

RÉCUPÉRER LA CONFIDENTIALITÉ À L'ÈRE DE L'IA : **LA PROTECTION DES DONNÉES PERSONNELLES EN TANT QUE BIEN PUBLIC**

Un appel à la responsabilité partagée
et à un renforcement des mesures de
protection afin de préserver la confidentialité
des consommateurs à l'ère du numérique.

L'INTELLIGENCE ARTIFICIELLE REND LES CHOIX INDIVIDUELS EN MATIÈRE DE CONFIDENTIALITÉ INSUFFISANTS

Il y a cinquante ans, les données personnelles relevaient en grande partie de la sphère privée par principe.ⁱ Aujourd'hui, ces données peuvent être partagées, vendues ou échangées instantanément, avec ou sans votre consentement. Le mouvement mondial des consommateurs réclame des mesures urgentes pour protéger votre confidentialité.

Les consommateurs ont besoin de protections collectives plus solides pour garantir que les données à caractère personnel soient utilisées de manière responsable, transparente et équitable à l'ère de l'intelligence artificielle.

La confidentialité ne peut plus être gérée uniquement par le biais de choix individuels. Sa protection devrait être une responsabilité partagée, et non un devoir individuel.

LE PROBLÈME: LES CONSOMMATEURS DOIVENT GÉRER LES RISQUES SYSTÉMIQUES LIÉS À LA CONFIDENTIALITÉ

La protection de la vie privée est considérée comme relevant de la responsabilité de chacun : lire de longues mentions légales, gérer des paramètres complexes et fournir des données personnelles en échange de la prestation de services numériques.

Cette approche ne reflète plus la manière dont l'intelligence artificielle (IA)ⁱⁱ utilise les données des consommateurs. Les systèmes d'IA sont désormais capables de prédire des informations nous concernant que nous n'avons jamais explicitement partagéesⁱⁱⁱ, avec des conséquences imprévisibles liées aux choix de conception et à l'absence de gouvernance.

Parmi les préjudices potentiels, on peut citer le fait de se voir facturer des tarifs plus élevés, de se voir refuser un crédit ou une assurance, d'être orienté vers des options moins avantageuses ou d'être ciblé en fonction de caractéristiques déduites. Les consommateurs en situation de vulnérabilité sont souvent les plus durement touchés et disposent de très peu de voies de recours.

90% des défenseurs des consommateurs à travers le monde considèrent que la confidentialité et la sécurité constituent les principaux risques liés à l'IA pour les consommateurs.^{iv}

NOTRE OBJECTIF: FAIRE DE LA VIE PRIVÉE UNE PROTECTION COMMUNE

Considérer la confidentialité comme un bien public – à l'instar de la qualité de l'air ou de la sécurité routière – en instaurant des protections qui profitent à tous, au lieu de faire peser la charge sur les particuliers. Notre appel à l'action définit six principes, élaborés conjointement avec les associations de consommateurs, pour promouvoir la défense des consommateurs, instaurer des pratiques commerciales responsables et soutenir un renforcement de la législation.

L'objectif est simple : veiller à ce que personne ne puisse utiliser nos données pour nous faire payer plus cher, nous exclure de manière abusive ou exploiter nos vulnérabilités. Adopter une approche axée sur l'intérêt général ne signifie pas utiliser moins de données. Cela signifie gérer les données de manière à maximiser les avantages pour la collectivité tout en minimisant les inconvénients.

LE RÉSULTAT: UNE CONFIDENTIALITÉ RENFORCÉE FAVORISE LA CONFIANCE DANS L'ÉCONOMIE NUMÉRIQUE

La protection de la confidentialité est un facteur important pour instaurer la confiance dans l'économie numérique. Des systèmes transparents, responsables et soumis à des exigences de responsabilité réduisent les risques, permettent une utilisation sûre et équitable des données, et donnent aux consommateurs les moyens d'utiliser les services numériques en toute confiance. Des mesures solides de protection de la confidentialité renforcent la confiance des consommateurs et contribuent à garantir que l'innovation profite à tous.

Alors que l'IA permet aux prestataires de collecter, prédire et utiliser toujours plus d'informations, les préoccupations relatives à la confidentialité des données personnelles ne cessent de croître.

Les prestataires qui protègent la confidentialité des données personnelles peuvent bénéficier d'un avantage concurrentiel, mais uniquement lorsque les consommateurs ont réellement la possibilité de choisir, de changer de prestataire et de transférer leurs données chez un autre prestataire.

Définition : Une organisation qui développe ou exploite des systèmes de données à grande échelle, en utilisant des données à caractère personnel pour prendre des décisions, personnaliser des services ou influencer les choix des consommateurs.

QU'EST-CE QUE LA CONFIDENTIALITÉ ET QU'EST-CE QU'UN BIEN PUBLIC ?

CONFIDENTIALITÉ



signifie avoir le contrôle sur la manière dont vos informations et données personnelles sont collectées, utilisées et partagées.^v

UN BIEN PUBLIC



est une ressource ou une situation dont les avantages et les inconvénients sont partagés par l'ensemble de la communauté, ce qui nécessite une gouvernance collective plutôt qu'une gestion individuelle.

