Guide sur les données externalisées

COMPRENDRE, ÉVALUER ET MAÎTRISER LES RISQUES DES RÉGLEMENTATIONS EXTRATERRITORIALES

Contributeurs

L'élaboration de ce document est rendue possible grâce au savoir-faire d'AFNOR Normalisation en matière de coordination de travaux multipartites et de rédaction de guides pratiques.
Son contenu n'engage que ses auteurs.

Coordinateur :

Aubin MINESI, *Chef de Projet Normalisation Numérique*

Auteurs :

HEXATRUST • Dorothée DECROP, *Déléguée Générale*
DOCAPOSTE • Séverine DENYS, *Directrice des Affaires Institutionnelles*
OUTSCALE, Dassault Systèmes • David CHASSAN, *Directeur de la Stratégie*
FNTC • François-Luc DOYEZ, *Délégué Général*
OVHCLOUD • Elisa SHARPS, *Chargée d'Affaires Publiques*
WIMI • Timothée DEMOURES, *Chef de Cabinet*
ERCOM • Romain WALLER, *Directeur Business Unit*
NUMSPOT • Servane AUGIER, *Directrice des Affaires Publiques*
LEVIIA • William MÉAUZOONE, *Co-Fondateur*
CLEVER CLOUD • Axel LANIEZ, *Responsable des Affaires Publiques*

Synthèse

Le recours croissant aux services cloud a profondément transformé la gestion des données des organisations. **Si l'externalisation offre des gains indéniables en matière d'agilité et de performance, elle introduit également des risques juridiques majeurs – souvent sous-estimés – liés à l'application de réglementations à portée extraterritoriale.**

La localisation des données ne garantit pas leur protection juridique.

Dans le cloud, les données sont mobiles. Ce n'est donc pas leur lieu d'hébergement qui détermine le droit applicable, mais la juridiction à laquelle est soumis le prestataire. Des données hébergées en Europe peuvent ainsi être légalement accessibles à des autorités étrangères, parfois sans information ni contrôle du client.

Le risque juridique est un risque stratégique.

L'exposition des données à des législations extraterritoriales implique que celles-ci peuvent être réquisitionnées, consultées ou exploitées dans une logique de guerre économique ou à d'autres fins. Une telle situation est susceptible de compromettre la protection de données sensibles, de porter atteinte au secret des affaires et de, in fine, fragiliser les activités d'une organisation.

La maîtrise du risque passe par une démarche structurée.

Toute stratégie d'externalisation doit reposer sur :

- une classification préalable des données selon leur sensibilité et leur criticité ;
- une analyse juridique approfondie des prestataires et de leur chaîne de sous-traitance ;
- une évaluation de compatibilité entre les réglementations applicables ;
- des exigences contractuelles renforcées en matière de transparence, de réversibilité et de notification.

Les référentiels de confiance sont des leviers essentiels.

Les qualifications et certifications participent concrètement à la création d'un cadre de protection vis-à-vis des lois extraterritoriales qui seraient incompatibles avec le droit européen. Elles constituent des outils opérationnels de sécurisation juridique et de pilotage des risques.

En conclusion, **choisir un prestataire cloud, c'est aussi choisir un cadre juridique**. La gouvernance des données externalisées doit être intégrée au plus haut niveau de décision. Ce guide fournit aux organisations les clés de compréhension et d'action nécessaires pour faire des choix éclairés.

Sommaire

Editos

Jean-Noël DE GALZAIN
Président d'Hexatrust

Bernard BAILET
Président de la Fédération des Tiers de Confiance du numérique

Choisir un prestataire, c'est aussi choisir une loi

Nos données sont devenues le cœur battant de notre économie et de notre société. Elles portent nos savoir-faire, nos secrets industriels, nos services publics, notre vie quotidienne. Or, dans un monde où la quasi-totalité des usages numériques passent par des prestataires externes – notamment des services cloud – la question n'est plus seulement de savoir où sont stockées nos données, mais surtout sous quelle loi elles tombent.

