d’IA capables de prendre des décisions sans intervention humaine et qui sont cependant susceptibles d’avoir des conséquences sur les humains ou, en agissant sur d’autres agents d’IA, de provoquer des effets boule de neige.

Tableau 3 : Problèmes de fiabilité documentés chez les systèmes d’IA générative, les agents d’IA et les systèmes multi-agents ²¹⁹

Problème de fiabilité	Exemples
Hallucination	— Citation de précédents inexistants dans des dossiers juridiques — Citation de politiques de réduction tarifaire inexistantes pour des passagers endeuillés — Fourniture d’informations médicales inexactes et partiales — Fourniture d’informations obsolètes sur des événements
Problème de raisonnement de base	— Absence de calculs mathématiques — Absence de déduction de relations de cause à effet de base
Défaillance hors distribution (défaillance relative à des entrées peu familières ou inhabituelles)	— Mauvaise classification d’images lorsque l’éclairage de fond ou le contexte change
Utilisation erronée des outils	— Violation de la vie privée par l’exposition de l’image privée d’un utilisateur via un agent IA qui l’envoie à un outil tiers — Problème de mémoire de travail à court terme
Défaillance des systèmes multi-agents : mauvaise coordination et conflit	— Échec de gestion des ressources partagées en raison d’un conflit entre les motivations individuelles et les objectifs de bien-être collectif

Risque de déqualification et désinvestissement du travail

L’adoption de l’IA s’est initialement répandue comme une traînée de poudre après la sortie de ChatGPT le 30 novembre 2022. Cependant, son déploiement au sein des entreprises n’a pas été aussi fructueux que prévu. La plupart des projets concrets ne parviennent pas à générer les gains escomptés²²⁰, et des données récentes à grande échelle indiquent que l’utilisation de l’IA n’entraîne pas d’augmentation immédiate de la productivité ²²¹. Au-delà du battage médiatique, l’utilisation intensive de l’IA au travail progresse, mais ne concerne qu’une minorité de la main-d’œuvre²²². En résumé, si une

²¹⁹ Y. Bengio et al., « Rapport international sur la sécurité de l’IA 2026 », art cit, p. 83.
²²⁰ D. Grow, « Unlocking AI’s full potential requires operational excellence », art cit.
²²¹ Anders Humlum et Emilie Vestergaard, *Large language models, small labor market effects*, s.l., National Bureau of Economic Research, 2025.
²²² Fin 2025, 26 % des travailleurs aux États-Unis affirme utiliser chaque semaine l’IA dans leurs fonctions dont seulement 12 % chaque jour Gallup, *Frequent Use of AI in the Workplace Continued to Rise in Q4*, <https://www.gallup.com/workplace/701195/frequent-workplace-continued-rise.aspx>, 25 janvier 2026, (consulté le 28 février 2026). En Europe, en 2025, 15,1 % des sondés déclarent utiliser l’IA pour leur travail. Eurostat, *32.7% of EU people used generative AI tools*

certaine automatisation est en cours, rien n'indique qu'une disruption de l'IA, capable de générer les énormes gains économiques promis, soit imminente. Et il n'est pas certain qu'elle se produise.

Comme l'ont fait valoir avec force Acemoglu et Johnson²²³, il n'existe pas de développement capitaliste axé sur l'efficacité ; les résultats macroéconomiques d'une efficacité technique accrue dépendent du contexte institutionnel. Des technologies puissantes peuvent s'avérer non rentables et ne pas être déployées si la structure du marché empêche les investisseurs d'en tirer profit ; elles peuvent entraîner la paupérisation de la main-d'œuvre si elles conduisent à des licenciements massifs. En ce qui concerne l'IA, l'impact de la technologie sur le travail et l'emploi n'est pas encore clair et dépend des décisions actuellement prises – ou non – en matière de réglementation, de stratégies d'affaires par les firmes ou d'organisation interne par les administrations.

D'un côté, les marchés financiers anticipent la disparition ou la contraction drastique de secteurs entiers, en particulier dans le domaine des logiciels, de la gestion de fortune ou encore de la programmation logistique²²⁴, ce qui, si cela devait se réaliser, aurait un impact massif sur l'emploi. D'un autre côté, les problèmes de fiabilité évoqués plus haut, la difficulté des modèles d'IA à s'engager dans des tâches impliquant une planification longue, à réaliser des tâches pratiques en utilisant la robotique, leur incapacité à résoudre des problèmes nouveaux et/ou nécessitant un raisonnement composite complexe²²⁵ constituent des freins majeurs à l'automation dont on ne sait pas si et, le cas échéant, à quel rythme ils pourront être résolus. Cette incertitude est aggravée par les fragilités économiques du boom de l'IA qui font planer, au-delà des questions techniques, un doute sur la poursuite d'investissements dont la rentabilité n'est pas avérée²²⁶.

Davantage qu'un choc d'emploi massif, l'usage de plus en plus fréquent de l'IA dans un cadre professionnel conduit à une transformation du travail. À cet égard, diverses études pointent des évolutions inquiétantes. D'abord, un problème de motivation : comme la GenIA permet d'obtenir très rapidement et facilement un résultat assez bon, il est très difficile pour les personnes de trouver la motivation nécessaire pour faire l'effort nécessaire pour continuer à travailler afin d'obtenir de très bons résultats, ce qui favorise la médiocrité et alimente les clichés²²⁷. L'usage répété de l'IA contribue aussi rapidement à la perte de compétences, l'accumulation d'une dette cognitive se traduisant par de moindres performances intellectuelles²²⁸. Par ailleurs, la dégradation de la qualité érode la confiance entre les collègues, ce qui fragilise les collectifs de travail

in 2025, <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251216-3>, 16 décembre 2025, (consulté le 28 février 2026). Voir aussi The Economist, « Investors expect AI use to soar. That's not happening », *The Economist*, 26 novembre 2025, 26 nov. 2025p. ; Gallup, *AI Use at Work Rises*, <https://www.gallup.com/workplace/699689/ai-use-at-work-rises.aspx>, 14 décembre 2025, (consulté le 7 janvier 2026).

²²³ Daron Acemoglu et Simon Johnson, *Power and Progress: our thousand-year struggle over technology and prosperity*, New York, PublicAffairs, 2024, 546 p.

²²⁴ Hannah Erin Lang, « AI Gave Investors a Glimpse of the Future This Month. And They Sold Their Stocks. », *Wall Street Journal*, 27 févr. 2026p.

²²⁵ Y. Bengio et al., « Rapport international sur la sécurité de l'IA 2026 », art cit, p. 30.

²²⁶ C. Sam et al., « A Guide to the Circular Deals Underpinning the AI Boom », art cit ; B. Elder, « How high are OpenAI's compute costs? », art cit.

²²⁷ Yvonne Jie Chen et al., « Better Technology, Worse Motivation: GenAI's Mediocrity Trap », *Available at SSRN 5208163*, 2025.

²²⁸ Nataliya Kosmyna et al., « Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task », *arXiv preprint arXiv:2506.08872*, 2025, vol. 4.

et pourrait détériorer le résultat de la coopération²²⁹. Enfin, les capacités d'esprit critique s'érodent, mais surtout se transforment, de sorte que l'effort de réflexion critique se déplace de l'exécution des tâches elles-mêmes à des tâches de supervision consistant à intégrer et contrôler la qualité des résultats de l'IA.

Prises ensemble, ces études suggèrent que le danger le plus immédiat semble être une épidémie de démoralisation de la main-d'œuvre. Dans ce cas, nous pourrions assister à une courbe en J inversée, car les gains de productivité à court terme seraient rapidement éclipsés par la détérioration de la qualité du travail (Figure 11). Une étude récente suggère justement que l'intensification du travail associé à l'IA génère une dynamique régressive de ce type :

« Une fois l'enthousiasme suscité par l'expérimentation retombé, les employés peuvent constater que leur charge de travail a augmenté discrètement et se sentir débordés par toutes les tâches qui leur incombent soudainement. Cette augmentation progressive de la charge de travail peut à son tour entraîner une fatigue cognitive, un épuisement professionnel et une capacité de décision amoindrie. La hausse de productivité observée au début peut alors laisser place à une baisse de la qualité du travail, à une augmentation du turnover et à d'autres problèmes »²³⁰.

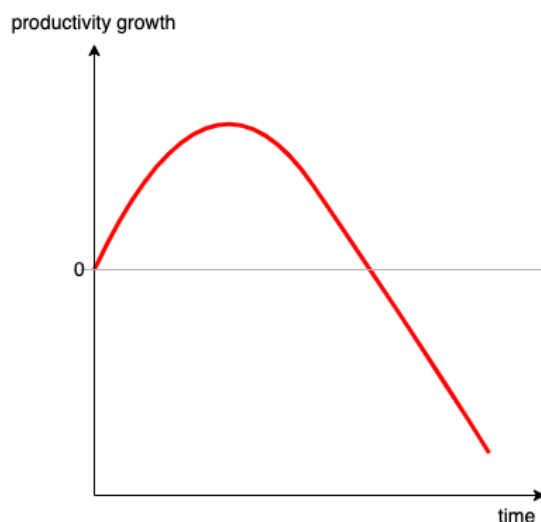
Le défi pour les organisations est donc de trouver des solutions pour préserver un haut niveau de compétences et de technicité, alors même que la possibilité d'automatiser certains processus les dévalorise. Dans ce cadre, une réflexion sur les métiers et les cadres juridiques et socioéconomiques permettant de préserver les savoir-faire est essentielle, notamment pour conserver la robustesse des processus administratifs qui fondent la confiance des citoyens dans l'action publique. Plus largement, pour parer aux dangers que font peser l'épuisement et l'isolement du travail compulsif en tête-à-tête avec l'IA, l'organisation du travail devra faire en sorte de créer les conditions pour que les pauses imprévues, les discussions et les moments de réflexion aient lieu, car ces moments participent à la fois au bien-être des travailleurs et à la fiabilité du travail lui-même²³¹.

²²⁹ Kate Niederhoffer et al., « AI-Generated “Workstop” Is Destroying Productivity », *Harvard Business Review*, 22 septembre 2025, 22 sept. 2025p.

²³⁰ Aruna Ranganathan et Xingqi Maggie Ye, « AI Doesn't Reduce Work—It Intensifies It », *Harvard Business Review*, 9 février 2026, 9 févr. 2026p.

²³¹ Sarah O'Connor et John Burn-Murdoch, « Is AI making work more intense? », *Financial Times*, 19 févr. 2026p.

Figure 11 : La possibilité d'une courbe en J inversé de la productivité du travail avec le déploiement à grande échelle de l'IA dans les organisations



Une étude portant sur l'adoption de l'IA dans des administrations publiques suisses²³² montre que les obstacles organisationnels sont les plus importants dans l'implémentation efficace de l'IA dans le processus de travail. On retrouve ici la question de l'érosion du travailleur collectif et du risque de démobilisation du travail qui pèsent sur l'« acceptabilité » de l'IA par les employés et les cadres. Mais il s'agit aussi d'une question de gestion du processus d'implémentation, comme noté par le cabinet de consulting Deloitte qui souligne que « si les organisations ne disposent pas d'une stratégie cohérente en matière d'IA, une lassitude vis-à-vis des projets pilotes risque de se manifester »²³³.

Ce problème de la fatigue de l'IA est une question centrale. Avec l'IA, les outils disponibles se multiplient ; or, apprendre à utiliser de nouveaux outils, c'est beaucoup de travail. Comment peut-on tout apprendre ? Si les personnes se sentent submergées par le rythme, elles vont se désintéresser. Et si ce phénomène prend de l'ampleur, cela pourrait paralyser les organisations dans leur ensemble et nuire à leur fonctionnement, l'espoir d'accroissement de la productivité se traduisant alors au contraire par une perte d'efficacité.