LES BIENS PUBLICS ONT DEUX CARACTÉRISTIQUES FONDAMENTALES

NON EXCLUABLE : personne ne peut échapper à son incidence.

NON-RIVALROUS : le bénéfice dont profite une personne ne réduit pas celui des autres.

	EXCLUABLE	NON EXCLUABLE
RIVALISANT	BIENS PRIVÉS  alimentation  vêtements  voitures	BIENS COMMUNS  poisson  bois  charbon
NON-RIVALISANT	PRODUITS DE CLUB  cinémas  gyms  plages privées	BIENS PUBLICS  air pur  sécurité routière

78% des consommateurs américains seraient favorables à une réglementation sur la manière dont les entreprises peuvent collecter, stocker, partager et utiliser nos données personnelles.^{vi}

EXEMPLES DE BIENS COMMUNS



AIR PUR : Personne ne peut échapper à la pollution atmosphérique, et le fait qu'une personne y soit exposée ne réduit en rien l'exposition d'une autre. La société s'appuie sur des mesures de protection collectives, telles que les normes d'émissions et les réglementations en matière de qualité de l'air, plutôt que d'attendre des individus qu'ils gèrent eux-mêmes ce risque.



SÉCURITÉ ROUTIÈRE : routes sûres, véhicules moins dangereux, limitations de vitesse et port de la ceinture de sécurité obligatoire : ces mesures protègent tout le monde, y compris ceux qui choisissent personnellement d'y renoncer. Le consentement individuel n'est pas le principe directeur de la sécurité routière.



LA CONFIDENTIALITÉ n'est pas un bien public au sens strict du terme, mais elle fonctionne de plus en plus comme tel. L'IA engendre des risques qui touchent tout le monde, rendant ainsi les mesures de protection collectives de plus en plus nécessaires.

SIX PRINCIPES POUR FAIRE DE LA CONFIDENCIALITÉ UN BIEN COMMUN

Si la confidentialité est une condition commune plutôt qu'une responsabilité individuelle, nous avons besoin de règles communes qui protègent tout le monde. Notre cadre repose sur six principes:

1 

LES DONNÉES SERVENT AVANT TOUT LES INTÉRÊTS DES CONSOMMATEURS

Les prestataires doivent utiliser les données à caractère personnel d'une manière qui profite aux consommateurs et qui soit conforme à la finalité pour laquelle ces données ont été collectées.

2 

PROTÉGER CONTRE LE PROFILAGE NÉFASTE DE L'IA

Protéger les personnes non seulement contre la collecte excessive de données, mais aussi contre les prédictions et le profilage préjudiciables.

3 

GARANTIR LA RESPONSABILISATION ET UNE APPLICATION EFFICACE DE LA LOI

La protection des consommateurs devrait être intégrée aux systèmes d'IA, aux marchés et aux cadres réglementaires, plutôt que de compter sur les individus pour défendre eux-mêmes leurs droits.

4 

FAVORISER LA SIMPLICITÉ DE LA SORTIE, LA PORTABILITÉ ET UN VÉRITABLE CHOIX

Les consommateurs devraient pouvoir transférer et supprimer leurs données sans aucune entrave.

5 

OBLIGATION DE TESTS PRÉALABLES, DE SUIVI ET D'INTERVENTION HUMAINE

Les systèmes d'IA doivent être testés, surveillés et contrôlés avant et après leur déploiement afin de garantir le respect des mesures de protection de la confidentialité. Les préjudices systémiques pouvant être difficiles à détecter, la surveillance doit se concentrer sur les résultats concrets ainsi que sur le respect des exigences réglementaires.

6 

GARANTIR DES RECOURS ET DES INDEMNISATIONS EFFICACES EN CAS D'ATTEINTES À LA VIE PRIVÉE

Les consommateurs doivent pouvoir comprendre les décisions prises, contester les résultats et obtenir réparation dans des délais raisonnables en cas d'atteinte à la confidentialité.

PROTÉGER ENSEMBLE LA CONFIDENTIALITÉ DES DONNÉES À CARACTÈRE PERSONNEL

L'IA a fait de la confidentialité un enjeu collectif.



De nombreux risques liés à la vie privée sont aujourd'hui de nature collective plutôt qu'individuelle. En effet, l'IA peut en apprendre davantage sur vous à partir d'informations concernant d'autres personnes qui vous ressemblent, même si vous n'avez jamais partagé ces informations vous-même. Considérer la vie privée comme un bien public revient à confier les responsabilités de gouvernance aux acteurs les mieux à même de gérer ces risques collectifs, plutôt que de laisser les consommateurs y faire face seuls.

Les consommateurs ne peuvent pas se protéger seuls.



Même si vous ne partagez pas vos informations personnelles, les fournisseurs peuvent déduire des informations vous concernant à partir des données de votre famille, de vos amis ou de personnes qui vous ressemblent. L'inverse est également vrai : vos données peuvent révéler des informations sur d'autres personnes qui n'ont elles-mêmes rien partagé. La vie privée est donc une condition partagée. Aucun individu ne peut la protéger pleinement – ni y renoncer – à lui seul.

Les entreprises ne peuvent pas résoudre le problème à elles seules.



