KELDARX

01

WHITE PAPER · B2C

Vos données vous appartiennent. Vraiment ?

Ce que les GAFAM ne vous disent pas sur votre vie numérique

Pascal NAPARTY · PDG & Fondateur, KELDARX

Juin 2026 · Temps de lecture : 12 min

En résumé

‣ Vous utilisez des dizaines d'applications Cloud qui stockent vos données sur des serveurs que vous ne contrôlez pas.

‣ Le Cloud Act américain (2018) autorise les autorités américaines à accéder à vos données, même hébergées en Europe.

‣ Vos données personnelles représentent une valeur économique considérable — exploitée par les plateformes, pas par vous.

‣ Trois risques majeurs menacent votre vie numérique : la captivité, l'exposition et la fragmentation.

‣ Le RGPD, la Loi 25 québécoise et le Cyber Resilience Act vous donnent des droits. Les exercer reste complexe dans les faits.

‣ L'architecture Local-First rend désormais possible la souveraineté numérique individuelle — sans compétences techniques.

‣ KEY est la première plateforme qui vous donne la propriété physique et mathématique de vos actifs numériques.

Introduction : L'illusion de la propriété numérique

Quand avez-vous lu les conditions générales d'utilisation de votre dernière application installée ?

La plupart d'entre nous ne le font jamais. Et c'est précisément sur ce silence que repose l'un des transferts de valeur les plus discrets de l'histoire économique moderne.

Chaque jour, vous créez, partagez et stockez des données : photos, documents, messages, positions géographiques, habitudes de consommation, données de santé, informations financières. Vous avez l'impression que ces données vous appartiennent. Elles sont dans "votre" Cloud, sur "votre" téléphone, dans "votre" compte.

La réalité juridique et technique est différente.

En cliquant "J'accepte", vous avez accordé des droits étendus sur ces données à des entreprises dont vous ne connaissez ni les actionnaires, ni les serveurs, ni les contrats avec les gouvernements.

Ce white paper vous explique ce que cela signifie concrètement — et comment reprendre le contrôle.

1. Ce que vous avez signé sans le lire

Les plateformes numériques les plus utilisées au monde partagent un modèle économique commun : vous êtes le produit.

Ce n'est pas une métaphore. C'est une réalité commerciale documentée.

Vos données alimentent des algorithmes de ciblage publicitaire, des modèles d'entraînement d'intelligence artificielle, des analyses comportementales vendues à des tiers. La valeur de vos données ne disparaît pas une fois votre session terminée. Elle s'accumule, se croise, se monétise.

Ce que vous avez réellement accepté

En validant les conditions générales d'utilisation (CGU) de la plupart des plateformes grand public, vous avez typiquement accordé :

- Le droit d'utiliser vos données pour "améliorer les services" — formulation qui couvre l'entraînement des IA.
- Le droit de partager vos données avec des "partenaires" non nommés.
- Le droit de conserver vos données après la fermeture de votre compte.
- Le droit de modifier ces conditions unilatéralement, avec une simple notification.

Le Cloud Act : quand vos données deviennent américaines

En 2018, les États-Unis ont adopté le **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act). Cette loi autorise les autorités américaines à exiger l'accès aux données stockées par des entreprises américaines, **quelle que soit la localisation physique des serveurs**.

Vos données hébergées sur Google Drive, iCloud, Dropbox ou OneDrive — même sur des serveurs européens — sont potentiellement accessibles aux autorités américaines sans notification préalable [1].

Le Conseil d'État français et la Cour de Justice de l'Union Européenne ont tous deux identifié cette loi comme incompatible avec les droits fondamentaux européens. La tension juridique persiste, sans résolution définitive à ce jour.

Point de vue KELDARX

La question n'est pas de savoir si vous avez quelque chose à cacher. La question est de savoir si vous acceptez que d'autres décident à votre place ce qui vous appartient.

2. Vos données ont une valeur que vous ne percevez pas

L'économie de la donnée personnelle est l'une des industries les plus rentables du XXIe siècle.

Le paradoxe de la valeur

Vous produisez une matière première précieuse. Vous la livrez gratuitement. D'autres la monétisent. Vous n'en percevez aucun retour.