4.4. Une trajectoire matérielle insoutenable

Le déploiement à grande échelle de l'IA repose sur le développement et le maintien d'infrastructures critiques, en particulier les centres de données. Leur fonctionnement nécessite d'importantes ressources et entraîne des conséquences écologiques et climatiques non négligeables. Même si le but de la recherche en IA est d'optimiser les

²³² Oliver Neumann, Katharina Guirguis et Reto Steiner, « Exploring artificial intelligence adoption in public organizations: a comparative case study », *Public Management Review*, 2 janvier 2024, vol. 26, n° 1, p. 114-141.

²³³ Deloitte, *The State of AI in the Enterprise - 2026 AI report* | Deloitte US, s.l., 2026, p. 9.

modèles d'IA sous-jacents de manière à réduire les besoins de calcul et donc d'énergie, sans encadrement réglementaire, l'effet attendu est un effet rebond, c'est-à-dire une augmentation de l'efficacité par unité, mais un impact croissant du fait de l'augmentation des usages.

Le développement des centres de données, pour entraîner les modèles d'IA et répondre aux requêtes, contribue à accroître la demande globale d'énergie. Pour l'Agence Internationale de l'Energie, la consommation d'électricité des centres de données en général devrait doubler entre 2024 et 2030, majoritairement en raison de la consommation liée à l'IA. Dans l'ensemble, la part des centres de données dans la consommation d'électricité devrait passer de 1,5 % à 3 % sur la même période²³⁴. Au sein de cette trajectoire générale, il existe des variations notables. Aux États-Unis, la part pourrait s'élever jusqu'à 12 % dès 2028 ; en Irlande, elle représente déjà 20 % de la consommation du pays, tandis qu'en Suisse, elle représentait 6 % de la consommation en 2024 et pourrait atteindre 15 % en 2035²³⁵. L'électricité pour les centres de données doit être fournie en continu ; même si une partie devrait être couverte par le déploiement des renouvelables, elle repose aussi sur des énergies fossiles et, aux États-Unis, elle est nettement plus intensive en carbone que l'électricité en général²³⁶. Ces soubassements matériels constituent des limites au développement de l'IA, comme le reconnaissent les entreprises du secteur. Par exemple, Google explore la possibilité de déployer un « système d'infrastructure d'IA spatiale [...qui] offrirait un immense potentiel de scalabilité tout en minimisant l'impact sur les ressources terrestres »²³⁷. Du point de vue du coût comme de la robustesse, la mise en orbite de ce centre de données relève pour l'instant de la science-fiction²³⁸ ; en revanche, ces projets attestent de l'acuité du problème écologique bien terrestre du fantasme d'une société tout IA.

Comme la demande se concentre dans quelques clusters, les effets locaux peuvent être importants en termes de tensions sur les réseaux et de hausse des prix. En Suisse, la production d'électricité dans le canton de Zurich atteint les limites de ses capacités sous la pression du hub de centres de données hébergés tandis que les terrains disponibles viennent à manquer²³⁹. Cette augmentation substantielle de la consommation d'énergie constitue un obstacle supplémentaire à la réalisation des objectifs de réduction des émissions de gaz à effet de serre²⁴⁰.

L'impact en termes d'émissions de carbone associé à l'IA tout au long du cycle de vie et des usages de l'eau reste flou en raison de l'absence de régulation et du manque de transparence des entreprises, mais semble prendre une tendance insoutenable²⁴¹. En

²³⁴ IEA, *Understanding the energy-AI nexus – Energy and AI – Analysis*, <https://www.iea.org/reports/energy-and-ai/understanding-the-energy-ai-nexus>, 2025, (consulté le 1 mars 2026).

²³⁵ Tamara Keller Albisser Julian Schmidli and Pascal, *Silent power guzzlers: Switzerland's booming data centres*, <https://www.swissinfo.ch/eng/swiss-ai/silent-power-guzzlers-switzerlands-booming-data-centres/89724159>, 25 juillet 2025, (consulté le 1 mars 2026).

²³⁶ Gianluca Guidi et al., « Environmental burden of United States data centers in the artificial intelligence era », *arXiv preprint arXiv:2411.09786*, 2024.

²³⁷ Travis Beals, « Exploring a space-based, scalable AI infrastructure system design », *research.google*, 4 novembre 2025, <https://research.google/blog/exploring-a-space-based-scalable-ai-infrastructure-system-design/> (consulté le 04.03.2026).

²³⁸ Loren Grush, « Why AI Data Centers in Space Aren't Totally Science Fiction », *Bloomberg.com*, 13 janv. 2026p.

²³⁹ T.K. Albisser Julian Schmidli and Pascal, « Silent power guzzlers », art cit.

²⁴⁰ Sophia Chen, « Data centres will use twice as much energy by 2030 — driven by AI », *Nature*, 10 avril 2025.

²⁴¹ Alex de Vries-Gao, « The carbon and water footprints of data centers and what this could mean for artificial intelligence », *Patterns*, 17 décembre 2025, p. 101430.

2025, une étude de référence estime que les centres de données ont émis entre 32,6 et 79,7 millions de tonnes d'équivalent CO₂. La même année, leur empreinte hydrique est évaluée entre 312,5 et 764,6 milliards de litres, comparable à la consommation globale de bouteilles d'eau (446 milliards de litres).²⁴² Le développement de l'IA repose également sur l'utilisation de matériaux critiques, en particulier des minerais et métaux. Bien qu'essentiels pour estimer la durabilité de la technologie, ceux-ci ne sont généralement pas comptabilisés dans le calcul de l'empreinte écologique globale des infrastructures numériques²⁴³.

Dans ce sens, une étude systémique sur l'impact environnemental du numérique en Suisse conclut que la trajectoire est incompatible avec les objectifs de soutenabilité à long terme, notamment en termes d'extraction de minerais. Le rapport souligne aussi que si l'impact des utilisateurs finaux est majoritaire en 2024, la tendance devrait s'inverser d'ici à 2035 avec 56 % de l'impact causé par les centres de données, en particulier sous la pression de l'IA²⁴⁴. Par ailleurs, ceux-ci ont contribué à 20 % de l'empreinte totale des TIC sur le changement climatique. Ils ont notamment des répercussions importantes en termes d'eutrophisation et d'accroissement de l'écotoxicité de l'eau douce, ainsi que dans l'utilisation insoutenable de ressources fossiles. Le développement de l'IA jouera donc un rôle majeur dans la manière dont le pays respectera ou non les limites planétaires dans les prochaines décennies²⁴⁵.

En résumé, la trajectoire actuelle du déploiement de l'IA à grande échelle impliquera, en Suisse comme ailleurs, des impacts et dépendances écologiques préoccupants. Or, l'estimation de l'impact matériel de cette technologie demeure insuffisante, notamment du fait du manque d'informations présentées par les entreprises du secteur²⁴⁶. En raison de leur importance, leur mesure la plus précise possible est une condition indispensable à la pleine compréhension de la place et des besoins suisses dans cet écosystème technologique. Du fait du postulat Fivaz 24.4649 accepté le 12 février 2025, le Conseil fédéral s'engage d'ores et déjà à présenter un rapport chiffré sur l'impact énergétique actuel et futur de l'IA²⁴⁷. Cet effort nécessaire devrait toutefois dépasser la seule dimension énergétique, en s'accompagnant d'une étude des impacts et des dépendances écologiques de ces technologies.

Conclusion

Le déploiement des systèmes d'IA est déjà révolutionnaire mais soulève simultanément des interrogations sérieuses. En dépit de capacités technologique importantes, la situation de dépendance de la Suisse à tous les niveaux du stack de l'IA (modèle, capacités de calcul, données...) est patente. Elle pose des risques à la fois multiples et sévères, notamment sur le plan de la sécurité, des atteintes à la personnalité et aux droits

²⁴² *Ibid.*

²⁴³ Berthelot, Adrien, et al. "Estimating the environmental impact of Generative-AI services using an LCA-based methodology." *Procedia CIRP* 122 (2024): 707-712.

²⁴⁴ Louis Guegant, Louise Aubet et Lea Bitard, *Les impacts environnementaux du numérique en Suisse*, s.l., 2025.

²⁴⁵ Louis Guégan, Louise Aubet et Léa Bitard (Resilio), « Les impacts environnementaux du numérique en Suisse », *Livre blanc E4S & Resilio*, septembre 2025, <https://sustainableit.ch/downloads/study/fr/whitepaper.pdf>, (consulté le 24.02.2026).

²⁴⁶ A. de Vries-Gao, « The carbon and water footprints of data centers and what this could mean for artificial intelligence », art cit.

²⁴⁷ Parlement suisse, « Stratégie pour une intelligence artificielle souveraine en Suisse », *parlament.ch*, 12 décembre 2024, <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaefft?AffairId=20244679>, (consulté le 02.03.2026).

politiques, en termes d'accroissement des coûts économiques et d'atteinte à l'intégrité de l'action publique.

Au-delà de ces menaces de subordination à des firmes hors de contrôle du législateur, s'ajoutent des problèmes qui concernent les effets de la technologie elle-même sur les processus de travail : fiabilité incertaine, déqualification, détérioration de la coopération, désinvestissements des personnes... Ces phénomènes se conjuguent et peuvent contrecarrer les gains attendus de l'automatisation, laissant le bilan d'ensemble sur le plan de l'efficacité incertain tandis que le risque d'une dégradation des rapports humains est aisément identifiable.

5. Préserver les capacités de pilotage et renforcer l'autonomie stratégique

Nos recommandations pour l'action publique au niveau des cantons et leur positionnement au niveau fédéral s'articulent autour de trois axes.

5.1. L'administration publique doit choisir le rythme et l'étendue du déploiement de l'IA en fonction de ses objectifs propres

- L'engouement pour l'IA véhicule un optimisme technologique qui va de pair avec une accélération et une multiplication de l'offre d'outils et de plateformes. Dans un tel contexte, tenter de se situer à la frontière de l'innovation fait courir un risque de désorganisation de l'action publique, source à la fois d'inefficacité potentielle, d'insatisfaction des employés publics et des usagers et de failles de sécurité.
- Les études empiriques ne démontrent pas, pour l'instant, de gains d'efficacité significatifs au niveau des organisations dans leur ensemble associés à l'IA et font apparaître des effets pervers importants. Des diminutions de coûts peuvent parfois être mises en évidence à une échelle micro, mais elles ne se retrouvent pour l'instant pas à une échelle plus grande, pour des raisons qui ne sont pas encore bien comprises (dysfonctionnements, pertes de la qualité de la coopération...). Dès lors, *il est urgent de ne pas se précipiter dans le déploiement de ces outils au niveau des processus administratifs dans leur ensemble.*

Recommandation 1: Définir les objectifs politiques et administratifs en amont et conserver leur caractère prioritaire par rapport à une logique de transformation tirée par la technologie. Cette réflexion permettra de choisir soigneusement les types de modèles d'IA, d'hébergement et d'usages qui permettent de garantir le strict respect du cadre légal, réglementaire et déontologique

**

- En revanche, la rapidité de la diffusion d'usages fantôme de l'IA par les employé·e·s publics témoigne d'une efficacité locale pour un certain nombre de processus, d'une insatisfaction quant aux tâches à effectuer et comporte des risques majeurs pour l'intégrité et la fiabilité de l'action publique.
- Dès lors, il importe d'engager plus avant une mutation de l'organisation administrative qui repose, certes, sur la formation aux enjeux numériques (avec une priorité sur la littératie des données²⁴⁸), mais aussi et surtout sur une réflexion

²⁴⁸ La **littératie des données** comprend les compétences permettant de collecter, de gérer, d'évaluer et d'utiliser les données de manière critique et réfléchie dans leur contexte respectif, ceci en respectant les principes d'éthique des données et de la protection

au niveau des métiers, c'est-à-dire du type de complexe tâches/compétences qui ne correspond pas nécessairement à la logique de cloisonnement des services.