Car avec les réglementations extraterritoriales, la règle est simple : ce n'est pas la localisation qui compte, mais la nationalité du prestataire. Autrement dit, vos données peuvent être hébergées à Paris, mais rester accessibles à des autorités étrangères. Le *CLOUD Act* américain ou le FISA en donnent des exemples frappants : ces textes permettent à leurs gouvernements respectifs d'exiger l'accès à des données, même si elles concernent des citoyens ou des entreprises européens, sans contrôle de nos propres autorités françaises et européennes.

Ces enjeux ne sont pas théoriques. Rappelez-vous l'affaire Microsoft Ireland : une filiale américaine a été sommée de transmettre à la justice des données stockées en Europe. Plus près de nous, des collectivités locales françaises ont dû revoir leurs choix de prestataires cloud à la suite des alertes de l'ANSSI, qui craignait une dépendance excessive vis-à-vis d'opérateurs non européens. Dans les deux cas, une même leçon s'impose : déléguer ses données, c'est aussi déléguer une partie de son autonomie.

C'est pourquoi nous insistons sur la nécessité d'une prise de conscience collective. L'externalisation est une formidable opportunité : elle permet aux entreprises de toutes tailles, comme aux administrations, de bénéficier de services agiles, puissants et sécurisés. Mais elle comporte un corollaire inévitable : la dépendance. Dépendance économique, face à des acteurs en situation quasi-monopolistique. Dépendance technique, avec des conditions de réversibilité souvent floues. Et surtout, dépendance juridique, face à des réglementations étrangères qui peuvent entrer en contradiction avec nos propres lois européennes.

L'enjeu est clair : il en va de notre autonomie stratégique. Les arrêts brutaux de services, les réquisitions de données ou les fluctuations géopolitiques peuvent mettre en péril la continuité d'activité de milliers d'organisations. Imaginez une PME innovante dont les brevets hébergés chez un opérateur étranger se retrouvent soudain accessibles à une autorité hors d'Europe. Ou encore une collectivité territoriale incapable d'accéder à ses données sensibles suite à un blocage transfrontalier. Ces scénarios ne sont pas de la science-fiction : ils se sont déjà produits.

La publication de ce guide est donc une étape essentielle. Il ne s'agit pas de fermer nos portes, mais de reprendre la main. Exiger la transparence de nos prestataires, vérifier leur exposition aux lois extraterritoriales, favoriser les solutions européennes certifiées (SecNumCloud, eIDAS), voilà les premières pierres d'une stratégie numérique responsable.

En tant que représentants des tiers de confiance du numérique et des acteurs français de la cybersécurité, nous lançons un appel : que chaque utilisateur – entreprise, administration, citoyen – comprenne que ses choix numériques sont aussi des choix de souveraineté. La donnée n'est pas une ressource comme une autre. Elle est notre patrimoine commun. La protéger, c'est protéger notre capacité à innover, à décider, à agir librement.

Catherine MORIN-DESAILLY
Sénatrice de la Seine-Maritime

Maîtriser la donnée pour préserver notre autonomie stratégique

Autrefois, la manne mondiale était le pétrole, aujourd'hui, c'est la donnée qui crée la richesse. Elle est le nouvel or noir, véritable moteur d'un monde et d'une économie qui se sont entièrement numérisés. Dès lors, il faut considérer qu'elle constitue un actif stratégique majeur et que sa maîtrise est vitale à notre autonomie et au devenir de nos démocraties.

Pourtant depuis plus d'une décennie, nous continuons à externaliser massivement nos services numériques, à recourir, le plus souvent, à des acteurs extra-européens, nous soumettant à des législations extraterritoriales et à des mécanismes d'ingérence juridique. Nous nous privons là d'un contrôle réel des conditions d'accès de traitement ou de transfert de nos données.