Ce modèle est rendu possible par deux mécanismes :

1. **L'invisibilité** — vous ne voyez pas vos données "partir"
2. **La valeur de l'accès immédiat** — vous acceptez le contrat car le service est pratique maintenant

Ce modèle a un chiffre concret. Selon le rapport financier annuel 2023 de Meta Platforms, Inc. — publié obligatoirement auprès des autorités boursières américaines et accessible au public [2] :

Région	Revenus générés par utilisateur et par an
États-Unis & Canada	~210 à 220 $
Europe	~75 à 80 $
Asie-Pacifique	~18 à 20 $
Reste du monde	~13 à 15 $
Moyenne mondiale	**~40 à 45 $**

Ces revenus sont générés **presque exclusivement grâce à la publicité ciblée**, elle-même alimentée par l'analyse fine de vos données personnelles et de vos comportements en ligne.

En Europe, votre vie numérique vaut environ **75 à 80 $ par an pour Meta**. Vous n'en percevez aucun centime. Vous payez avec votre intimité.

La crise de confiance est documentée

Selon l'**Edelman Trust Barometer 2025**, la confiance envers les grandes entreprises technologiques atteint un niveau historiquement bas dans les pays développés [3]. Les utilisateurs sont de plus en plus conscients de l'exploitation de leurs données — mais se sentent sans alternative viable.

Ce sentiment d'impuissance est la principale barrière à la reprise de contrôle.

> KEY est conçu pour lever cette barrière.

La captivité invisible

Vos photos sur iCloud. Vos emails sur Gmail. Vos documents sur Google Drive. Vos contacts sur votre téléphone Android. Chaque service vous rend un peu plus dépendant — et un peu plus difficile à quitter.

Ce phénomène a un nom dans l'industrie : le **vendor lock-in**. Il n'est pas accidentel. Il est conçu.

3. Les 3 risques que vous sous-estimez

Ces risques entraînent des conséquences concrètes sur votre vie quotidienne et votre avenir numérique.

Risque 1 — La captivité sans sortie de secours

Que se passe-t-il si une plateforme désactive votre compte ? Si elle augmente ses tarifs ? Si elle ferme le service ?

Ces scénarios ne sont pas hypothétiques :

- Des comptes sont désactivés sans préavis pour violation présumée des CGU.
- Des services sont arrêtés unilatéralement (Google+ fermé, Google Stadia abandonné, Google Photos modifié).
- Les prix des abonnements Cloud ont augmenté significativement entre 2022 et 2025 [4].

Quand cela arrive, vos données sont-elles récupérables ? Dans quel format ? Dans quel délai ? La réponse dépend de la bonne volonté d'une entreprise dont les intérêts ne sont pas alignés avec les vôtres.

Risque 2 — L'exposition à votre insu

Vos données ne sont pas seulement collectées. Elles peuvent être exposées.

Les violations de données (data breaches) touchent des centaines de millions d'utilisateurs chaque année. Les données compromises sont revendues sur des marchés parallèles, croisées avec d'autres sources, utilisées pour des fraudes à l'identité.

La réglementation progresse :

- Le **RGPD** européen (2018) impose des obligations strictes aux entreprises et vous confère des droits (accès, rectification, effacement, portabilité) [5].
- La **Loi 25** québécoise (2023) impose des sanctions pouvant atteindre **25 M$ ou 4% du chiffre d'affaires mondial** [6].
- Le **Cyber Resilience Act** (CRA, Commission Européenne, 2024) impose des standards de sécurité aux logiciels commercialisés en Europe [7].
- La **Directive NIS 2** responsabilise pénalement les dirigeants en cas de négligence sur la sécurité des données [8].

Ces textes protègent vos droits. Ils ne réparent pas une fuite de données déjà survenue.

> **Point de vue KELDARX**
>
> La conformité réglementaire protège les entreprises de sanctions. Elle ne protège pas vos données. La protection de vos données commence par vous.

Risque 3 — La fragmentation et la perte de contrôle

Le troisième risque est le plus insidieux car il est graduel.

Chaque nouvelle application installée. Chaque nouveau service activé. Chaque nouvelle permission accordée. Votre vie numérique se fragmente en dizaines de silos détenus par autant d'entreprises différentes.

Résultat : vous ne savez plus où sont vos données, qui y accède, et ce qui se passe avec elles. Cette fragmentation a un coût réel :

- Temps perdu à retrouver une information dispersée entre plusieurs outils.
- Versions multiples d'un même document impossibles à réconcilier.
- Impossibilité de reconstruire un historique personnel cohérent.
- Charge mentale administrative croissante.