Même les entreprises qui s'engagent à renforcer leurs pratiques de protection de la vie privée sont confrontées à un problème d'action collective. Agir seul peut constituer un désavantage si les concurrents continuent à collecter et à monétiser des données excessives sur les consommateurs. Des règles communes permettent aux entreprises d'agir de concert sans qu'aucune d'entre elles n'ait à payer le prix d'être la première à franchir le pas.

POURQUOI LA CONFIDENTIALITÉ DEVRAIT-ELLE ÊTRE CONSIDÉRÉE COMME UN BIEN PUBLIC ?

Les plus démunis subissent les plus grands préjudices.



L'IA peut renforcer la discrimination, la manipulation et la classification inéquitable des consommateurs à une échelle qu'aucun individu ne peut identifier ni contester. Les consommateurs en situation de vulnérabilité sont souvent les plus touchés, ce qui accentue les inégalités existantes.^{vii}

La confidentialité est une question d'équité, et non de secret.



La confidentialité ne signifie pas que l'on cache quelque chose. Il s'agit à ce que les informations personnelles ne puissent pas être utilisées pour surfacturer les gens, les exclure abusivement d'opportunités, manipuler leurs choix ou exploiter leurs vulnérabilités. Même des données apparemment inoffensives peuvent être combinées et analysées de manière à influencer la vie des gens d'une façon qu'ils ne verront peut-être jamais ou ne comprendront jamais.

L'autogestion fait porter un lourd fardeau à l'utilisateur.



Les modèles actuels de « notification et consentement » supposent que les consommateurs veillent eux-mêmes à la protection de leur vie privée sur chaque service. Dans la pratique, de nombreux consommateurs ont le sentiment qu'ils n'ont guère d'autre choix que de partager leurs données pour pouvoir accéder aux services numériques. La protection de la vie privée ne devrait pas dépendre de la vigilance de chacun.

L'ÉCONOMIE ACTUELLE DES DONNÉES AXÉE SUR L'IA, EXPOSE LES CONSOMMATEURS À DES RISQUES À CHAQUE ÉTAPE

ÉTAPE 1:



Les données sont collectées à des fins autres que celles de service au consommateur.

Un modèle économique classique considère les données des consommateurs comme une matière première à extraire, à traiter et à monétiser au-delà des intérêts du consommateur. Le partage des données peut apporter de réels avantages, notamment en matière de prévention des escroqueries ou des fraudes,^{viii} et les consommateurs peuvent apprécier la personnalisation lorsqu'elle est pertinente. Cependant, la collecte d'un volume de données supérieur au nécessaire peut être source de préjudice.

EXEMPLE : UNE BANQUE UTILISE DES DONNÉES POUR METTRE FIN À UNE ARNAQUE

Une banque détecte un paiement inhabituel et met fin à une tentative d'escroquerie avant que l'argent ne soit prélevé sur le compte d'un client. Cela protège les consommateurs, car les données sont utilisées dans un but précis. En revanche, la collecte, la réutilisation et l'échange de données sans limites clairement définies suppriment cette protection. Pour que le consommateur en tire un bénéfice, il faut que l'objectif soit clairement défini.

ÉTAPE 2:



Création illicite de données et de profils nouveaux concernant le consommateur.

L'IA exploite les données existantes issues de l'étape 1 pour générer de nouveaux profils comportementaux et des prévisions concernant les individus, y compris des informations qu'ils n'ont jamais explicitement partagées. Ces prévisions évoluent à une vitesse et à une échelle qui dépassent les cadres de consentement individuels, et les mesures de protection existantes ne régissent souvent pas de manière adéquate la manière dont ces prévisions sont élaborées ou utilisées.^{ix}

EXEMPLE : UTILISATION DES DONNÉES D'UN PROGRAMME DE FIDÉLITÉ AU-DELÀ DU CONSENTEMENT

Un consommateur adhère au programme de fidélité d'un supermarché et accepte de recevoir des offres personnalisées. Des années plus tard, ces mêmes données d'achat sont utilisées par un système d'intelligence artificielle pour prédire des caractéristiques sensibles, telles que des risques pour la santé, des difficultés financières ou des changements majeurs dans la vie. Le profil ainsi établi est partagé avec des tiers avec lesquels le consommateur ne s'attendait absolument pas à entrer en contact. Son consentement initial ne couvrait pas la création ni le partage de ce profil comportemental.

ÉTAPE 3:



Les décisions opaques prises par l'IA ont une incidence sur l'accès des consommateurs aux produits et services, sans qu'il n'existe de voie de recours claire.

Les prédictions faites lors de l'étape 2 peuvent influencer les prix, les produits et les opportunités, souvent à l'insu des personnes concernées et sans que celles-ci puissent contester le résultat.^x

EXEMPLE : CALCUL DU TAUX HYPOTHÉCAIRE SANS EXPLICATION

Un consommateur renouvelle son hypothèque et se voit proposer un taux plus élevé que prévu. Plutôt que de s'appuyer sur des facteurs traditionnels – tels que l'âge, le code postal ou l'historique des sinistres –, le système de tarification basé sur l'IA du prêteur analyse un large éventail de données pour prédire le risque et la rentabilité, tirant potentiellement des conclusions sur le consommateur à partir de données personnelles que celui-ci n'a jamais divulguées. Le consommateur ne reçoit aucune explication claire concernant ce taux plus élevé et n'a guère la possibilité de comprendre, de remettre en question ou de contester cette décision.