- La question essentielle que pose l'IA est celle des frontières souhaitables de l'automatisation et de la préservation des compétences pour garantir une maîtrise humaine des processus.
- La réflexion métier doit donc porter à la fois sur le découpage (automatisation ou non) et sur les conditions de la préservation des compétences. Cette question concerne à la fois les administrations, les employé·e·s publics (qui doivent donc être associés), et, au-delà, l'ensemble du tissu socio-économique.

Recommandation 2: Mettre en œuvre des programmes continus de formation et de développement des compétences en matière de littératie des données et d'humanités numériques et renforcer la formation initiale pluridisciplinaire dans le domaine au niveau de l'enseignement secondaire et au sein des hautes écoles de manière à diffuser une culture numérique critique au sein de l'administration et dans la société.

Recommandation 3: Sur la base d'une concertation avec les employé·e·s publics de l'administration, consolider des normes professionnelles concernant les usages de l'IA et des stratégies de préservation des compétences par métier.

**

- Étant donné la criticité des enjeux à la fois sur le plan des RH, sur le plan politique et sur le plan de la sécurité, des formes d'expérimentation doivent précéder toute forme de généralisation. A ce titre, les échanges intercantonaux, voire avec des administrations d'autres pays, doivent permettre de bénéficier des retours d'expérience et de contrebalancer la pression marketing des acteurs de l'industrie. Les cantons pourraient demander que l'Administration numérique suisse (ANS) non seulement recense les expériences et favorise la fertilisation croisée entre les différentes entités administratives, mais, au-delà, pilote les projets stratégiques pour lesquels des économies d'échelle sont attendues et les enjeux de standardisation sont importants.

Recommandation 4 : Encourager les échanges d'expériences sur le déploiement de systèmes d'IA et la fertilisation croisée aux différents niveaux.

des données. Une utilisation éthique des données implique également de tenir compte des aspects économiques, sociaux et écologiques liés à celle-ci. Prendre conscience de la trace numérique que l'on laisse en utilisant des services informatiques est un élément tout aussi essentiel de la littératie des données. Académies suisses des sciences, « Charte suisse de littératie des données », 15 mai 2024.

Recommandation 5 : Mutualisation par le Département des institutions et du numérique (DIN), au niveau cantonal, et par la Conférence latine des directeurs·trices du numérique (CLDN), au niveau des cantons latins, par l'ANS, au niveau fédéral, des retours d'expérience. Pilotage des projets stratégiques par l'ANS.

5.2. Faire de l'action publique en matière d'IA un levier de la souveraineté numérique

- L'action publique en matière d'IA comprend une multitude de leviers (formation, réglementation, commande publique, investissement...) mais elle ne s'insère dans une logique de souveraineté numérique que si elle s'articule à un ensemble de mesures visant à garantir une autonomie stratégique sur l'ensemble du stack numérique.
- Pour les administrations publiques, construire un stack numérique compatible avec la préservation de la souveraineté et opérer un déploiement IA respectueux de l'intégrité de l'action publique exige les principales mesures suivantes :

Recommandation 6 : Privilégier au sein des administrations le déploiement d'approches d'IA open source - sous réserve des écueils juridiques relatifs à l'Open Source exposés précédemment - et frugales. Favoriser le développement de solutions "internes" publiques pouvant être commercialisées à "l'externe",

Recommandation 7 : Consolider et accélérer le passage à un cloud souverain privé pour l'ensemble des administrations en mutualisant les infrastructures et les outils au niveau intercantonal et/ou fédéral.

Recommandation 8 : Transitionner vers des solutions logicielles et des outils open source pour échapper aux effets de *lock-in* dans des plateformes propriétaires, en planifiant en particulier la sortie des plateformes propriétaires intégrées.

Recommandation 9 : Adopter des pratiques, des règles et/ou des contrats en matière de données conservatrices de manière à prévenir les comportements prédateurs des acteurs dominants et conditionner les contrats publics à des accords d'accessibilité des données pour augmenter la quantité et la qualité des statistiques directement disponibles pour l'action publique. Favoriser l'accès aux données publiques et privées pour le développement de modèles souverains

**

- Favoriser par l'action cantonale le développement d'un écosystème IA performant compatible avec les valeurs de la Confédération et minimisant les vulnérabilités économiques et militaires.

Recommandation 10 : Par une commande publique exigeante, permettre à des acteurs locaux de monter en compétences aux différents niveaux du stack (solutions, outils d'IA, cloud, logiciels...). Pour cela, procéder à une étude plus poussée des règles en matière de marché public et considérer les flexibilités que celles-ci offrent.

Recommandation 11 : Utiliser la concertation au sein de l'administration sur les métiers (cf. recommandation 3) pour faire émerger de nouvelles normes de pratiques professionnelles dans l'économie de manière à préserver les compétences et la productivité à long terme du tissu socio-économique local.

Recommandation 12 : Conditionner les soutiens publics importants aux entreprises (y compris les start-up) à des mesures de précaution relativement à leur dépendance aux fournisseurs d'un seul pays pour leur infrastructure cloud et encourager le développement de la cyberassurance.

Recommandation 13 : Prendre des participations publiques et/ou attribuer au canton une *Golden Share* dans les entreprises numériques et actives dans le domaine de l'IA locales à caractère stratégique, de manière à doter l'administration d'un pouvoir de veto sur les décisions concernant les intérêts vitaux du canton et prévoir la possibilité de limiter les investissements étrangers dans des entreprises considérées comme infrastructures critiques

Recommandation 14 : Soutenir le rôle de Genève comme forum international en matière de régulation de l'IA et de développement coopératif de solutions technologiques ouvertes, sobres et responsables.

Recommandation 15 : Soutien à la recherche pluridisciplinaire sur les transformations numériques et leur impact économique, social, politique et écologique.

Recommandation 16 : Mise en place d'un Conseil Scientifique (pluridisciplinaire) du Numérique (CSN) auprès du DIN et/ou de la Conférence latine des directeurs·trices du numérique (CLDN) ou, dans le meilleur des cas, au niveau fédéral pour appuyer la politique des autorités en la matière.

5.3. Protéger les personnes, préserver la nature

- Conformément à la volonté populaire de protection de l'intégrité numérique, les autorités cantonales doivent adopter une politique proactive en matière de systèmes d'IA.
- Cela concerne d'abord les processus administratifs et la gestion des services publics pour lesquels un niveau de garantie maximal doit être apporté afin de conserver la confiance de la population dans l'action publique.
- Cela concerne ensuite les normes dans ce domaine adoptées par l'ensemble des acteurs opérant dans le canton.

Recommandation 17 : vérifier que le droit cantonal assure suffisamment le respect des droits fondamentaux lors de l'utilisation et du développement de modèles d'IA, le cas échéant, adopter de nouvelles règles, en s'inspirant du projet de loi fédérale « AP-IA » et des points d'amélioration identifiés ci-dessus.

Recommandation 18 : Créer un registre des systèmes de prise de décision basés sur l'IA et produire un rapport bisannuel d'auto-évaluation des risques par l'administration qui pourrait être discuté au CSN (cf. recommandation 16) avant sa publication.

Recommandation 19 : Mettre en place des procédures de recours effectives pour les personnes concernées, de manière à pouvoir indemniser les victimes et sanctionner les entités responsables, par exemple via des voies de droit extraordinaire sous la forme d'une plainte ou d'une dénonciation et/ou des mesures administratives et des sanctions pénales sur le même modèle que la LPD.

★★

- La croissance exponentielle des systèmes d'IA est insoutenable sur le plan écologique en raison de la demande d'énergie qu'elle implique, mais également des besoins en métaux rares, en terrain et en eau.
- Le canton doit donc établir des procédures permettant de mesurer et d'anticiper les pressions environnementales et de définir des lignes directrices concernant l'empreinte écologique acceptable de ces systèmes.

Recommandation 20 : Rendre publiques les données concernant la consommation électrique et l'impact écologique liées au déploiement de l'IA dans l'administration publique et le secteur privé. Bien sûr, cette question doit être pensée en lien avec la recherche de la sobriété écologique du numérique dans son ensemble.

Recommandation 21 : Fixer des objectifs pluriannuels au niveau de l'administration et des grands acteurs privés en termes de réduction de l'empreinte écologique de l'IA.

Recommandation 22 : Soutenir la recherche et le développement de technologies plus parcimonieuses en ressources matérielles et

énergétiques, notamment en favorisant le développement de modèles d'IA frugaux et spécialisés et des pratiques durables de collecte et de stockage des données et d'entraînement des modèles d'IA.

Tableau 4. Synthèse des recommandations

5.1 L'ADMINISTRATION DOIT CHOISIR LE RYTHME ET L'ÉTENDUE DU DÉPLOIEMENT DE L'IA EN FONCTION DE SES OBJECTIFS	
Limiter les risques pour l'administration	R1 : Définir les objectifs politiques et administratifs en amont et conserver leur caractère prioritaire par rapport à une logique de transformation tirée par la technologie.
Définir frontières de l'automatisation et préserver les compétences.	R2 : Mettre en œuvre des programmes continus de formation en matière de littératie des données et renforcer la formation initiale pluridisciplinaire dans les hautes écoles et le secondaire. R3 : Consolider les normes professionnelles concernant les usages de l'IA sur la base d'une concertation avec les employé·e·s.
Favoriser la fertilisation croisée	R4 : Encourager les échanges d'expériences sur le déploiement de systèmes IA aux niveau intercantonal. R5 : Mutualiser, par le DIN, au niveau cantonal, et par l'ANS, au niveau fédéral, les retours d'expérience.
5.2 FAIRE DE L'ACTION PUBLIQUE EN MATIÈRE D'IA UN LEVIER DE LA SOUVERAINETÉ NUMÉRIQUE	
Garantir une autonomie stratégique sur l'ensemble du stack	R6 : Privilégier au sein des administrations le déploiement de modèles d'IA open source et frugaux. R7 : Consolider et accélérer le passage à un cloud souverain privé pour l'ensemble des administrations. R8 : Transitionner vers des solutions logicielles ouvertes et des outils open source pour échapper aux effets de <i>lock-in</i> dans des systèmes propriétaires. R9 : Adopter des pratiques en matière de données conservatrices et conditionner les contrats publics à des accords d'accessibilité de données pour renforcer les capacités statistiques des administrations.
Favoriser le développement d'un écosystème IA performant et compatible avec les valeurs de la Confédération	R10 : Par une commande publique exigeante permettre à des acteurs locaux de monter en compétences et de devenir compétitifs aux différents niveaux du stack. R11 : Utiliser la concertation pour préserver les compétences et la productivité à long terme du tissu socio-économique local. R12 : Conditionner les soutiens publics importants aux entreprises à des mesures de précaution relativement à leur diversification de leur fournisseur cloud. R13 : Attribuer au canton une <i>Golden Share</i> dans les entreprises numériques locales à caractère stratégique. R14 : Soutenir le rôle de Genève comme forum international en matière de régulation de l'IA et de développement coopératif de solutions ouvertes, sobres et responsables. R15 : Soutenir la recherche pluridisciplinaire sur les transformations numériques et leur impact économique, social, politique et écologique. R16 : Mettre en place un Conseil Scientifique (pluridisciplinaire) du Numérique (CSN) auprès du DIN pour appuyer la politique du Canton en la matière

5.3 PROTÉGER LES PERSONNES, PRÉSERVER LA NATURE

Adopter une politique proactive en matière d'IA par la gestion des processus administratifs et la mise en place de normes.

R17 : Vérifier que le droit cantonal assure suffisamment le respect des droits fondamentaux lors de l'utilisation et du développement de modèles d'IA et, le cas échéant, adopter de nouvelles règles.