Les chiffres sont accablants :

- Selon le **McKinsey Global Institute**, les travailleurs du savoir passent en moyenne **1,8 heure par jour** — soit près de **20 % de leur semaine de travail** — à rechercher des informations, des documents ou à solliciter des collègues pour trouver la bonne donnée [9].
- L'IDC (International Data Corporation) estime ce temps à 2,5 heures par jour, soit 30 % du temps de travail, souvent sans trouver l'information cherchée [10].
- **Gartner** souligne que près de **la moitié des professionnels** admettent avoir régulièrement des difficultés à localiser le bon document au bon moment — conduisant à recréer des documents qui existent déjà [11].

Ce n'est pas un problème d'organisation personnelle. C'est la conséquence directe d'une vie numérique fragmentée entre des dizaines de silos non connectés.

4. La souveraineté numérique n'est plus réservée aux États

Pendant longtemps, la souveraineté numérique était un concept géopolitique. Les États débattaient de l'hébergement de leurs données publiques et de leur indépendance vis-à-vis des hyperscalers américains.

Ce débat descend aujourd'hui au niveau de l'individu.

Trois ruptures convergent simultanément pour rendre possible la souveraineté numérique personnelle.

Rupture 1 — La maturité réglementaire

Le RGPD, la Loi 25, le CRA, le Data Act européen convergent vers un principe fondamental : **vos données vous appartiennent, et vous avez le droit de les contrôler**.

Ces textes ne sont pas que des obligations pour les entreprises. Ce sont des droits pour vous :

- **Droit d'accès** : obtenir une copie de toutes les données détenues sur vous.
- **Droit de rectification** : corriger des données inexactes.
- **Droit à l'effacement** : demander la suppression de vos données.
- **Droit à la portabilité** : récupérer vos données dans un format réutilisable.
- **Droit d'opposition** : refuser certains usages de vos données.

Le problème : exercer ces droits reste complexe dans les faits. La plupart des individus ne le font jamais. KEY automatise cette démarche.

Rupture 2 — La maturité technologique du Local-First

L'architecture **Local-First** est un paradigme technologique qui inverse le modèle Cloud dominant : vos données sont stockées et traitées en priorité sur vos propres appareils. La synchronisation Cloud est optionnelle et sous votre contrôle total.

Cette approche n'était pas praticable à grande échelle il y a cinq ans. Les avancées en matière de bases de données légères (SQLite), de chiffrement embarqué fort et de synchronisation sélective la rendent désormais accessible au grand public.

Le **WEF Global Risks Report 2025** identifie la dépendance aux infrastructures logicielles étrangères comme une faille systémique [12]. Ce que les États commencent à adresser pour leur propre souveraineté, les individus peuvent désormais l'adresser pour eux-mêmes.

Rupture 3 — La demande de souveraineté comme standard

Les chiffres sont sans équivoque :

- **81 %** des adultes estiment n'avoir que peu ou pas de contrôle sur les données collectées par les entreprises technologiques [13].
- **79 %** des utilisateurs sont préoccupés par la manière dont les entreprises utilisent les données qu'elles collectent [13].
- **71 %** des personnes interrogées craignent que la collecte et la monétisation de leurs données personnelles constitue un risque pour leur vie privée [14].
- L'**Edelman Trust Barometer** enregistre depuis plusieurs années une baisse constante de la confiance du public envers les réseaux sociaux et les grandes plateformes technologiques. La protection de la vie privée et la cybersécurité sont désormais les priorités absolues des utilisateurs pour restaurer cette confiance [3].

La demande de souveraineté numérique existe, massive et documentée. L'offre adaptée, jusqu'à présent, manquait.

> **Point de vue KELDARX**
>
> La souveraineté numérique individuelle n'est pas un luxe technophile. C'est la prochaine étape logique de la protection de vos droits fondamentaux à l'ère numérique.

5. Reprendre le contrôle sans être ingénieur

La principale objection est souvent : *"c'est trop technique pour moi".*

Cette objection était légitime en 2015. Elle ne l'est plus en 2026.

Le no-code change la donne

Les plateformes de gestion de données modernes éliminent la barrière technique. Vous n'avez pas besoin de comprendre comment fonctionne une base de données pour en utiliser une. Vous n'avez pas besoin de configurer un serveur pour bénéficier d'une architecture Local-First.

L'analogie est simple : vous conduisez une voiture sans comprendre le moteur à combustion. Vous utilisez un smartphone sans programmer d'application. Vous pouvez gérer souverainement vos données sans être développeur.