Au Parlement, particulièrement au Sénat, nous avons pointé très tôt les dangers à l'œuvre et l'urgence de la mise en œuvre d'une stratégie globale et offensive, au risque pour l'Europe de devenir une colonie du monde numérique. Nous avons toujours plaidé pour une régulation européenne assortie d'une politique industrielle et volontariste, pour une troisième voie, loin du néolibéralisme américain à la solde des big Tech, détenues par une élite technologique et de l'autoritarisme étatique de la Chine.

Alors que les crises successives ont démontré ces dernières années à quel point nos dépendances technologiques étaient devenues dangereuses, cette cause a fini, au-delà des initiés, par gagner du terrain, parmi nos concitoyens, au sein de nos entreprises, de nos administrations et collectivités.

Mais au-delà de cette prise de conscience, il faut désormais agir. Une stratégie globale associant prévention et éducation, réglementation et choix industriels s'impose.

Cela passe par le levier de la commande publique dans le respect des règles de concurrence, reposant sur un Small business ou un Buy European Act, nous l'espérons à venir. Elle doit aussi reposer sur des principes de transparence de la chaîne de sous-traitance, de la traçabilité des traitements de la réversibilité des services, de la maîtrise de la localisation, de l'exposition juridique des données. Sans ces garanties, nous ne pourrons réduire les risques ni construire une filière numérique européenne de confiance, promesse d'emploi.

L'Europe dispose désormais des leviers politiques, juridiques et industriels nécessaires pour reprendre en main notre destin numérique, encore faut-il que les acteurs, tout ce tissu de petites moyennes et grandes entreprises, bénéficient ainsi d'orientations et de soutiens clairs.

J'espère que c'est le rôle que pourra jouer ce guide : offrir un cadre clair, de compréhension et d'évaluation des risques liés aux réglementations extraterritoriales, afin de permettre à chacun d'opérer des choix éclairés en cohérence avec nos valeurs et nos intérêts.

Olivier SICHEL
Directeur Général du Groupe Caisse des Dépôts

Mobilisation collective pour un numérique de confiance

La valorisation des données numériques et l'intelligence artificielle sont de puissants leviers pour accélérer la transformation écologique de notre économie, renforcer la compétitivité de nos entreprises, ou améliorer la qualité de nos services publics et de santé.

Cependant, pour que cette révolution numérique profite à l'intérêt général, il est crucial de maîtriser ces technologies et de garantir la sécurité de nos données stratégiques. Une mobilisation collective est nécessaire pour créer un numérique souverain, puissant et de confiance au niveau européen.

Le contexte économique et géopolitique est particulièrement favorable à cette bascule technologique car il a permis une prise de conscience collective des acteurs publics et privés et des citoyens, de la dépendance de l'Europe à des solutions étrangères.

Le groupe Caisse des Dépôts est mobilisé pour être un moteur de cette transformation numérique. Notre ambition est de bâtir, avec l'ensemble de l'écosystème, les fournisseurs comme les clients, une chaine de valeur du numérique européenne. Nous sommes mobilisés pour créer des infrastructures et des plateformes européennes d'un bout à l'autre de la chaîne de valeur du numérique.

Pour atteindre cet objectif collectif, il est primordial de connaitre les risques et de mesurer ses dépendances. Ce guide est un outil précieux pour guider les choix d'infrastructure dans un environnement numérique complexe à la fois au niveau technologique et réglementaire. Il permet de compléter le dispositif dont je salue la création : l'indice de résilience numérique (IRN). Cet indice permet de mesurer les dépendances numériques à 360° : logiciels, données, infrastructures, actifs technologiques, compétences internes, gouvernance et résilience aux chocs. Avec ce guide et l'IRN, l'objectif est de fournir aux entreprises, aux collectivités territoriales et à l'ensemble des acteurs publics, une boussole concrète pour reconquérir leur autonomie numérique et ainsi renforcer leur sécurité. Emparez-vous de ces outils !

Je remercie l'association Hexatrust et ses membres pour la production, sous l'égide d'AFNOR Normalisation, de ce guide de sensibilisation aux enjeux de protection des données. Chaque brique compte pour permettre le déploiement d'un numérique de confiance dans notre économie et nos services publics.