CONSTRUIRE UNE ÉCONOMIE NUMÉRIQUE QUI PROTÈGE LES CONSOMMATEURS ET OFFRE DES AVANTAGES PLUS LARGES

Une approche axée sur le bien public ne signifie pas que nous avons besoin de moins de données. Cela signifie gérer les données de manière à maximiser les avantages tout en minimisant les inconvénients pour les consommateurs.

CONFIANCE ET PARTICIPATION NUMÉRIQUE



Les consommateurs devraient pouvoir utiliser les services numériques sans avoir l'impression de devoir, en contrepartie, renoncer à leur vie privée. Des protections de base solides permettent de réduire les incertitudes quant à la manière dont les données à caractère personnel sont collectées, utilisées et partagées. Lorsque la confidentialité est protégée par défaut, les consommateurs peuvent participer à l'économie numérique en toute confiance.

EXEMPLE

Un consommateur peut assister à un événement public ou recourir à un service essentiel sans que sa présence ne fasse l'objet d'un suivi, d'un profilage ou d'un ciblage à des fins commerciales sans rapport avec l'événement ou le service en question.

DES MARCHÉS PLUS EFFICACES



Le cadre actuel en matière de protection de la vie privée repose souvent sur le fait que les particuliers identifient les problèmes après que le préjudice a déjà été causé. Une approche axée sur l'intérêt général fait peser la responsabilité sur les prestataires et les régulateurs afin de prévenir les préjudices avant même qu'ils ne surviennent. Des règles claires et une obligation de rendre des comptes apportent une plus grande sécurité tant aux consommateurs qu'aux entreprises.

EXEMPLE

La sécurité alimentaire protège toute personne qui achète des produits alimentaires, et pas seulement celles qui lisent les étiquettes. La protection des données devrait fonctionner de la même manière, avec des mesures de protection intégrées au système plutôt que de compter sur les consommateurs pour gérer eux-mêmes tous les risques.

PLUS DE CHOIX ET D'INNOVATION



Aujourd'hui, les services qui comptent le plus grand nombre d'utilisateurs disposent souvent d'un avantage considérable en matière de données : un volume de données plus important permet d'améliorer les produits, d'affiner le ciblage et de renforcer la position sur le marché. Des mesures solides de protection de la vie privée, associées à des droits effectifs de portabilité et de changement de fournisseur, peuvent offrir à de nouveaux services la possibilité de se démarquer sur la qualité, la confiance et l'innovation plutôt que sur le volume de données qu'ils ont accumulées.

EXEMPLE

Un prestataire proposant des services respectueux de la confidentialité peut se différencier en gagnant la confiance des consommateurs, plutôt qu'en collectant toujours plus de données personnelles.

CROISSANCE ÉCONOMIQUE AVEC CONFIANCE



La confiance est l'un des piliers de l'économie numérique. Lorsque les consommateurs ont l'assurance que leurs données seront utilisées de manière responsable, ils sont, selon nous, plus enclins à adopter de nouvelles technologies et de nouveaux services. Les entreprises bénéficient ainsi de relations clients plus solides, tandis que les innovateurs peuvent développer des produits créateurs de valeur sans avoir recours à des pratiques de collecte de données de plus en plus intrusives. Des mesures communes de protection de la confidentialité permettent également de garantir que les entreprises se font concurrence sur la base de la confiance et de l'innovation, plutôt que sur la quantité de données qu'elles parviennent à extraire des consommateurs.^{xi}

COMMENT Y PARVENIR : LES PRINCIPES FONDAMENTAUX DE LA CONFIDENTIALITÉ EN TANT QUE BIEN PUBLIC

Si la confidentialité relève davantage d'une condition collective que d'une responsabilité individuelle, la gouvernance devrait passer de la gestion des choix des consommateurs à l'orientation du comportement des prestataires et des systèmes. Ces six principes fournissent un cadre permettant d'y parvenir.^{xii}



PRINCIPE 1: LES DONNÉES AU SERVICE DES INTÉRÊTS DES CONSOMMATEURS

Les prestataires doivent utiliser les données à caractère personnel d'une manière qui profite aux consommateurs et qui soit conforme à la finalité pour laquelle ces données ont été collectées.

- **Des critères plus stricts pour les personnes les plus exposées.** Les systèmes d'IA devraient appliquer des protections plus strictes – telles que la désactivation du profilage et du ciblage, ainsi que la mise en place de paramètres de protection par défaut – lors du traitement de données concernant des enfants, des consommateurs âgés ou d'autres personnes susceptibles d'être exposées à des risques.
- **Traitement équitable des données, indépendamment du consentement.** Toute collecte et utilisation de données doivent être loyales et proportionnées, avec ou sans le consentement du consommateur. Le consentement ne doit pas autoriser un traitement abusif susceptible de causer un préjudice ou d'engendrer un risque déraisonnable, de même qu'il ne saurait autoriser le traitement des données d'une autre personne.
- **Utiliser des technologies garantissant la protection de la confidentialité.** Les prestataires devraient privilégier les approches qui apportent une réelle utilité, y compris la personnalisation le cas échéant, sans pour autant nécessiter une collecte massive de données à caractère personnel. La technologie offre déjà cette possibilité.^{xiii}
- **Assurer des normes de sécurité renforcées.** Les prestataires doivent maintenir des normes de sécurité proportionnées au caractère sensible des données qu'ils détiennent et à l'ampleur de leurs activités. Un cadre de protection de la vie privée susceptible d'être compromis par une violation évitable ne sert pas l'intérêt général. Les obligations en matière de sécurité doivent être permanentes et vérifiables.