Ce que la souveraineté numérique concrète signifie

Modèle GAFAM (aujourd'hui)	Modèle KEY (demain)
Vos données sur leurs serveurs	Vos données sur vos appareils
Accès révocable unilatéralement	Accès permanent et inconditionnel
Monétisation de vos comportements	Aucune exploitation commerciale
Fragmentation en dizaines de silos	Centralisation souveraine
Conformité dépendante d'un tiers	Conformité native et vérifiable

KEY : la plateforme de souveraineté individuelle

KEY est construite sur trois piliers non négociables :

1. **Local-First** — vos données restent physiquement chez vous par défaut — on-premises ou Cloud selon vos besoins
2. **No-Code** — aucune compétence technique requise pour une gouvernance complète de vos données
3. **Architecture ouverte** — aucun vendor lock-in possible, portabilité totale garantie

> KEY n'est pas une alternative à un service Cloud existant. C'est une rupture de paradigme : vous passez de locataire de vos données à propriétaire.

Conclusion : La question que vous devriez vous poser aujourd'hui

Vos données sont-elles en sécurité ? Probablement pas autant que vous le croyez.

Avez-vous le contrôle de vos données ? Probablement moins que vous ne le pensez.

Pouvez-vous reprendre ce contrôle sans tout réapprendre ? Oui — et c'est précisément ce que KEY rend possible.

La souveraineté numérique n'est pas une question technique. C'est une question de choix.

Le monde réglementaire (RGPD, Loi 25, NIS 2, CRA) vous donne les droits. La technologie (Local-First, no-code) vous donne les outils. KEY vous donne la plateforme.

Il ne manque plus que votre décision.

Sources & références

[1] CLOUD Act (Clarifying Lawful Overseas Use of Data Act), Congrès américain, 2018 — congress.gov

[2] Meta Platforms, Inc. — Form 10-K 2023 (rapport annuel déposé auprès de la SEC) / Earnings Releases 2023 — investor.fb.com

[3] Edelman Trust Barometer 2025 — edelman.com/trust/2025-trust-barometer

[4] MacRumors — "Apple Hikes iCloud+ Subscription Prices in Many Countries Around the World" (juin 2023) — macrumors.com · Microsoft — Annonce hausse Microsoft 365 Personal et Family (octobre 2024)

[5] RGPD — Règlement (UE) 2016/679 du Parlement Européen et du Conseil, 27 avril 2016, Art. 15-21 — eur-lex.europa.eu

[6] Loi 25 sur la protection des renseignements personnels dans le secteur privé, Gouvernement du Québec, 2023 — legisquebec.gouv.qc.ca

[7] Cyber Resilience Act (CRA), Règlement (UE) 2024/2847, Commission Européenne — digital-strategy.ec.europa.eu

[8] Directive NIS 2 (UE 2022/2555), Commission Européenne — digital-strategy.ec.europa.eu

[9] McKinsey Global Institute — "The social economy: Unlocking value and productivity through social technologies" — mckinsey.com

[10] IDC (International Data Corporation) — Étude sur le temps de recherche de l'information en entreprise — idc.com

[11] Gartner — Enquête sur la localisation des documents professionnels — gartner.com

[12] WEF — Global Risks Report 2025, World Economic Forum — weforum.org/publications/global-risks-report-2025/

[13] Pew Research Center — "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" — pewresearch.org

[14] YouGov & Amnesty International — Enquête multinationale sur la surveillance et la vie privée numérique — amnesty.org

Toutes les marques, noms de produits et logos mentionnés dans ce document sont la propriété de leurs détenteurs respectifs. Leur mention est purement informative et ne constitue aucune forme d'affiliation ou d'approbation.

À propos de KELDARX

KELDARX développe KEY, la première plateforme qui donne à chacun les capacités technologiques que seuls les grands industriels pouvaient s'offrir.

KEY repose sur trois piliers : l'architecture Local-First (vos données sur vos appareils par défaut — on-premises ou Cloud selon vos besoins, toujours sous votre contrôle), le déterminisme mathématique (résultats 100 % prévisibles et vérifiables — l'IA assiste, elle ne décide jamais), et une base de données obscurcie qui rend vos actifs numériques invisibles aux accès non autorisés — ransomware inclus. Ses solutions métiers à venir permettront pour la première fois aux particuliers et aux entreprises de partager la même infrastructure souveraine pour contrôler leur vie numérique.

Your Digital Life. Your rules.

Pascal Naparty — PDG & Fondateur, KELDARX

Passez à l'étape suivante

Rejoignez la liste d'attente KEY — soyez parmi les premiers à reprendre le contrôle de votre vie numérique.

→ keldarx.com

Pour toute question : **contact@keldarx.com**