Introduction

Les usages numériques sont devenus omniprésents dans nos environnements professionnels et personnels, transformant nos organisations et nos modes de production. En même temps que cette augmentation des usages, le recours à des services externalisés s'est fortement intensifié. Ce phénomène s'incarne par le **recours aux services cloud**, qui permettent d'accéder à des ressources informatiques à distance, sans en détenir localement ni les logiciels ni les infrastructures.

Cette externalisation modifie le régime de responsabilité sur les données et s'accompagne d'un transfert d'une partie des leviers de contrôle opérationnels aux prestataires et à leurs sous-traitants. Les logiciels et les données ne sont donc plus gérés dans un périmètre unifié et propre à l'utilisateur, ce qui en complexifie la gouvernance.

L'externalisation dans le cloud permet une abstraction des contraintes physiques de localisation. **Les prestataires et leurs sous-traitants peuvent opérer et intervenir depuis plusieurs juridictions, parfois sans visibilité exhaustive pour le client**. Cela soulève des enjeux de loi applicable et d'injonctions d'accès : les données peuvent être soumises à des réglementations différentes, voire contradictoires, selon les pays où elles sont stockées ou traitées. Ces contraintes extraterritoriales imposent une vigilance accrue et une adaptation des pratiques opérationnelles et contractuelles.

Ce guide a pour objectif d'éclairer le lecteur sur ce changement de paradigme juridique. Il propose des clés de compréhension et des pratiques adaptées pour tirer pleinement parti des avantages de l'externalisation, tout en maîtrisant ses risques. Il se veut un outil pédagogique pour mieux appréhender les enjeux de l'externalisation des services numériques dans le cloud, en particulier dans un contexte internationalisé et soumis à des tensions économiques et géopolitiques croissantes.

1 *Cloud Computing :* comprendre l'externalisation

Le *cloud computing*, ou *service d'informatique en nuage*, fait référence à un service numérique fourni à un client qui permet un accès par réseau en tout lieu et à la demande à un ensemble partagé de ressources informatiques configurables, modulables et variables de nature centralisée, distribuée ou fortement distribuée, qui peuvent être rapidement mobilisées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services[1]. Cette pratique présente des intérêts techniques et économiques multiples (ex : mutualisation des ressources hardware, des équipements et des compétences). Ainsi, en une seule décennie, le cloud s'est imposé comme un pilier du numérique et comme l'une des architectures dominantes des systèmes d'information.

À l'horizon 2026, le volume de données créées et utilisées dans le monde devrait atteindre 200 zettabytes, soit trois fois plus qu'en 2020. On estime qu'environ 100 zettabytes d'entre elles seront stockées dans le cloud, soit 50 % des données mondiales[2].

Le corollaire de cette pratique, qu'il s'agisse de cloud public[3] ou privé[4], est que les données, les traitements et les moyens techniques qui les supportent ne sont plus sous le contrôle exclusif de leur propriétaire. Ce changement d'usage doit dès lors être parfaitement compris pour appréhender l'ensemble des conséquences techniques et juridiques qu'il impose.

Distribution géographique des traitements de données : la fin des frontières

Le fait de confier ses données et leur usage à un prestataire de cloud ne signifie pas qu'une seule machine ou un seul site en assure la gestion. Au contraire, pour atteindre les performances attendues, le prestataire peut utiliser des infrastructures complexes, réparties sur plusieurs sites (zones de disponibilité), parfois situées dans plusieurs pays, y compris pour un seul et même client, en particulier dans le cas du cloud public. Ce découpage autorise, pour des raisons d'efficacité technique notamment, la réplication, le déplacement ou le basculement des données, traitements et sauvegardes, au sein des régions et zones opérées par le prestataire et, le cas échéant, par ses sous-traitants, sous réserve des clauses contractuelles et des contraintes réglementaires applicables. On peut parler ainsi de distribution géographique, ou, « déterritorialisation », des données. En ce sens, elles ne sont plus attachées à un serveur ou à un lieu unique.