PRINCIPE 2: PROTECTION CONTRE LE PROFILAGE EN LIGNE

Protéger les personnes non seulement contre la collecte excessive de données, mais aussi contre les prédictions et le profilage abusifs

- **Pas de réutilisation automatique des données pour l'entraînement de l'IA.** Les données collectées dans un but précis ne devraient pas être réutilisées pour entraîner des systèmes d'IA d'une manière qui soit en contradiction avec la législation applicable, les obligations en matière de protection de la vie privée, les engagements contractuels ou les attentes raisonnables des consommateurs. De telles utilisations devraient être réglementées dès le moment de la collecte et soumises à des principes de transparence, de proportionnalité et de contrôle.
- **Limites relatives aux données prédites et aux profils.** Les obligations doivent s'étendre à ce que les systèmes d'IA sont autorisés à prédire et à utiliser pour agir – y compris l'état de santé, la vulnérabilité financière, ainsi que les valeurs ou convictions déduites d'autres informations – et pas seulement aux données collectées. Les limites doivent être proportionnées : plus l'impact potentiel sur l'accès des consommateurs aux services, à l'emploi ou à d'autres conséquences est important, plus les contrôles doivent être stricts.
- **Utilisations interdites et restreintes.** Certaines utilisations des données devraient être interdites, indépendamment du consentement, notamment la prédiction de caractéristiques protégées de manière à permettre une discrimination illégale, un traitement inéquitable, l'exploitation ou la manipulation ; le ciblage fondé sur la vulnérabilité ; ou l'utilisation de profils comportementaux pour manipuler la prise de décision.



PRINCIPE 3: GARANTIR LA RESPONSABILISATION ET L'APPLICATION EFFECTIVE DE LA LOI

La protection des consommateurs doit être intégrée aux systèmes d'IA, aux marchés et aux cadres réglementaires, plutôt que de laisser aux individus le soin de défendre leurs droits.

- **La mise en application nécessite des investissements.** Les organismes de régulation doivent disposer de l'expertise technique, du mandat légal et des ressources nécessaires pour réguler efficacement les systèmes d'IA.
- **Le choix des consommateurs et la protection de la vie privée doivent constituer des priorités réglementaires.** Les cadres réglementaires devraient garantir que le pouvoir de marché ne soit pas utilisé pour empêcher les consommateurs de changer de fournisseur ou pour restreindre leur vie privée et leur liberté de choix, afin que l'échelle profite aux consommateurs plutôt que de renforcer le contrôle sur leurs données.
- **Gouvernance transfrontalière.** Des normes minimales contraignantes en matière de collecte et de traitement des données devraient s'appliquer quel que soit le lieu où une entreprise a son siège social ou où les données sont traitées. L'application transfrontalière de la réglementation et le partage d'informations devraient garantir des protections cohérentes.

COMMENT Y PARVENIR : LES PRINCIPES FONDAMENTAUX DE LA CONFIDENTIALITÉ EN TANT QUE BIEN PUBLIC



PRINCIPE 4: FAVORISER LA SIMPLICITÉ DE LA FIN DE CONTRAT, PORTABILITÉ ET CHOIX RÉEL

Les consommateurs devraient pouvoir transférer et supprimer leurs données sans entrave.

- **Portabilité et compatibilité entre les services.** La portabilité des données et, le cas échéant, l'interopérabilité peuvent favoriser le choix des consommateurs, l'innovation et la confiance lorsqu'elles sont mises en œuvre de manière sécurisée, respectueuse de la confidentialité et proportionnée.^{xiv} Les consommateurs devraient pouvoir choisir les services qui protègent le mieux leur vie privée sans être prisonniers d'un système.
- **Suppression simple du compte.** Les consommateurs devraient pouvoir fermer un compte et faire effacer leurs données à caractère personnel par le biais d'une procédure aussi simple que celle utilisée pour s'inscrire.
- **Retrait du consentement.** Lorsque le traitement repose sur le consentement, les consommateurs devraient pouvoir le retirer aussi facilement qu'ils l'ont donné, à tout moment et sans pénalité.



PRINCIPE 5: OBLIGATION DE TESTS PRÉALABLES, DE SUIVI ET D'INTERVENTION HUMAINE

Les systèmes d'IA doivent être testés, surveillés et audités avant et après leur déploiement afin de garantir le respect des garde-fous en matière de protection de la vie privée. Les préjudices systémiques pouvant être difficiles à détecter, la surveillance doit se concentrer sur les résultats concrets ainsi que sur le respect des exigences réglementaires.