R18 : Créer un registre cantonal des systèmes de prise de décision basés sur l'IA et produire d'un rapport d'auto-évaluation des risques.

R19 : Mettre en place des procédures simplifiées de recours et de sanctions.

Définir des lignes directrices pour l'empreinte écologique des systèmes IA.

R20 : Rendre publiques les données concernant la consommation électrique et l'impact écologique liées au déploiement de l'IA dans l'administration publique et le secteur privé.

R21 : Fixer des objectifs pluriannuels au niveau de l'administration et des grands acteurs privés en termes de réduction de l'empreinte écologique de l'IA.

R22 : Soutenir la recherche et le développement de technologies plus parcimonieuses en ressources matérielles et énergétiques.

ANNEXES

A. Aspects saillants de la régulation aux États-Unis, dans l'Union Européenne et en Chine

On observe actuellement une forte divergence à l'échelle internationale en matière de régulation de l'IA.

Les États-Unis, entre dérégulation fédérale et réglementation locale

Aux États-Unis, depuis l'installation d'une nouvelle administration en janvier 2025, la réglementation sur l'IA a connu des changements importants avec un virage radical vers la dérégulation au niveau fédéral que les États ont tenté de contrecarrer par une activité législative accrue.

L'administration Trump 2 inscrit le développement de l'IA dans le contexte d'une rivalité systémique avec la Chine. L'état d'esprit est celui d'un alignement total sur les demandes des entreprises les plus puissantes du secteur de la Tech auxquelles il s'agit de laisser l'initiative, comme l'exprime le vice-président J.D. Vance : « une réglementation excessive du secteur de l'IA pourrait tuer une industrie en pleine transformation alors qu'elle est sur le point de décoller ; nous mettrons tout en œuvre pour encourager les politiques favorables à la croissance de l'IA. »²⁴⁹. Une des premières et plus significatives décisions en la matière a été la révocation par le Président Trump d'un décret de Joe Biden relatif à la sécurité des systèmes d'IA et qui obligeait « les développeurs de systèmes d'IA qui présentent des risques pour la sécurité nationale, l'économie, la santé ou la sécurité publique des États-Unis à partager les résultats des tests de sécurité avec le gouvernement américain »²⁵⁰. En somme, les autorités fédérales gardaient un droit de regard sur les évolutions à la frontière de l'IA. Ce n'est plus le cas.

En parallèle, l'exécutif a soutenu les efforts des Big Tech en faveur d'une loi établissant un moratoire de 10 ans sur toute régulation au niveau des États de l'IA. Cette tentative, n'a pas abouti, mais signale une orientation dépourvue d'ambiguïté²⁵¹. Celle-ci a été confirmée dans un décret présidentiel de décembre 2025 qui établit une task force chargée de contester les dispositions prises au niveau des états²⁵² qui contreviendraient à la politique de l'exécutif visant à « maintenir et renforcer la domination mondiale des États-Unis dans le domaine de l'IA grâce à un cadre politique national peu contraignant en matière d'IA »²⁵³.

²⁴⁹ Steven Levy, « How the Loudest Voices in AI Went From 'Regulate Us' to 'Unleash Us' », *Wired*, 30 mai 2025, 30 mai 2025p.

²⁵⁰ David Shepardson, « Trump revokes Biden executive order on addressing AI risks », *Reuters*, 21 janv. 2025p. ; Jeff Mason et al., « Biden administration aims to cut AI risks with executive order », *Reuters*, 30 oct. 2023p.

²⁵¹ Alex Rogers et Stephen Morris, « Big Tech pushes for 10-year ban on US states regulating AI », *Financial Times*, 18 juin 2025p.

²⁵² Dylan Champagne, *President Trump Targets State AI Regulations*, <https://www.theregreview.org/2026/02/26/champagne-president-trump-targets-state-based-ai-regulations/>, 26 février 2026, (consulté le 4 mars 2026).

²⁵³ US Executive Order, *Ensuring a National Policy Framework for Artificial Intelligence*, <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>, 11 décembre 2025, (consulté le 4 mars 2026).

La volonté dérégulatrice de la présidence US contraste avec une activité législative intense au niveau local²⁵⁴. L'état du Colorado a ainsi adopté une loi visant à prévenir les risques de biais algorithmiques, qui « exige qu'un développeur d'un système d'intelligence artificielle à haut risque (système à haut risque) fasse preuve d'une diligence raisonnable pour protéger les consommateurs contre tout risque connu ou raisonnablement prévisible de discrimination algorithmique »²⁵⁵. En Californie, la loi SB-53 entrée en vigueur au mois de septembre 2025 est emblématique des exigences de transparence et de responsabilité que le législateur peut avoir vis-à-vis des entreprises qui développent les modèles d'IA, avec une insistance sur les questions de sécurité (Tableau 5).

Tableau 5: Analyse de la loi californienne SB-53 par le cabinet BCLP ²⁵⁶

« Signée le 29 septembre 2025, la loi SB 53, intitulée « Transparency in Frontier Artificial Intelligence Act » (loi sur la transparence dans le domaine de l'intelligence artificielle de pointe), est une réglementation radicale qui oblige les grands développeurs de pointe à divulguer leur cadre d'évaluation des risques au public et à renforcer leur responsabilité en matière de signalement des incidents de sécurité. La composante « transparence » est particulièrement notable : la TFAIA exige des développeurs de pointe qu'ils « rédigent, mettent en œuvre et publient de manière claire et visible » un cadre d'évaluation des risques sur leur site web. Ce cadre doit décrire comment le développeur intègre les normes nationales/internationales et les meilleures pratiques du secteur. Le rapport public doit également inclure un mécanisme de communication avec le développeur, les résultats soumis par le modèle, les utilisations prévues du modèle et toute restriction ou condition d'utilisation du modèle. Il exige en outre que les modèles de pointe signalent les incidents de sécurité critiques, notamment « l'accès non autorisé », la perte de contrôle du modèle entraînant des blessures corporelles ou la mort, ou les dommages résultant de la matérialisation d'un risque catastrophique. Un risque catastrophique est un risque prévisible qui entraîne 1) la mort ou des blessures corporelles de 50 personnes ou plus ou une perte de plus d'un milliard de dollars résultant : 1) d'une assistance IA de niveau expert dans la création d'armes, 2) d'une cyberattaque ou d'un comportement qui serait considéré comme un crime s'il était commis par une personne, y compris le meurtre, le vol, l'agression ou l'extorsion, ou 3) d'un échappement au contrôle du développeur ou de l'utilisateur. La TFAIA offre une protection élargie aux lanceurs d'alerte qui signalent des violations de la loi. La loi ne prévoit aucun droit d'action privé. Le procureur général peut intenter une action civile en cas de non-respect de la loi. La sanction ne peut dépasser 1 million de dollars par violation. »

En Europe, un effort de réglementation en suspens

L'Union Européenne (UE) a une approche basée sur les risques et les droits fondamentaux, matérialisée dans une régulation horizontale qui prévoit des obligations strictes pour les IA²⁵⁷. D'abord, le règlement de l'UE sur l'IA (AI Act) ainsi que la directive

²⁵⁴ Le cabinet d'avocat Bryan Cave Leighton Paisner LLP propose un suivi exhaustif de l'activité législatives sur le sujet dans les différents états américains voir BCLP, *US state-by-state AI legislation snapshot*, <https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html>, 2026, (consulté le 4 mars 2026).

²⁵⁵ Colorado General Assembly, *SB24-205 Consumer Protections for Artificial Intelligence* | Colorado General Assembly, <https://leg.colorado.gov/bills/sb24-205>, 17 mai 2024, (consulté le 4 mars 2026).

²⁵⁶ BCLP, *California - SB53*, <https://infographics.bclplaw.marketing/>, 2025, (consulté le 4 mars 2026).

²⁵⁷ Joanna Bryson, « Human-Centred Control of AI Is Both Possible and Necessary » dans *The Role of Transatlantic Cooperation in AI Human Oversight in Defence*, Amsterdam, IOS Press, 2026, p.

relative à la responsabilité du fait des produits défectueux, deux textes adoptés en 2024 – stipulent clairement que les logiciels sont des produits et, à ce titre, soumis aux mêmes considérations en matière de responsabilité que tout autre produit. Ce point est important car il engage la responsabilité des entreprises qui déploient des dispositifs d'IA quant aux préjudices qu'ils pourraient causer. Ensuite, l'IA Act procède à un certain nombre d'interdictions, notamment en ce qui concerne la surveillance de masse par le biais de scans biométriques ou de dispositifs de type crédit social. Enfin, la directive définit le type d'informations et les procédures d'enregistrement nécessaires pour les systèmes d'IA susceptibles d'avoir un impact considérable sur la vie des êtres humains, par exemple en termes de soins médicaux, d'accès aux écoles, de recrutement de prestations sociales, de prêts bancaires...

Ce cadre juridique ambitionne donc de garantir une transparence et une responsabilité suffisantes dans les produits numériques associés à l'intelligence artificielle de manière à ce que des responsabilités puissent être engagées en cas de dysfonctionnement et à poser un certain nombre de garde-fous pour protéger les droits humains fondamentaux. Dans les faits, cependant, l'AI Act ne fournit pas les protections promises. En termes de transparence, les obligations concernant les méthodes d'entraînement des modèles ne sont dans l'ensemble pas respectées, une exception notable étant le LLM suisse Apertus²⁵⁸. Sous la pression d'un lobbying intense des Big Tech, de l'administration étasunienne, mais également de grandes firmes et de start-ups européennes, la Commission a introduit des délais supplémentaires et des restrictions aux exigences et aux pénalités concernant les activités identifiées comme à « haut risque »²⁵⁹. En somme, la détermination des autorités européennes à mettre en œuvre cette réglementation ambitieuse est aujourd'hui incertaine, d'autant que la Commission a déjà reculé sur la question de la taxation des géants du numérique²⁶⁰.

La Chine à la pointe d'un contrôle gouvernemental de l'IA

Si, aux États-Unis, l'accent est mis sur la levée des contraintes sur les acteurs privés au nom de l'innovation, et qu'en Europe, la préoccupation concerne davantage les libertés individuelles et l'engagement a posteriori de la responsabilité des acteurs qui déploient l'IA, en Chine c'est un encadrement a priori qui prévaut de manière à garantir une supervision gouvernementale effective de l'IA.

En Chine, des dispositifs de surveillance de masse sont déployés de longue date, largement tolérés sinon acceptés par la population ; ils procèdent d'abord de l'initiative des acteurs privés mais avec une forme de supervision du régulateur qui n'est pas

²⁵⁸ Euractiv, *Researchers have trouble finding AI training data summaries*, <https://www.euractiv.com/news/researchers-have-trouble-finding-ai-training-data-summaries/>, 2 mars 2026, (consulté le 4 mars 2026).

²⁵⁹

Edith Hancock, « EU Floats Tweaks, New Grace Periods in AI Act », *Wall Street Journal*, 7 nov. 2025p. ; Raluca Besliu, *What's Driving the EU's AI Act Shake-Up?*, <https://techpolicy.press/whats-driving-the-eus-ai-act-shakeup>, 13 novembre 2025, (consulté le 4 mars 2026) ; Barbara Moens et Melissa Heikkilä, « How the EU botched its attempt to regulate AI », *Financial Times*, 20 nov. 2025p.

²⁶⁰ Gregorio Sorgi, *Victory for Trump as EU backs down on digital taxes in next budget*, <https://subscriber.politicopro.com/article/2025/07/victory-for-trump-as-eu-backs-down-on-digital-taxes-in-next-budget-00448914>, 11 juillet 2025, (consulté le 5 mars 2026).

exempte de tension²⁶¹. Le déploiement de l'IA s'inscrit dans ce contexte dans lequel la préservation des capacités de supervision gouvernementale a un caractère prioritaire.