Absence de frontière numérique

Si le cloud repose sur des infrastructures bien tangibles – datacenters et serveurs –, la localisation des données qu'il héberge ne se réduit donc pas à un unique point d'hébergement. À l'ère de l'externalisation généralisée, les données ne sont plus attachées à un lieu physique fixe : elles évoluent dans un environnement dynamique et circulent d'un point A à un point B ; la majeure partie du temps sans que l'utilisateur s'en aperçoive.

Dès qu'une donnée est générée ou modifiée, elle entre aussitôt dans un cycle de traitement distribué. Fragmentée, dupliquée, synchronisée et parfois déplacée en continu, la donnée fait l'objet d'opérations automatisées, visant la haute disponibilité, faible latence et résilience. Le tout peut s'opérer en quelques secondes, voire en temps presque réel, sans intervention humaine.

Invisible mais constant, ce flux révèle la nature intrinsèquement vivante du cloud, au sein duquel la donnée devient fondamentalement mobile. Pour les utilisateurs, cette réalité pose une question majeure : comment garder le contrôle sur une donnée que l'on est incapable de localiser ?

[1] Légifrance : https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000049563594
[2] Cybercrime Magazine : https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/?utm
[3] Le cloud public repose sur une infrastructure mutualisée gérée par un fournisseur externe. Les ressources d'un même serveur sont partagées entre plusieurs clients qui se partagent la disponibilité des ressources, dans un modèle multi-tenant avec facturation à l'usage sans frais d'accès au service.
[4] Le cloud privé désigne une infrastructure dédiée exclusivement à une seule organisation. Cette architecture peut être hébergée dans les datacenters de l'entreprise (on-premise) ou externalisée chez un prestataire spécialisé, tout en conservant un caractère exclusif.

Si la spatialisation devient floue, le risque juridique se précise. Ce n'est plus la géographie des octets (i.e. : *data residency*) qui fait foi, mais l'origine des opérateurs et de leurs sous-traitants (i.e. : *data governance*). En pratique, la bonne question n'est donc plus « où sont mes données ? » ni « où sont mes serveurs ? » mais « qui peut les contrôler, en disposer, sur requête de quel juge, et sous quelles clauses contractuelles ? ».

Modèles de services : IaaS, PaaS, SaaS

Modèle interne	Modèle IAAS	Modèle PAAS	Modèle SAAS
Code applicatif	Code applicatif	Code applicatif	Code applicatif
Données	Données	Données	Données
Logiciels de base	Logiciels de base	Logiciels de base	Logiciels de base
Systèmes d'exploitation	Systèmes d'exploitation	Systèmes d'exploitation	Systèmes d'exploitation
Couches de virtualisation	Couches de virtualisation	Couches de virtualisation	Couches de virtualisation
Plates-formes matérielles	Plates-formes matérielles	Plates-formes matérielles	Plates-formes matérielles
Réseau de stockage	Réseau de stockage	Réseau de stockage	Réseau de stockage
Réseau de sauvegarde	Réseau de sauvegarde	Réseau de sauvegarde	Réseau de sauvegarde
Réseau interne	Réseau «privé»	Réseau «privé»	Réseau «privé»
Réseau externe	Réseau externe	Réseau externe	Réseau externe
Partenaires externes	Partenaires externes	Partenaires externes	Partenaires externes
INTERNE	**INFRASTRUCTURE AS A SERVICE**	**PLATEFORM AS A SERVICE**	**SOFTWARE AS A SERVICE**

Sous la responsabilité de l'entreprise — Sous la responsabilité du fournisseur

Il n'existe pas qu'un seul type de cloud : lorsque l'on parle de services cloud, on fait généralement référence à trois niveaux de services, IaaS, PaaS et SaaS, que l'on peut décrire comme suit :

Infrastructure as a Service (IaaS) : l'IaaS est un service de cloud computing offrant des ressources informatiques matérielles (stockage, réseau, baies de serveurs) au sein d'un environnement virtualisé, par le biais d'Internet ou d'une autre connexion[5].