- **Évaluations préalables au déploiement.** Les systèmes d'IA utilisés dans des domaines à fort impact, tels que la santé ou les services financiers, devraient faire l'objet d'évaluations fondées sur les risques avant leur déploiement. L'évaluation devrait être proportionnée au cas d'utilisation, à la sensibilité des données concernées, ainsi qu'à la gravité et à la probabilité d'un préjudice potentiel.^{xv}
- **Intervention humaine.** La surveillance humaine devrait permettre aux prestataires d'identifier, de remettre en question et de corriger les résultats préjudiciables.
- **Audit continu.** Les prestataires doivent surveiller et auditer activement les systèmes d'IA tout au long de leur cycle de vie. Les audits et les tests doivent permettre d'identifier les résultats discriminatoires, les dérives du système, les impacts disproportionnés sur des groupes spécifiques et les préjudices émergents.
- **Rapports de transparence.** Les entités réglementées doivent rendre compte des performances de leurs systèmes par rapport aux normes requises, en rendant les résultats visibles aux autorités de régulation et au public.



PRINCIPE 6: GARANTIR DES RECOURS ET DES INDEMNISATIONS EFFICACES EN CAS D'ATTEINTES À LA PRI

Les consommateurs doivent pouvoir comprendre les décisions, contester les résultats et obtenir réparation en temps opportun en cas d'atteinte à la confidentialité.

- **A Un interlocuteur clair pour les consommateurs.** Chaque juridiction devrait disposer d'un organisme désigné, doté du mandat et des ressources nécessaires pour apporter une aide humaine en matière de plaintes, d'enquêtes et de mise en application de la loi. Les consommateurs doivent savoir vers qui se tourner pour obtenir de l'aide.
- **Des décisions compréhensibles et contestables.** Lorsque l'IA influence des décisions ayant des conséquences importantes, les consommateurs devraient recevoir des explications formulées en des termes que les consommateurs et les régulateurs peuvent comprendre et sur lesquelles ils peuvent agir.
- **Les mesures de dédommagement doivent être à la mesure du préjudice.** Lorsque l'IA porte préjudice à de larges groupes de consommateurs, les mesures de réparation doivent également être mises en œuvre à grande échelle. Les associations de consommateurs et les régulateurs devraient pouvoir intenter des actions collectives au nom de toutes les personnes concernées, plutôt que de laisser les individus chercher seuls à obtenir réparation.^{xvi}

OBTENIR DE MEILLEURS RÉSULTATS POUR LES PARTIES PRENANTES

POUR LES CONSOMMATEURS



Une approche fondée sur le bien public signifie que la protection de la confidentialité ne dépend plus des connaissances, du temps ou des ressources de chaque consommateur. Les personnes sont protégées par le système lui-même. Cela :

- décharge les individus de la gestion des risques systémiques liés à la confidentialité;
- protège contre toute exploitation, quelles que soient les capacités ou les compétences numériques;
- crée des voies efficaces pour contester les décisions prises par l'IA ;
- favorise le choix et l'interopérabilité entre les services ;
- renforce les mécanismes de responsabilité envers les consommateurs.

POUR LE SECTEUR PRIVÉ



Des règles claires sont bénéfiques pour les entreprises. Elles permettent notamment :

- de faire la distinction entre l'utilisation des données qui crée une véritable valeur ajoutée et les pratiques qui se limitent à une simple exploitation ;
- d'instaurer des conditions de concurrence homogènes applicables à l'ensemble du marché ;
- de renforcer la confiance des consommateurs en tant qu'atout concurrentiel, plutôt que de considérer la protection de la vie privée comme un simple coût de mise en conformité.^{xvii}

POUR LES GOUVERNEMENTS



Un cadre fondé sur la notion de bien public donne aux gouvernements les outils nécessaires pour agir de manière proactive, plutôt que de réagir une fois que le préjudice est déjà survenu. Cela :

- permet de passer d'une approche réactive en matière d'application de la loi à des mesures de protection au niveau du système ;
- renforce la confiance du public dans les systèmes numériques et les institutions chargées de leur supervision ;
- fournit une base pour la coopération transfrontalière sur une question qui ne connaît pas de frontières nationales.

UN APPEL COLLECTIF POUR LA RECONNAISSANCE DES DONNÉES À CARACTÈRE PERSONNEL COMME BIEN PUBLIC



BENIN SANTE ET SURVIE
DU CONSOMMATEUR
(BSSC)



UN APPEL COLLECTIF POUR LA RECONNAISSANCE DES DONNÉES À CARACTÈRE PERSONNEL COMME BIEN PUBLIC

CONSUMER VOICE



epic.org / ELECTRONIC
PRIVACY
INFORMATION
CENTER

**FIJIAN
COMPETITION &
CONSUMER
COMMISSION**

idec
instituto de defesa
de consumidores



koodos

FORBRUKERRÅDET

မြန်မာစားသုံးသူများသမဂ္ဂ
**MYANMAR
CONSUMERS UNION**
Rights and Responsibilities thru Education