Ces spécificités du contexte chinois ne doivent cependant pas masquer le fait que les autorités de ce pays partagent avec un grand nombre de gouvernements la même inquiétude quant aux menaces que représente pour la société, les personnes et la planète le déploiement de l'IA. Dans cette perspective, nous dit un éditorial de la revue *Nature*, « le pays a introduit depuis 2022 une série de lois et de normes techniques qui obligent les développeurs à soumettre les modèles d'IA générative au régulateur pour des évaluations de sécurité préalables au déploiement et à inclure des filigranes visibles et indélébiles sur les contenus générés par l'IA, afin de prévenir la fraude et la désinformation »²⁶². Confirmant ces avancées, le dernier rapport sur la sécurité de l'IA de l'organisation basée aux États-Unis *Future of Life* souligne positivement les avancées de la réglementation en Chine, notamment « les exigences contraignantes en matière d'étiquetage des contenus et de signalement des incidents, ainsi que les normes techniques nationales volontaires décrivant des processus structurés de gestion des risques liés à l'IA »²⁶³.

À l'aune de ces avancées, la proposition du gouvernement chinois de créer un organisme appelé Organisation mondiale de coopération en matière d'intelligence artificielle (WAICO), qui rassemblerait les nations dans le but de mettre en place un système mondial de gouvernance de l'IA pourrait contribuer à la construction d'un cadre international pour renforcer la sécurité de l'IA et prévenir des incidents majeurs²⁶⁴.

À l'échelle internationale, les approches en termes de réglementation divergent. Aux États-Unis, les autorités fédérales ont fait le choix d'un cadre réglementaire peu contraignant pour les firmes alors que l'approche européenne est davantage soucieuse de la protection des droits humains fondamentaux et de la responsabilité des firmes pour les préjudices que les produits d'IA pourraient causer. En Chine, en revanche, la régulation intervient en amont. Elle implique une validation *a priori* par les autorités administratives des modèles déployés et l'obligation d'un filigranage afin de maintenir une traçabilité de l'IA.

²⁶¹ Genia Kostka, « China's social credit systems and public opinion: Explaining high levels of approval », *New Media & Society*, 2018, p. 1461444819826402 ; Fan Liang et al., « Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure », *Policy & Internet*, 2018, vol. 10, n° 4, p. 415-453 ; Mareike Ohlberg, Ahmed Shazeda et Bertrand Lang, *The complex implementation of China's Social Credit System*, <https://www.merics.org/en/china-monitor/content/5071>, 12 décembre 2017, (consulté le 10 avril 2019).

²⁶² *Nature*, « China is leading the world on AI governance: other countries must engage », *Nature*, 11 décembre 2025, vol. 648, n° 8093, p. 251-251.

²⁶³ *Future of Life, FLI AI Safety Index, op. cit.*, p. 4.

²⁶⁴ Elizabeth Gibney, « China wants to lead the world on AI regulation — will the plan work? », *Nature*, 1 décembre 2025, p. d41586-025-03902-y.

B. Liste des entretiens

Les auteurs remercient pour leur disponibilité et les informations et analyses partagées les personnes suivantes ainsi que celle ayant préféré conserver l'anonymat:

- Prof. Adrien Alberinin (UNIGE),
- M. François Charlet (Vaudoise Assurance)
- Prof. Markus Christen (UZH)
- Dr. Daniel Fasel (Navique)
- Prof. François Fleuret (UNIGE)
- Dr. Bertrand Loison (OFS)
- Katharina Frey (ETHZ)
- Me. Dr. Christian Laux (Laux Lawyers)
- Mme. Estelle Pannatier (Algorithm Watch Switzerland)
- M. Gérald Vernez (digivolution)

Bien entendu, aucune de ces personnes n'est engagée de quelque manière que ce soit par le contenu de ce rapport dont la responsabilité incombe aux seul·e·s auteur·e·s.

C. Déclaration de transparence

- Cédric Durand ne rapporte aucun conflit d'intérêts potentiel.
- Yaniv Benhamou rapporte être membre expert du Groupe d'accompagnement de la Confédération Régulation IA et de l'Autorité indépendante d'examen des plaintes en matière de radiotélévision (AIEP). Les propos dans le rapport n'engagent que les auteur·e·s, et non ces deux autorités.
- Diego Kuonen rapporte être président du Groupe d'experts du Centre de compétences en science des données (DSCC) de la Confédération suisse. Les propos dans le rapport n'engagent que les auteur·e·s, et non le DSCC.
- Gaia Valenti ne rapporte aucun conflit d'intérêts potentiel.

Références

Académies suisses des sciences, « Charte suisse de littératie des données », 15 mai 2024.

Acemoglu Daron et Johnson Simon, *Power and Progress: our thousand-year struggle over technology and prosperity*, New York, PublicAffairs, 2024, 546 p.

Albisser Tamara Keller Julian Schmidli and Pascal, *Silent power guzzlers: Switzerland's booming data centres*, <https://www.swissinfo.ch/eng/swiss-ai/silent-power-guzzlers-switzerlands-booming-data-centres/89724159>, 25 juillet 2025, consulté le 1 mars 2026.

Amodei Dario, *Statement on our discussions with the Department of War*, <https://www.anthropic.com/news/statement-department-of-war>, février 2026, consulté le 28 février 2026.

Amodei Dario, *The Adolescence of Technology*, <https://www.darioamodei.com/essay/the-adolescence-of-technology>, janvier 2026, consulté le 17 février 2026.

Anchisi Mélissa, *Assemblée citoyenne sur l'intelligence artificielle*, s.l., EPFL AI Center, 2026.

Baily Martin, Byrne David, Kane Aidan et Soto Paul, « Generative AI at the Crossroads: Light Bulb, Dynamo, or Microscope? », *arXiv preprint arXiv:2505.14588*, 2025.

Barasa Hilda, Tay Peichin, McBride Keegan, Iosad Alexander et Mökander Jakob, *Sovereignty in the Age of AI: Strategic Choices, Structural Dependencies and the Long Game Ahead*, London, Tony Blair Institute for Global Change, 2026.

Bates Laura, « How tech turned against women », *Financial Times*, 21 févr. 2026 p.

BCLP, *California - SB53*, <https://infographics.bclplaw.marketing/>, 2025, consulté le 4 mars 2026.

BCLP, *US state-by-state AI legislation snapshot*, <https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html>, 2026, consulté le 4 mars 2026.

Bellanger François, Notions, enjeux et limites de la délégation d'activités étatiques, in La délégation d'activités étatiques au secteur privé (Favre Anne-Christine, Martenet Vincent, Poltier Etienne), Schulthess 2016, cité : Bellanger, p. 57.

Bengio Yoshua, Clare Stephen, Prunkl Carina, Andriushchenko Maksym, Bucknall Ben, Murray Malcolm, Bommasani Rishi, Casper Stephen, Davidson Tom et Douglas Raymond, « Rapport international sur la sécurité de l'IA 2026 », *arXiv preprint arXiv:2602.21012*, 2026.

Benhamou Bernard, Souveraineté numérique : quelles stratégies pour la France et l'Europe ? publié le 27 octobre 2020, accessible sur <<https://www.vie-publique.fr/parole-dexpert/276126-souverainete-numerique-queelles-strategies-pour-la-france-et-leurope>>. (cité : Benhamou B., Souveraineté numérique).

Benhamou Yaniv, Bernard Frédéric et Durand Cédric, *Souveraineté numérique: étude pluridisciplinaire pour la Suisse*, 2023, Genève, Digital Law Center, 2023.

Benhamou Yaniv, Big Data and the Law: a holistic analysis based on a three-step approach – Mapping property-like rights, their exceptions and licensing practices, *SZW-RSDA 04/2020* | p. 393-418, cité: Benhamou 2020.

Benhamou Yaniv, Creative Value Chains - Copyright and Beyond for a Better Value Distribution, Bristol University Press, 2026, cité: Benhamou 2026.

Benhamou Yaniv, ERARD Frédéric, KRAUS Daniel E. L'avocat a-t-il aussi le droit d'être dans les nuages? In: *Revue de l'avocat*, 2019, vol. 22, n° 3, p. 119–126, cité: Benhamou/Erard/Kraus

Benhamou Yaniv, Open Source Ai: Does the Copyleft Clause Propagate to Proprietary Ai Models? Revisiting the Definition of Derivatives in the Ai-Context, publié le 11 novembre 2024, accessible sur <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5016757>. (cité: Benhamou 2024).

Benhamou Yaniv/ Andrijevic Ana, The protection of AI-generated pictures (photograph and painting) under copyright law. In: *Research Handbook on Intellectual Property and Artificial Intelligence*, Abbott Ryan, Geffen David (Ed.), Cheltenham : Elgar, 2022. p. 198–217. (cité : Benhamou/Andrijevic).

Benhamou Yaniv/ Bernard Frédéric/ Durand Cédric, Souveraineté numérique : étude pluridisciplinaire pour la Suisse, <<https://archive-ouverte.unige.ch/unige:168718>> .; (cité Benhamou/Bernard/Durand, p... (

Benhamou Yaniv/ De Werra Jacques/ Pascal Nathanaël/ Chaix Gabriel, Procédure de consultation relative à la nouvelle loi sur les plateformes de communication et les

Benhamou Yaniv/ Dulong de Rosnay Mélanie, Open Licensing and Data Trust for Personal and Non-Personal Data: a blueprint to support the commons and Privacy, 56 *International Review of Intellectual Property and Competition Law (IIC)*, publié le 9 septembre 2025, accessible sur <<https://link.springer.com/article/10.1007/s40319-025-01636-y>>. (cité : Benhamou/Dulong de Rosnay, p.)

Benhamou, Yaniv / De werra, Jacques. Propriété intellectuelle et concurrence déloyale. Analyse du droit suisse et perspectives de droit allemand. In: *Propriété intellectuelle et concurrence déloyale : les liaisons dangereuses ?* Puttemans Andrée/ Gendreau Ysolde/ De Werra Jacques (Ed.). Bruxelles. Bruxelles : Larcier, 2017. p. 183–208. (cité : Benhamou/De Werra 2017).

Besliu Raluca, *What's Driving the EU's AI Act Shake-Up?*, <https://techpolicy.press/whats-driving-the-eus-ai-act-shakeup> , 13 novembre 2025, consulté le 4 mars 2026.

Birnhack Michael D., In Defense of Privacy-as-Control (Properly Understood), *Jurimetrics* 65, 2026, pp.143-194, accessible <<https://ssrn.com/abstract=5042930>> (cité: Birnhack, p...).

Bobrowsky Meghan, An-Pham Drew et Pipe Alana, « Big Tech's AI Push Is Costing a Lot More Than the Moon Landing », *Wall Street Journal*, 7 févr. 2026 p.

Bogmans Christian, Gomez-Gonzalez Patricia, Ganpurev Ganchimeg, Melina Giovanni, Pescatori Andrea et Thube Sneha, « Power hungry: How ai will drive energy demand », *IMF Working Papers*, 2025, vol. 81, n° 4, p. 2025.

Braun Binder Nadja/ Burri Thomas/ Lohmann Melinda Florina/ Simmler Monika/ Thouvenin Florent/ Vokinger Kerstin Nöelle, Künstliche Intelligenz : Handlungsbedarf im

Schweizer Recht, Jusletter du 28 juin 2021, accessible sur <https://www.ius.uzh.ch/dam/jcr:892b9df7-169e-43fb-aa6c-4df89c2cb8cc/2021Jusletter_k%C3%BCnstl_Intelligenz.pdf>. (cité : Braun Binder/ Burri/ Lohmann/ Simmler/ Thouvenin/ Vokinger, Künstliche Intelligenz : Handlungsbedarf im Schweizer Recht).