Exemples de fournisseurs de IaaS : Amazon Web Services (AWS), Microsoft Azure, OUTSCALE Dassault Systèmes, OVHcloud, NumSpot.

Platform as a Service (PaaS) : le PaaS est un service de cloud computing fournissant aux clients (généralement des développeurs ou entreprises de développement d'applications logicielles) une plate-forme permettant le développement, l'exécution et la gestion d'applications logicielles, sans avoir à gérer l'infrastructure matérielle sous-jacente[6].

Exemples de fournisseurs de PaaS : Google App Engine, SAP Cloud, Red Hat OpenShift, Kubernetes, Clever Cloud, OVHcloud, NumSpot.

[5] CNIL : https://www.cnil.fr/fr/definition/iaas
[6] CNIL : https://www.cnil.fr/fr/definition/paas

Software as a Service (SaaS) : le SaaS est un service de cloud computing dans lequel le fournisseur offre une solution logicielle, accessible depuis Internet, en tant que service. Le client n'a pas à gérer l'infrastructure sous-jacente, à installer ou à mettre à jour l'application[7].

Exemples de fournisseurs de SaaS : Salesforce, Google, Microsoft, Dassault Systèmes, Docaposte.

La donnée comme actif stratégique

Les données incarnent l'activité des organisations, qu'elles soient publiques ou privées. Elles constituent leur patrimoine immatériel, et dans le cas des entités ne produisant pas de biens matériels, l'intégralité de leur activité.

Ces données relèvent de la propriété des entités qui les produisent. Même lorsque celles-ci choisissent de recourir à des services cloud, la propriété des données demeure inchangée. Il ne s'agit pas d'un transfert de propriété, mais uniquement d'un transfert de responsabilité en matière de stockage et/ou de traitement.

À ce titre, tout accès ou transmission d'une donnée sans base légale valable ou sans accord préalable et explicite du titulaire constitue un accès illicite ou une violation des obligations contractuelles.

Au-delà de la question de l'accès non autorisé ou non informé, la protection des données s'impose également pour des raisons de confidentialité. Certaines données sont confidentielles en raison de leur caractère personnel – c'est notamment le cas de toutes les informations relatives aux salariés en entreprise ou de données de santé que peut traiter une entreprise qui opère dans ce secteur.

D'autres données peuvent revêtir une valeur stratégique liée au secret des affaires : savoir-faire de fabrication, portefeuille clients, stratégies d'innovation, etc. Leur divulgation représente un risque manifeste pour leur propriétaire.

C'est pourquoi la classification des données est essentielle pour identifier celles qui ne doivent en aucun cas être accessibles à des tiers sans autorisation explicite.

Il existe à cet effet des référentiels de classification des données sensibles, tels que :

- Le guide de l'ANSSI sur les données et traitements sensibles ;
- Le guide de l'Afep et du MEDEF d'identification des données sensibles visées par la loi dite de blocage (décret n°2022-207 du 18 février 2022) ;
- Les dispositions du RGPD (article 9) concernant les « catégories particulières de données » ;
- Le guide de l'Afep, du MEDEF et du SISSE à usage des entreprises d'identification des données sensibles.

[7] CNIL : https://www.cnil.fr/fr/definition/saas#:~:text=Le%20SaaS%20(Software%20as%20a,mettre%20%C3%A0%20jour%20l'application

2 L'externalisation et le risque juridique

L'externalisation des données dans le cloud entraîne leur gestion dans un environnement désormais multi-juridictionnel. Cette déterritorialisation implique une recomposition des lois applicables et des juridictions compétentes sur ces données.

Bien que le régime juridique principal reste celui du pays du propriétaire des données, d'autres législations peuvent s'y ajouter. En effet, le cadre juridique du pays du prestataire de services cloud peut s'ajouter à celui du pays ou des pays par lesquels les données transitent ou sont temporairement stockées, notamment quand les lois du pays d'origine du prestataire ont une portée extraterritoriale, c'est-à-dire qu'elles s'appliquent là où le ressortissant exerce son activité.