ONPECO
OBSERVATORIO NACIONAL
PARA LA PROTECCIÓN DEL CONSUMIDOR

LEMBAGA KONSUMEN YOGYAKARTA
YOGYAKARTA CONSUMER INSTITUTE

**PARADIGM
INITIATIVE**

**Privacy
Foundation**

Proconsumer



**SVERIGES
KONSUMENTER**
THE SWEDISH CONSUMERS' ASSOCIATION

**SOUTH SUDAN
CONSUMER
PROTECTION
ORGANIZATION**

ttc
สภาองค์กรของผู้บริโภค
Thailand Consumers Council

**TheNetwork
for Consumer Protection**

TRIBUNAL
ECUATORIANA DE
CONSUMIDORES
Y USUARIOS

**VOICES OF
PRIVACY**



SIGNATORIES

Le document intitulé " Récupérer la confidentialité à l'ère de l'IA : la protection des données personnelles en tant que bien public " est soutenu par les organisations suivantes :

ORGANISATION	PAYS
Acción del Consumidor (ADELCO)	Argentine
Association for the Defence of Consumers and the Environment (ADEC - Association pour la Défense de l'Environnement et des Consommateurs)	Sénégal
Benin Health and Consumers' Survival (BSSC - Bénin Sante et Survie du Consommateur)	Bénin
Brazilian Institute of Consumer Protection (IDEC - Instituto Brasileiro de Defesa do Consumidor)	Brésil
Bulgarian National Association Active Consumers (BNAAC)	Bulgarie
Consumer Advocacy and Empowerment Foundation of Nigeria (CADEF)	Nigéria
Consumer Association of Mauritius (ACIM - Association des Consommateurs de l'Ile Maurice)	Maurice
Consumer Council of Fiji	Fidji
Consumer Defence Association (ADECO - Associação para Defesa do Consumidor)	République du Cap-Vert
Consumer Defence Group of Mali (REDECOMA - Regroupement pour la défense des consommateurs du Mali)	Mali
Consumer Education and Research Centre (CERC)	Inde
Consumer NZ	Nouvelle-Zélande
Consumer Policy Research Centre (CPRC)	Australie
Consumer Protection Association of Mercosur (PROCONSUMER - Asociación de Protección de los Consumidores del Mercosur)	Argentine
Consumer Protection Association	Koweït
Consumer Reports	États-Unis
Consumer Unity and Trust Society (CUTS)	Inde
Consumer VOICE	Inde
Consumers Association of Bangladesh	Bangladesh
Consumers Council of Canada	Canada
Consumers Japan	Japon
Electronic Privacy Information Center (EPIC)	États-Unis

ORGANISATION	PAYS
Empower India	Inde
Federation of Consumers and Users (CECU - Federación de Consumidores y Usuarios)	Espagne
Fijian Competition & Consumer Commission (FCCC)	Fidji
Fundación Ambio	Costa Rica
Hong Kong Consumer Council	Hong Kong
Kenya Consumers Organisation	Kenya
Koodos Labs	États-Unis
Myanmar Consumers Union	Myanmar
National Observatory for Consumer Protection (ONPECO)	République Dominicaine
Norwegian Consumer Council (Forbrukerrådet)	Norvège
Privacy Foundation NZ	Nouvelle-Zélande
Paradigm Initiative	Nigéria
South Sudan Consumer Protection Organisation (SSCPO)	Soudan du Sud
Swedish Consumers' Association (Sveriges Konsumenter)	Suède
Thailand Consumer Council	Thaïlande
The Network for Consumer Protection	Pakistan
Tribune of Consumers and Users of Ecuador (Tribuna Ecuatoriana de Consumidores y Usuarios)	Équateur
Tunisian Organisation to Inform the Consumer (OTIC - l'Organisation Tunisienne pour Informer le Consommateur)	Tunisie
Voices of Privacy	États-Unis
Yayasan Lembaga Konsumen Indonesia	Indonésie
Yemen Association for Consumer Protection	Yémen
Yogyakarta Consumer Institute (Lembaga Konsumen Yogyakarta)	Indonésie

REMERCIEMENTS

Nous tenons à remercier nos collègues de Consumers International qui ont participé à la rédaction et à l'élaboration de ce document, notamment : Erin Parsons, Nandini Harihareswara, Alexandra Straessle, Stefan Hall et Brooke Kingsland.

Ce document a été élaboré par Consumers International avec les conseils et la contribution d'un groupe consultatif multipartite sur l'IA, ainsi que de plusieurs partenaires externes. La liste des organisations participantes figure ci-dessous.

Nous remercions tous les contributeurs pour leurs précieuses réflexions et leurs commentaires, tout en précisant que les principes présentés ici ne reflètent pas nécessairement les points de vue individuels de toutes les organisations impliquées.

ORGANISATION
Amazon.com, Inc.
Consumentenbond NL
Consumer Policy Research Centre (CPRC)
Consumer Reports
Danish Consumer Council
DuckDuckGo
Javier Ruiz Diaz
Jeannie Paterson, PhD
Koodos Labs
Que Choisir Ensemble
Visa, Inc.

Consumers International rassemble plus de 200 organisations membres dans plus de 100 pays afin de renforcer l'autonomie des consommateurs et de défendre leurs droits partout dans le monde. Nous sommes leur voix au sein des instances internationales de décision et sur le marché mondial, afin de garantir qu'ils soient traités en toute sécurité, de manière équitable et honnête.