Bryson Joanna, « Human-Centred Control of AI Is Both Possible and Necessary » dans *The Role of Transatlantic Cooperation in AI Human Oversight in Defence*, Amsterdam, IOS Press (coll. « NATO Science for Peace and Security Series »:), 2026.

Carvalho Carine, 25_POS_13 - L'état doit prévenir la discrimination algorithmique dans son utilisation de l'intelligence artificielle (IA), <https://www.vd.ch/gc/seances-du-grand-conseil/point-seance/point/b988879d-5120-47b3-90bf-6c83aff02ade/meeting/1026879>, 25 février 2025, consulté le 18 mars 2026.

Champagne Dylan, *President Trump Targets State AI Regulations*, <https://www.theregreview.org/2026/02/26/champagne-president-trump-targets-state-based-ai-regulations/>, 26 février 2026, consulté le 4 mars 2026.

Chancellerie fédérale, « Terminologie - Réseau de compétences en intelligence artificielle ».

Chancellerie fédérale, *Réseau de compétences en intelligence artificielle*, https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/kuenstliche_intelligenz/kinetzwerk.html, janvier 2026, consulté le 3 mars 2026.

Chancellerie fédérale, *SB021 - Stratégie pour l'utilisation de systèmes d'IA dans l'administration fédérale*, <https://www.bk.admin.ch/bk/fr/home/digitale-transformation-ikt-lenkung/vorgaben/sb021-strategie-einsatz-von-ki-systemen-in-der-bundesverwaltung.html>, 11 décembre 2025, consulté le 3 mars 2026.

Chappuis Benoit, Alberini Adrien, *Secret professionnel et solutions cloud In: Revue de l'avocat*, 2017, vol. 2017, n° 8, p. 337. Cité : Chappuis/Alberini

Chavanne Yannick, *Le marché IT suisse bousculé par une vague d'acquisitions en 2025*, <https://www.ictjournal.ch/articles/2025-12-19/le-marche-it-suisse-bouscule-par-une-vague-dacquisitions-en-2025>, 19 décembre 2025, consulté le 18 mars 2026.

Chavanne Yannick, *Souveraineté numérique et cloud : les clarifications de l'avocat Sylvain Métille* in *ICT journal*, publié le 5 mars 2026, accessible sur <<https://www.ictjournal.ch/interviews/2026-03-05/souverainete-numerique-et-cloud-les-clarifications-de-lavocat-sylvain-metille>>, cité : Chavanne, [ictjournal.ch/interviews/2026-03-05](https://www.ictjournal.ch/interviews/2026-03-05)

Chen Sophia, « Data centres will use twice as much energy by 2030 — driven by AI », *Nature*, 10 avril 2025.

Chen Yvonne Jie, Gong Jie, Li Jin et Zhao Zibo, « Better Technology, Worse Motivation: GenAI's Mediocrity Trap », *Available at SSRN 5208163*, 2025.

CHf – Chancellerie fédérale, *Plan de mise en œuvre Sous-stratégie en matière d'IA*, publié le 11 décembre 2025, accessible sur <<https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.bk.admin.ch/dam/bk/fr/dokumente/dti/themen/umsetzungsplan-ki-strategie.pdf.download.pdf/Umsetzungsplan%2520zur%2520KI->

[Strategie%2520der%2520Bundesverwaltung%2520-%2520FR.pdf&ved=2ahUKEwji_sKE1I2UAXURgf0HHeliDNwQFnoECBUQAQ&usg=AOvVaw0x3bt-a1qvgs5tIRzDBvVI>](#), cité: CHf, Plan de mise en œuvre Sous-stratégie en matière d'IA

CHf – Chancellerie fédérale, Stratégie Utilisation de systèmes d'IA dans l'administration fédérale, publié le 11 décembre 2025, accessible sur < <https://www.bk.admin.ch/dam/bk/fr/dokumente/dti/Vorgaben/StrategienundTeilstrategie/ki-teilstrategie.pdf.download.pdf/Strat%C3%A9gie%20Utilisation%20de%20syst%C3%A8mes%20d%E2%80%99IA%20dans%20l%E2%80%99administration%20f%C3%A9d%C3%A9rale.pdf>>, cité : CHf, Stratégie Utilisation de systèmes d'IA dans l'administration fédérale

Colorado General Assembly, *SB24-205 Consumer Protections for Artificial Intelligence* | Colorado General Assembly, <https://leg.colorado.gov/bills/sb24-205> , 17 mai 2024, consulté le 4 mars 2026.

Commission européenne, Communication de la Commission, Une stratégie européenne pour les données, COM (2020) 66 final , accessible sur < <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066>>, cité: Commission européenne, Une stratégie européenne pour les données

Confédération suisse, Message concernant un crédit d'engagement pour la mise en place d'un Swiss Government Cloud (SGC), publié le 22 mai 2024, accessible sur < <https://www.news.admin.ch/news/message/attachments/87803.pdf>>, cité : Confédération suisse, Message concernant un crédit d'engagement pour la mise en place d'un Swiss Government Cloud (SGC)

Conseil de l'Europe, Rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit, publié le 05 septembre 2025, accessible sur <<https://rm.coe.int/1680afae68> >, cité : Conseil de l'Europe, Rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit.

Conseil fédéral, Réglementation de l'IA: le Conseil fédéral veut ratifier la Convention du Conseil de l'Europe, 12 février 2025, publié le 12 février 2025, accessible sur < <https://www.admin.ch/fr/nsb?id=104110> >, cité: Conseil fédéral, Réglementation de l'IA: le Conseil fédéral veut ratifier la Convention du Conseil de l'Europe.

Conseil fédéral, Souveraineté numérique de la Suisse, publié le 26 novembre 2025, accessible sur < <https://cms.news.admin.ch/dam/fr/der-schweizerische-bundesrat/PMaPuzW8Wqon/Beilage+01+Bericht+in+Erf%C3%BCllung+des+Postulats+22.4411+FR+zu+BRA+EDA.pdf> >, cité: Conseil fédéral, Souveraineté numérique de la Suisse.

Conseil fédéral, Stratégie Suisse numérique 2026, publié le 12 décembre 2025, accessible sur <<https://digital.swiss/fr/> >. (cité: Conseil fédéral, Stratégie Suisse numérique).

De Montenay Lorraine, Petit Benoit, Diguët Cécile et Fourboul Eric, *Prospective d'évolution des consommations des data centers à court, moyen et long terme de 2024 à 2060*, <https://librairie.ademe.fr/energies/8910-prospective-d-evolution-des->

consommations-des-data-centers-a-court-moyen-et-long-terme-de-2024-a-2060.html , janvier 2026, consulté le 25 février 2026.

De Werra Jacques / Benhamou Yaniv, Cyberassurance : instrument utile pour la cybersécurité des entreprises ? in : Jusletter 24 août 2020, accessible sur <<https://www.digitallawcenter.ch/sites/default/files/publications/article-jacques-de-werra-yaniv-benhamou-cyberassurance-jusletter.pdf>>. (cité : De Werra/Benhamou).

de Werra Jacques, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non-personnelles (par des licences obligatoires ou des licences « FRAND ») ?, SZW-RSDA 04/2020 | p. 365-392, cité : de Werra

De Werra Jacques, Patents and trade secrets in the internet age. In: *Zeitschrift für Papyrologie und Epigraphik*, 2015, vol. 134. Halbbd. 2, p. 123–190, accessible sur <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2684616 >. (cité : De Werra 2015).

Deloitte, *The State of AI in the Enterprise - 2026 AI report* | Deloitte US, s.l., 2026.

DETEC - Département fédéral de l'environnement, des transports, de l'énergie et de la communication, Mise à disposition et échanges de données pour la conduite automatisée dans le trafic routier, publié le 7 décembre 2018, accessible sur <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.astra.admin.ch/dam/astra/fr/dokumente/abteilung_strassennetzeallgemein/bereitstellung-austausch-daten-automatisiertes-fahren.pdf.download.pdf/Mise%2520%25C3%25A0%2520disposition%2520et%2520%25C3%25A9changes%2520de%2520donn%25C3%25A9es%2520pour%2520la%2520conduite%2520automatis%25C3%25A9e%2520dans%2520le%2520trafic%2520routier.pdf&ved=2ahUKEwi_4f3c942UAXXu3AIHHYD4HfYQFnoECBsQAQ&usg=AOvVaw3Csrj2gOLg0gimcmseimjh>, cité: DETEC, Mise à disposition et échanges de données pour la conduite automatisée dans le trafic routier.

DINUM, *Souveraineté numérique : l'État accélère la réduction de ses dépendances extra-européennes*, <https://www.numerique.gouv.fr/sinformer/espace-presse/souverainete-numerique-reduction-dependances-extra-europeennes/> , 8 avril 2026, consulté le 21 avril 2026.

Durand Cédric et Rikap Cecilia, « “Pour sortir de la dépendance européenne aux Big Tech, il faut une politique numérique non alignée” », *Le Monde*, 9 janv. 2025 p.

Durand Cédric, « After AI », *NLR/Sidecar*, 15 janvier 2026.

Elder Bryce, « How high are OpenAI's compute costs? Possibly a lot higher than we thought », *Financial Times*, 12 nov. 2025 p.

ETHZ, *Apertus: a fully open, transparent, multilingual language model*, <https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a-fully-open-transparent-multilingual-language-model.html> , 2 septembre 2025, consulté le 18 mars 2026.

Euractiv, *Researchers have trouble finding AI training data summaries*, <https://www.euractiv.com/news/researchers-have-trouble-finding-ai-training-data-summaries/> , 2 mars 2026, consulté le 4 mars 2026.

Euractiv, *The German state pioneering digital sovereignty*, <https://www.euractiv.com/news/the-german-state-pioneering-digital-sovereignty/> , 15 septembre 2025, consulté le 21 avril 2026.

European Commission, Final Report of the Expert Group on B2B Data Sharing and Cloud Computing Contracts, publié le 2 avril 2025, accessible: < <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.aigl.blog/content/files/2025/04/Final-Report-of-the-Expert-Group-on-B2B-data-sharing-and-cloud-computing-contracts.pdf&ved=2ahUKEwiQ-8eI942UAxU3Zv4FWWATBesQFnoECBoQAAQ&usg=AOvVaw3Kz8KFCGRm6FrgawA5aI2> > , cité: European Commission, Final Report of the Expert Group on B2B Data Sharing and Cloud Computing Contracts

European Commission, *Commission Staff Working Document on Common European Data Spaces*, SWD(2022) 45 final, publié 23 février 2022, <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces>.

Eurostat, *32.7% of EU people used generative AI tools in 2025*, <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251216-3> , 16 décembre 2025, consulté le 28 février 2026.

Farrell Henry, Gopnik Alison, Shalizi Cosma et Evans James, « Large AI models are cultural and social technologies », *Science*, 2025, vol. 387, n° 6739, p. 1153-1156.

Flückiger Alexandre, (Re)faire la loi : Traité de légistique à l'ère du droit souple, Berne (Stämpfli), 2019, p. 244 (cité : Flückiger, Légistique).

Fourcade Marion et Healy Kieran, « Seeing like a market », *Socio-Economic Review*, 23 décembre 2016, p. mww033.

Francey Julien, art. 17 Petit commentaire LPD ((Benhamou Yaniv, Cottier Bertil ed.) Helbing Lichtenhahn, Bâle), cité: Francey.

Fédération Suisse des Avocats (FSA), Lignes directrices pour les avocates et les avocats concernant l'utilisation de l'IA, publiées le 6 janvier 2026, <<https://digital.sav-fsa.ch/fr/kiguidelines>> (cité : Lignes directrices FSA concernant l'utilisation de l'IA).

Future of Life, *FLI AI Safety Index*, Campbell, California, 2025.

Gallup, *AI Use at Work Rises*, <https://www.gallup.com/workplace/699689/ai-use-at-work-rises.aspx> , 14 décembre 2025, consulté le 7 janvier 2026.