Extraterritorialité : une portée juridique au-delà des frontières

On parle d'extraterritorialité pour désigner la faculté pour un État d'appliquer ses lois en dehors de ses frontières nationales. Ce mécanisme juridique, bien que complexe, est de plus en plus mobilisé dans un monde globalisé où les interactions économiques, numériques et humaines dépassent largement les limites territoriales.

Souvent invoquée dans une logique défensive, l'extraterritorialité permet aux États de répondre à des enjeux transnationaux majeurs, tels que :

- la lutte contre la criminalité internationale, notamment la corruption, le blanchiment, le financement du terrorisme, les sanctions économiques, qui ne connaissent pas de frontières ;
- la protection des droits fondamentaux, comme les droits humains ou la préservation de l'environnement, qui concernent l'ensemble de la communauté internationale.

Pour qu'un État puisse appliquer sa loi hors de son territoire, il doit établir un fondement de compétence suffisant avec les faits, les personnes ou les biens en cause. Dans le droit américain, on peut parler de *US nexus*[8].

Par extension, on appelle un *nexus* le lien juridique suffisant entre l'État et la situation concernée, permettant de justifier l'exercice de sa juridiction ou l'application de sa législation.

Lois extraterritoriales et cloud

Dans de nombreux États, les données sont d'abord perçues comme un enjeu de sécurité nationale. Elles permettent de détecter des menaces, de documenter des enquêtes judiciaires ou de soutenir des opérations de renseignement. En arrière-plan, ces mêmes données peuvent aussi être exploitées pour de l'intelligence économique : compréhension des marchés, repérage d'acteurs stratégiques, analyse de dépendances ou de vulnérabilités. Cette centralité des données est renforcée par leur hébergement massif dans des services cloud, souvent opérés par une poignée de grands fournisseurs extra-européens.

Dans des circonstances qualifiées d'exceptionnelles, les fournisseurs de services cloud peuvent être contraints par les autorités de transmettre les données de leurs clients, parfois sans en informer le propriétaire des données.

Ces transferts, motivés par l'application extraterritoriale de législations, s'inscrivent néanmoins dans un cadre juridique international fondé sur la protection de la vie privée et des données personnelles, des principes issus du droit international des droits de l'homme.

- ONU - Pacte international relatif aux droits civils et politiques (PIDCP)[9]: l'article 17 garantit à toute personne une protection contre les ingérences arbitraires dans sa vie privée, incluant la sauvegarde des données personnelles.
- Conseil de l'Europe - Convention 108[10]: impose que tout transfert vers un État tiers assure un « niveau de protection adéquat », établissant ainsi les fondements d'un encadrement global des flux transfrontaliers de données.

[8] In D.C. Andrews et J.-M. Newman, « Personal jurisdiction and choice of law in the Cloud », 73 Md. L. Rev. 313, 2013, p. 332 ; et « Perquisitionner les nuages - CLOUD Act, souveraineté européenne et accès à la preuve dans l'espace pénal numérique ». - Frederick T. Davis, Charlotte Gunka, Dans Revue critique de droit international privé 2021/1 N° 1, ISSN 0035-0958

[9] Nations Unies : https://www.ohchr.org/fr/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[10] Conseil de l'Europe : https://rm.coe.int/1680078b39

- Union européenne - Règlement européen général sur la protection des données (RGPD)[11]: l'article 47 interdit de transférer des données sans en avertir leur propriétaire.