Consumers International est un organisme caritatif (n° 1122155) et une société à but non lucratif à responsabilité limitée par garantie (n° 04337865) enregistrée en Angleterre et au Pays de Galles.

consumersinternational.org

🐦 @consumers_int

f /consumersinternational

- i Rule, J, *Private Lives and Public Surveillance: Social Control in the Computer Age* (1974). Londres : Schocken Books.
- ii Dans le cadre de ce rapport, l'intelligence artificielle (IA) désigne la capacité cognitive d'agents automatiques qui imite la cognition humaine dans le traitement de l'information et l'exécution de tâches pour lesquelles l'agent automatique a été formé. Banque mondiale, *Glossaire GovTech*. Disponible à l'adresse : <https://www.worldbank.org/en/programs/govtech/gtmi/gtmi-glossary>
- iii Le secteur de la publicité numérique utilise des taxonomies normalisées pour classer les personnes et les contenus avec lesquels elles interagissent, publiées par l'Interactive Advertising Bureau (IAB) Tech Lab. La taxonomie des contenus définit environ 700 catégories décrivant le sujet d'une page ou d'une application, tandis que la taxonomie des audiences classe les consommateurs en plus de 1500 segments ciblés selon des critères démographiques, d'intérêts et d'intention d'achat, y compris des données sensibles pouvant être partagées, échangées et synchronisées entre différents services numériques. Ces catégories peuvent également servir à déduire des caractéristiques plus spécifiques. IAB Tech Lab, *Taxonomie des audiences et Taxonomie des contenus*. Disponible à l'adresse : <https://iabtechlab.com/standards/#taxonomies>
- iv Consumers International, *Enquête mondiale sur l'IA* (2025).
- v Dans son ouvrage fondateur de 1967, Alan Westin définissait la confidentialité comme « le droit des individus, des groupes ou des institutions de déterminer eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées ». Westin, A., *Privacy and Freedom* (1967). New York : Atheneum.
- vi Consumer Reports, *Enquête sur les expériences des consommateurs américains : une enquête multimodale représentative à l'échelle nationale* (2024). Disponible à l'adresse : https://article.images.consumerreports.org/image/upload/v1728423752/prod/content/dam/surveys/Consumer_Reports_AES_September_2024.pdf
- vii Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), *Recommandation sur l'éthique de l'intelligence artificielle* (2022). Disponible à l'adresse : <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- viii Consumers International, *Mettre fin aux escroqueries en ligne : renforcer la cohérence et la coordination au service des consommateurs* (2026). Disponible à l'adresse : <https://www.consumersinternational.org/media/699948/consumers-international-stopping-online-scams-building-consistency-and-coordination-for-consumers.pdf>
- ix Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), *Le droit à la confidentialité à l'ère numérique : rapport* (2021). Disponible à l'adresse : <https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>
- x Conférence des Nations Unies sur le commerce et le développement (CNUCED), *Intelligence artificielle et protection des consommateurs* (2024), p. 12-13. Disponible à l'adresse : https://unctad.org/system/files/information-document/ccpb_artificial_intelligence_consumer_protection_en.pdf
- xi Organisation de coopération et de développement économiques (OCDE), *L'intersection entre la concurrence et la protection des données* (2024). Disponible à l'adresse : https://www.oecd.org/en/publications/2024/06/the-intersection-between-competition-and-data-privacy_b5ac1ae6.html
- xii Ces principes varient en fonction de la taille, du risque et de l'impact : les principes appliqués à un fournisseur dominant traitant des données sensibles à grande échelle ne sont pas les mêmes que ceux appliqués à un petit fournisseur ou à une utilisation à faible risque.
- xiii Il est possible de concevoir des systèmes capables d'apprendre des modèles sans centraliser les données de chaque individu, de répondre à des questions utiles sans exposer aucune personne et de conserver les informations sensibles sur l'appareil même du consommateur. Par exemple, l'apprentissage fédéré permet d'entraîner un modèle sur plusieurs appareils ou au sein de plusieurs organisations, de sorte que seules les connaissances acquises soient transmises au développeur, et non les données personnelles sous-jacentes. La confidentialité différentielle ajoute une quantité calibrée de bruit aux résultats, de sorte que les tendances utiles restent visibles sans qu'aucune personne ne puisse être identifiée à partir de celles-ci. Le traitement sur appareil conserve l'analyse sur le téléphone ou l'ordinateur du consommateur lui-même, de sorte que les informations sensibles n'atteignent jamais les serveurs d'une entreprise. Bureau du commissaire à l'information (ICO), *Guide sur les technologies renforçant la confidentialité* (2023). Disponible à l'adresse : <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/>
- xiv Data Transfer Initiative, *Une voie à suivre pour la portabilité de l'IA* (2025). Disponible à l'adresse : <https://dtinit.org/blog/2025/08/26/path-forward-AI-portability>
- xv Il convient de noter que plusieurs des thèmes abordés dans ce principe sont couverts par la réglementation européenne en vigueur.
- xvi Les voies de recours des consommateurs impliquent une communication claire des droits et des responsabilités, ainsi que des canaux de réclamation accessibles. Il convient de garantir un règlement rapide grâce à des mécanismes de recours obligatoires qui attribuent la responsabilité à ceux qui sont les mieux placés pour gérer un risque donné.
- xvii CGAP, « *La protection des données est-elle bénéfique pour les entreprises ?* » (2023). Disponible à l'adresse : <https://www.cgap.org/research/publication/is-data-privacy-good-for-business>