Gallup, *Frequent Use of AI in the Workplace Continued to Rise in Q4*, <https://www.gallup.com/workplace/701195/frequent-workplace-continued-rise.aspx> , 25 janvier 2026, consulté le 28 février 2026.

Genecand Adrien, *Stop à la dépendance vis-à-vis des systèmes américains – Pour des solutions IT 100% suisses*, s.l., 2025.

Ghosh Agnee, « Bonanza or Bubble? Where AI Goes From Here », *Bloomberg.com*, 18 mars 2026 p.

Gibney Elizabeth, « China wants to lead the world on AI regulation — will the plan work? », *Nature*, 1 décembre 2025, p. d41586-025-03902-y.

Gjesvik Lars, « Private infrastructure in weaponized interdependence », *Review of International Political Economy*, 2 mai 2022, p. 1-25.

Grow Dave, *Unlocking AI's full potential requires operational excellence*, <https://www.technologyreview.com/2025/10/01/1124593/unlocking-ais-full-potential-requires-operational-excellence/> , 1 octobre 2025, consulté le 3 janvier 2026.

Grush Loren, « Why AI Data Centers in Space Aren't Totally Science Fiction », *Bloomberg.com*, 13 janv. 2026p.

Guegant Louis, Aubet Louise et Bitard Lea, *Les impacts environnementaux du numérique en Suisse*, s.l., 2025.

Guidi Gianluca, Dominici Francesca, Gilmour Jonathan, Butler Kevin, Bell Eric, Delaney Scott et Bargagli-Stoffi Falco J, « Environmental burden of United States data centers in the artificial intelligence era », *arXiv preprint arXiv:2411.09786*, 2024.

Hagendorff Thilo, Derner Erik et Oliver Nuria, « Large reasoning models are autonomous jailbreak agents », *Nature Communications*, 5 février 2026, vol. 17, n° 1, p. 1435.

Hammond George, « Anthropic's breakout moment: how Claude won business and shook markets », *Financial Times*, 6 févr. 2026 p.

Hammond George, « Anthropic's breakout moment: how Claude won business and shook markets », *Financial Times*, 6 févr. 2026 p.

Hancock Edith, « EU Floats Tweaks, New Grace Periods in AI Act », *Wall Street Journal*, 7 nov. 2025 p.

Hashmi E., S. Y. Yayilgan, M. M. Yamin, S. Ali and M. Abomhara, "Advancing Fake News Detection: Hybrid Deep Learning With FastText and Explainable AI," in *IEEE access*, 2024, vol. 12, p. 44462-44480 .

Hawkins Zoe, Lehdonvirta Vili et Wu Boxi, « AI compute sovereignty: Infrastructure control across territories, cloud providers, and accelerators », *Cloud Providers, and Accelerators (June 20, 2025)*, 2025.

Humlum Anders et Vestergaard Emilie, *Large language models, small labor market effects*, s.l., National Bureau of Economic Research, 2025.

Ibrahim Lujain, Akbulut Canfer, Elasmara Rasmi, Rastogi Charvi, Kahng Minsuk, Morris Meredith Ringel, McKee Kevin R, Rieser Verena, Shanahan Murray et Weidinger Laura, « Multi-turn evaluation of anthropomorphic behaviours in large language models », *arXiv preprint arXiv:2502.07077*, 2025.

IEA, *Understanding the energy-AI nexus – Energy and AI – Analysis*, <https://www.iea.org/reports/energy-and-ai/understanding-the-energy-ai-nexus> , 2025, consulté le 1 mars 2026.

IP Ken, *Opinion | Frenzy over AI agent OpenClaw shows the lobster has escaped the pot*, <https://www.scmp.com/opinion/china-opinion/article/3346562/frenzy-over-ai-agent-openclaw-shows-lobster-has-escaped-pot> , 18 mars 2026, consulté le 18 mars 2026.

IPI – Institut Fédéral de la Propriété Intellectuelle, accès aux données non personnelles dans le secteur privé, publié le 1.3.2021, accessible sur < <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.news.admin.ch/newsd/message/attachments/66750.pdf&ved=2ahUKEwjT9d-C2o2UAXVg3QIHHXPSIUwQFnoECBsQAQ&usq=AOvVaw2uPJBvQQbllPUuQ-HwXphz> >, cité : IPI, accès aux données non personnelles dans le secteur privé

Isler Michel, Text and Data Mining in der medizinischen Forschung, LSR 2022, cité: Isler.

Jacot-Guillarmod Emilie, art. 9 Petit commentaire LPD (Benhamou Yaniv, Cottier Bertil ed.) Helbing Lichtenhahn, Bâle, cité: Jacot-Guillarmod.

Kaadoud Ikram Chraïbi, *IA et métacognition : savoir quand on peut faire confiance, ou non, à la machine n'est pas toujours évident*, <https://theconversation.com/ia-et-metacognition-savoir-quand-on-peut-faire-confiance-ou-non-a-la-machine-nest-pas-toujours-evident-279348> , 29 mars 2026, consulté le 22 avril 2026.

King Ian, Wu Jin, Davidson Stephanie et Bass Dina, « Why the AI Boom Will Make Phones, Cars and Electronics More Expensive », *Bloomberg.com*, 8 mars 2026 p.

Kosmyna Nataliya, Hauptmann Eugene, Yuan Ye Tong, Situ Jessica, Liao Xian-Hao, Beresnitzky Ashly Vivian, Braunstein Iris et Maes Pattie, « Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task », *arXiv preprint arXiv:2506.08872*, 2025, vol. 4.

Kostka Genia, « China's social credit systems and public opinion: Explaining high levels of approval », *New Media & Society*, 2018, p. 1461444819826402.

Kshirsagar Mihir, *Lifespan of AI Chips: The \$300 Billion Question*, <https://blog.citp.princeton.edu/2025/10/15/lifespan-of-ai-chips-the-300-billion-question/> , 15 octobre 2025, consulté le 3 mars 2026.

Kuonen Diego et Vernez Gérard, « Sécurité en mutation : l'effet IA. », *Cybersecurity trends*, 2025 p. 31-34.

Laghari, *STMicroelectronics s'envole en Bourse après un contrat à plusieurs milliards avec Amazon*, <https://www.lesechos.fr/tech-medias/hightech/stmicroelectronics-senvole-en-bourse-apres-un-contrat-a-plusieurs-milliards-avec-amazon-2214854> , 9 février 2026, consulté le 25 février 2026.

Lang Hannah Erin, « AI Gave Investors a Glimpse of the Future This Month. And They Sold Their Stocks. », *Wall Street Journal*, 27 févr. 2026 p.

Le Conseil fédéral, *Souveraineté numérique de la Suisse*, Berne, 2025.

Le peuple de Genève, « Art. 21A3 Droit à l'intégrité numérique ».

Levy Steven, « How the Loudest Voices in AI Went From 'Regulate Us' to 'Unleash Us' », *Wired*, 30 mai 2025, 30 mai 2025 p.

Liang Fan, Das Vishnupriya, Kostyuk Nadiya et Hussain Muzammil M, « Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure », *Policy & Internet*, 2018, vol. 10, n° 4, p. 415-453.

Lu Jackson G., Song Lesley Luyang et Zhang Lu Doris, « Cultural tendencies in generative AI », *Nature Human Behaviour*, 20 juin 2025, vol. 9, n° 11, p. 2360-2369.

Mann Michael, « The autonomous power of the state: its origins, mechanisms and results », *European Journal of Sociology/Archives européennes de sociologie*, 1984, vol. 25, n° 2, p. 185-213.

Margoni/Strowel, Contractual freedom and fairness, Research handbook on intellectual property licensing, 2025, cite: Margoni/Strowel

Maslej Nestor, Fattorini Loredana, Perrault Raymond, Gil Yolanda, Parli Vanessa, Kariuki Njenga, Capstick Emily, Reuel Anka, Brynjolfsson Erik, Etchemendy John, Ligett Katrina, Lyons Terah, Manyika James, Niebles Juan Carlos, Shoham Yoav, Wald Russell, Walsh Toby, Hamrah Armin, Santarlaschi Lapo, Lotufo Julia Betts, Rome Alexandra, Shi Andrew et Oak Sukrut, « Artificial Intelligence Index Report 2025 ».

Mason Jeff, Hunnicutt Trevor, Alper Alexandra et Mason Jeff, « Biden administration aims to cut AI risks with executive order », *Reuters*, 30 oct. 2023 p.

McCarthy John, Minsky Marvin L, Rochester Nathaniel et Shannon Claude E, « A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955 », *AI magazine*, 2006, vol. 27, n° 4, p. 12-14.

Mehmetaj Liburn, Intelligence artificielle : repères pratique pour les avocats, in *Revue de l'avocat* 1/2026, p. 29 ss, cité : Mehmetah.

Métille Sylvain, Les collectivités publiques face à l'externalisation informatique, publié le 4 novembre 2025, accessible sur < <https://smetille.ch/2025/11/04/jusletter-collectivites-publiques-externalisation-informatique/> >, cité : Métille, smetille.ch/2025/11/04.

Mettan Guy, *Pour préserver la souveraineté numérique du canton de Genève*, s.l., 2025.

Meyer Marguerite, Naegli Lorenz, Oertli Balz et Steiner Jennifer, « How tenaciously Palantir courted Switzerland », *Republik*, 8 décembre 2025.

Microsoft Switzerland, *Microsoft Deepens Switzerland's Digital Future with Strategic Investment in Cloud and AI Infrastructure, Startups, Skilling and Innovation*, <https://news.microsoft.com/de-ch/2025/06/02/microsoft-deepens-switzerlands-digital-future-with-strategic-investment-in-cloud-and-ai-infrastructure-startups-skilling-and-innovation/> , 2 juin 2025, consulté le 25 février 2026.

Mims Christopher, « How Businesses Are Manipulating ChatGPT Results », *Wall Street Journal*, 30 janv. 2026 p.

Moens Barbara et Heikkilä Melissa, « How the EU botched its attempt to regulate AI », *Financial Times*, 20 nov. 2025 p.

moteurs de recherche – prise de position, publié le 16 février 2026, accessible sur <https://digitallawcenter.ch/sites/default/files/publications/digital-law-center_ap-lpcom_prise-de-position_16.02.2026-1.pdf> (cité : Benhamou/ De Werra/Pascal/ Chaix, *Prise de position du Digital Law Center*).

National Museum of American History, *Electronic Neural Network, Mark I Perceptron*, https://americanhistory.si.edu/collections/object/nmah_334414 , 2026, consulté le 13 février 2026.

Nature, « China is leading the world on AI governance: other countries must engage », *Nature*, 11 décembre 2025, vol. 648, n° 8093, p. 251-251.

Neumann Oliver, Guirguis Katharina et Steiner Reto, « Exploring artificial intelligence adoption in public organizations: a comparative case study », *Public Management Review*, 2 janvier 2024, vol. 26, n° 1, p. 114-141.

Nicolet-dit-Félix Julien, *Pour un plan de désengagement des logiciels propriétaires et des solutions d'hébergement numérique états-unis*, s.l., 2025.

Niederhoffer Kate, Kellerman Gabriella Rosen, Lee Angela, Liebscher Alex, Rapuano Kristina et Hancock Jeffrey T., « AI-Generated “Workslop” Is Destroying Productivity », *Harvard Business Review*, 22 septembre 2025, 22 sept. 2025 p.

O'Connor Sarah et Burn-Murdoch John, « Is AI making work more intense? », *Financial Times*, 19 févr. 2026 p.

OCDE, *OECD AI Incidents Monitor, an evidence base for trustworthy AI*, <https://oecd.ai/en/incidents>, 2026, consulté le 27 février 2026.

OCDE, *Recommandations du Conseil sur l'intelligence artificielle*, <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449>, 3 mai 2024, consulté le 3 mars 2026.

OECD, *AI Principles Overview*, <https://oecd.ai/en/principles>, 2026, consulté le 3 mars 2026.

OECD, *Defining AI incidents and related terms*, s.l., (coll. « OECD Artificial Intelligence Papers »), 2024, vol.16.

OFCOM – Office fédéral de la communication, Etat des lieux sur la réglementation de l'intelligence artificielle, publié le 12 février 2025, accessible sur < https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.bakom.admin.ch/dam/fr/sd-web/MKUEgci9oDRD/Auslegeordnung%2520zur%2520Regulierung%2520von%2520%2520k%25C3%25BCnstlicher%2520Intelligenz_def.pdf&ved=2ahUKEWjSiKrY1I2UAX4hf0HHUZrKrwQFnoECBYQAQ&usg=AOvVaw0BnCth9Yc9Lv4P1YNpCTiR>, cité : OFCOM, Etat des lieux sur la réglementation de l'intelligence artificielle

OFIT – Office fédéral de l'informatique et de la télécommunication, Swiss Government Cloud, accessible sur < <https://www.bit.admin.ch/fr/sgc-fr>>, cité : OFIT, Swiss Government Cloud

OFJ – Office fédéral de la Justice, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificielle, publié le 31 août 2024, accessible sur <<https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/kuenstliche-intelligenz.html>>. (cité : OFJ, Analyse juridique de base dans le cadre de l'état des lieux sur les approches de régulation en matière d'intelligence artificiel).

OFJ – Office fédéral de la Justice, Guide pour l'élaboration de la législation fédérale, 2025, accessible sur <<https://www.bj.admin.ch/bj/fr/home/staat/legistik/hauptinstrumente.html>>. (cité : OFJ, Guide de la législation).

OFCOM – Office fédéral de la communication, Analyse des réglementations en matière d'intelligence artificielle dans différents pays et régions du monde, publié le 16 décembre 2024, accessible sur <https://www.bakom.admin.ch/dam/fr/sd-web/3DmSVH-UgRCm/analyse_laender.pdf>. (cité : OFCOM, Analyse des réglementations dans différents pays et régions du monde).

OFCOM – Office fédéral de la communication, Etat des lieux sur la réglementation de l'intelligence artificielle, publié le 12 février 2025 < <https://www.bakom.admin.ch/dam/fr/sd->

[web/MKUEgci9oDRD/Auslegeordnung%20zur%20Regulierung%20von%20k%C3%BCnstlicher%20Intelligenz_def.pdf](https://www.merics.org/en/china-monitor/content/5071)>. (cité : OFCOM, Etat des lieux).

Ohlberg Mareike, Shazeda Ahmed et Lang Bertrand, *The complex implementation of China's Social Credit System*, <https://www.merics.org/en/china-monitor/content/5071> , 12 décembre 2017, consulté le 10 avril 2019.

Pasquinelli Matteo, *The eye of the master: a social history of artificial intelligence*, London New York, Verso, 2023, 1 p.

Projet de loi constitutionnelle modifiant la constitution de la République et canton de Genève (Cst-GE) (A 2 00) (Pour une protection forte de l'individu dans l'espace numérique) (cité : PL-12945, p...).

Radunski Stefanie Pauli Michael, *Bund will sich von Abhängigkeit von Microsoft lösen*, <https://www.nzz.ch/schweiz/ploetzliche-kehrwende-der-bund-will-sich-von-abhaengigkeit-von-microsoft-loesen-ld.1934311> , 18 avril 2026, consulté le 21 avril 2026.

Ranganathan Aruna et Ye Xingqi Maggie, « AI Doesn't Reduce Work—It Intensifies It », *Harvard Business Review*, 9 février 2026, 9 févr. 2026 p.

Rikap Cecilia, *Teoría de la Dependencia Digital*, Caja Negra., s.l., 2026, 240 p.

Ring Suzi, « ICC staff print files and prepare for blackout as US sanctions loom », *Financial Times*, 30 sept. 2025 p.

Rogers Alex et Morris Stephen, « Big Tech pushes for 10-year ban on US states regulating AI », *Financial Times*, 18 juin 2025 p.

Rosenthal David/Veraldi Livio, Training AI language with third-party content and data from a legal perspective, in : Jusletter IT 25 mars 2025, no 65 ss. Cité: Rosenthal/Veraldi.

Rosner-Uddin Rafe et Ruehl Mercedes, « Palantir sues magazine that revealed Switzerland rejected its approaches », *Financial Times*, 22 févr. 2026 p.

Rosner-Uddin Rafe, « Amazon holds engineering meeting following AI-related outages », *Financial Times*, 10 mars 2026 p.

Rosner-Uddin Rafe, Georgiadis Philip et Heikkilä Melissa, « Amazon to axe another 16,000 corporate jobs », *Financial Times*, 28 janv. 2026 p.

Rouvroy Antoinette et Berns Thomas, « Gouvernamentalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », *Réseaux*, 2013, vol. 177, n° 1, p. 163-196.

Ruegger Vanessa/ Dias Fanny, Le droit à l'intégrité numérique selon l'article 21A de la Constitution genevoise in SJ 2026 pp.41-65. (cité : Ruegger/Dias, p....).

Rydlo Alexandre, *Intervention parlementaire - Intelligence artificielle: accompagnement de l'administration*, <https://www.vd.ch/actualites/decisions-du-conseil-detat/seance-du-conseil-detat/decision/id/b2a0bd19-f4db-4225-99d4-10610d727ff7> , 21 mai 2024, consulté le 18 mars 2026.

Sam Cédric, Dottle Rachel, Ghoash Agnee et Kyle Kim, « A Guide to the Circular Deals Underpinning the AI Boom », *Bloomberg.com*, 22 janv. 2026 p.

Sastry Girish, Heim Lennart, Belfield Haydn, Anderljung Markus, Brundage Miles, Hazell Julian, O'keefe Cullen, Hadfield Gillian K, Ngo Richard et Pilz Konstantin, « Computing

power and the governance of artificial intelligence », *arXiv preprint arXiv:2402.08797*, 2024.

Schechner Sam, Jin Berber et Mackrael Kim, « Europe Prepares for a Nightmare Scenario: The U.S. Blocking Access to Tech », *Wall Street Journal*, 24 janv. 2026 p.

Schmitt Fabienne, *Thierry Breton interdit d'entrée aux US : la guerre froide numérique est déclarée entre l'Europe et les Etats-Unis*, <https://www.lesechos.fr/monde/europe/sanctions-contre-thierry-breton-la-guerre-froide-numerique-est-declaree-entre-washington-et-bruxelles-2206708> , 24 décembre 2025, consulté le 17 février 2026.

Schweiser Armee, *Palantir Technologies Inc.*, Bern, 2024.

Seydtaghia Anouch, « Apertus, projet suisse majeur en IA, aura une nouvelle version au printemps », *Le Temps*, 10 févr. 2026 p.

Shepardson David, « Trump revokes Biden executive order on addressing AI risks », *Reuters*, 21 janv. 2025 p.

Shumer Matt, *Something Big Is Happening*, <https://shumer.dev/something-big-is-happening> , 9 février 2026, consulté le 17 février 2026.

Shwartz Vered, *Artificial intelligence needs to be trained on culturally diverse datasets to avoid bias*, <https://theconversation.com/artificial-intelligence-needs-to-be-trained-on-culturally-diverse-datasets-to-avoid-bias-222811> , 13 février 2024, consulté le 22 avril 2026.

Sorgi Gregorio, *Victory for Trump as EU backs down on digital taxes in next budget*, <https://subscriber.politicopro.com/article/2025/07/victory-for-trump-as-eu-backs-down-on-digital-taxes-in-next-budget-00448914> , 11 juillet 2025, consulté le 5 mars 2026.

SUPSI, *When AI gets it wrong: the problem of bias in data*, <https://www.supsi.ch/quando-l-ia-sbaglia-il-problema-degli-stereotipi-nei-dati>, 15 septembre 2023, consulté le 22 avril 2026.

Swiss Data Alliance, *Souveraineté numérique : façonner l'avenir numérique de la Suisse (livre blanc)*, s.l., 2025.

Synergy Research Group, *Cloud Market Share Trends - Big Three Together Hold 63% while Oracle and the Neoclouds Inch Higher*, <https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher> , 19 novembre 2025, consulté le 25 février 2026.

Tarkowski Alek, Cañigüeral Albert, Sieker Felix et Cominassi Felix, *Public AI: Policies for democratic and sustainable AI infrastructures*, <https://oecd.ai/en/wonk/public-ai-policies-for-democratic-and-sustainable-ai-infrastructures> , 5 décembre 2025, consulté le 8 mars 2026.

The Economist, « Investors expect AI use to soar. That's not happening », *The Economist*, 26 novembre 2025, 26 nov. 2025 p.

Thomas Daniel, Raval Anjli, Ring Suzi et Heikkilä Melissa, « Are Anthropic's new AI work tools game-changing for professionals? », *Financial Times*, 16 févr. 2026 p.

Thouvenin Florent, Ein Rechtsrahmen für KI in der Schweiz: Handlungsbedarf und Handlungsoptionen bei Transparenz und Datenschutz, Jusletter.ch 2025, cité: Thouvenin.

UNIGE, IA générative, guide à l'intention de la communauté universitaire, publié en septembre 2024, accessible sur <
https://www.unige.ch/numerique/download_file/44/0>, cité: UNIGE, IA générative, guide à l'intention de la communauté universitaire
https://www.ius.uzh.ch/dam/jcr:892b9df7-169e-43fb-aa6c-4df89c2cb8cc/2021Jusletter_künstl_Intelligenz.pdf

US Executive Order, *Ensuring a National Policy Framework for Artificial Intelligence*, <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/> , 11 décembre 2025, consulté le 4 mars 2026.

Verma Pranshu, « The rise of AI fake news is creating a 'misinformation superspreader' », *The Washington Post*, December 17, 2023.

Vries-Gao Alex de, « The carbon and water footprints of data centers and what this could mean for artificial intelligence », *Patterns*, 17 décembre 2025, p. 101430.

Wassmer Pascal, *La France veut migrer de Windows à Linux pour sa souveraineté numérique*, <https://www.rts.ch/info/monde/2026/article/la-france-abandonne-windows-pour-linux-une-question-de-souverainete-29209373.html> , 11 avril 2026, consulté le 21 avril 2026.

Wiggins Kaye et Indap Sujeet, « Elite law firm Sullivan & Cromwell admits to AI 'hallucinations' », *Financial Times*, 21 avr. 2026 p.

Wyssat Michael, 25_POS_36 - *Pour une stratégie cantonale de gestion souveraine du cloud et des données*, <https://www.vd.ch/gc/seances-du-grand-conseil/point-seance/point/0f567d48-7d88-4781-b91a-fa9517472457/meeting/1029644> , 25 novembre 2025, consulté le 18 mars 2026.

Wyssat Michael, 24_POS_57 - *Intégration de l'IA dans l'administration cantonale d'ici 2035: Quels défis et transformations pour la santé, la justice et l'enseignement?*, <https://www.vd.ch/gc/seances-du-grand-conseil/point-seance/point/a9c346c7-7696-4112-9225-d5a575c26eeb/meeting/1026866> , novembre 2024, consulté le 18 mars 2026.

Wyttenbach Judith, *Umsetzung von Menschenrechtsübereinkommen in Bundesstaaten: Gleichzeitig ein Beitrag zur grundrechtlichen Ordnung im Föderalismus*, Zurich (Dike) 2017. (cité : Wyttenbach, p....)

Yoon June, « Is an AI price war about to begin? », *Financial Times*, 19 févr. 2026 p.

Zuboff Shoshana, *The age of surveillance capitalism: the fight for the future at the new frontier of power*, London, Profile Books, 2019, 691 p.