Pour limiter les contradictions entre ces différents cadres juridiques, les États cherchent à encadrer ces transferts de données. Toutefois, pour les données des entités privées comme publiques, il n'existe pas d'accord général permettant de gérer de manière multilatérale l'application des différentes réglementations internationales. Il existe en revanche des *Mutual Legal Assistance Treaties (MLAT)*, traités d'entraide judiciaire, c'est-à-dire des accords bilatéraux entre États visant à faciliter la coopération policière et judiciaire, notamment en matière d'échange de renseignements et de données dans le cadre d'enquêtes et aux fins du recueil de preuves. Lorsqu'un fournisseur de services reçoit une demande d'accès à des données émanant d'un État étranger, il peut ainsi exiger que cette demande soit formulée et traitée dans le cadre d'un MLAT : la requête passe alors par les autorités judiciaires de l'État du fournisseur, qui en contrôlent la légalité, la proportionnalité et la conformité aux garanties procédurales nationales avant de permettre ou non la transmission des données. Certaines législations, au titre du CLOUD Act par exemple, permettent toutefois de solliciter directement des données sans recourir aux mécanismes d'entraide prévus par ces traités, ce qui permet ainsi de contourner de facto les garanties procédurales attachées aux MLAT.

Il est ainsi essentiel pour un utilisateur d'identifier clairement les législations à portée extraterritoriale auxquelles il peut être soumis, de comprendre l'étendue des pouvoirs qu'elles confèrent, ainsi que de connaître les cadres susceptibles d'assurer la protection de ses données.

[11] Eur-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

Réglementations applicables au cloud

Cadres extra-européens réclamant un accès aux données au-delà des frontières ou de la nationalité de l'hébergeur

À ce jour, certaines réglementations permettent spécifiquement l'accès aux données de citoyens, entreprises ou administrations, via les prestataires de services. Il convient également de noter que ces réglementations sont en constante évolution et leur portée peut être élargie à tout moment.

Les plus connues sont issues des États-Unis ou encore de la Chine. Ces deux pays ont en effet été pionniers dans le domaine du cloud et disposent par ailleurs d'une capacité particulièrement importante à les déployer à grande échelle.

L'application de ces lois est effective et documentée par des rapports de transparence des fournisseurs, avec une tendance haussière sur la longue période. Certaines sociétés par souci de transparence, publient des rapports officiels détaillant les demandes dont elles ont fait l'objet de la part de leurs administrations nationales et de celles des autres pays. Ainsi, depuis 2009, Google déclare le nombre de demandes de la part du gouvernement américain concernant plusieurs obligations légales :

- Demandes ne portant pas sur le contenu en vertu de la loi FISA ;
- Demandes portant sur le contenu en vertu de la loi FISA ;
- Demandes effectuées par le biais de lettres de sécurité nationale ;
- Liste des lettres de sécurité nationale adressées à Google.

À titre d'exemple, en vertu de la loi FISA, Google a reçu en 2023 des demandes concernant plus de 230 000 comptes utilisateurs[12]. Microsoft indique par ailleurs avoir reçu entre juillet et décembre 2024, 28 120 demandes d'accès aux données, concernant 52 335 comptes utilisateurs. Parmi elles, 64,51 % ont donné lieu à une divulgation d'informations[13].

Ces demandes ne font pas toujours l'objet d'une information auprès des détenteurs de comptes concernés.

De plus, l'entreprise ne peut pas s'y soustraire, contrairement aux demandes issues des autres pays.

Ces rapports de transparence démontrent que ces accès sont non seulement possibles, mais également massifs et en constante augmentation.

CLOUD Act, États-Unis

Le *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)* a été intégré au projet de loi de finances global de 2018 (*Omnibus Spending Bill*), adopté par la Chambre des représentants et le Sénat, puis promulgué par le président le 23 mars 2018. Le *CLOUD Act* modifie le *Stored Communications* Act de 1986.

Ce texte confère aux autorités américaines le droit de contraindre les entités soumises à la juridiction des États-Unis à fournir ou à donner accès aux informations dont elles ont la possession, la garde ou le contrôle, indépendamment du lieu où ces informations sont situées (y compris lorsqu'elles sont stockées en dehors des États-Unis). Le *CLOUD Act* prévoit la possibilité de conclure des accords bilatéraux (*executive agreements*) avec des États partenaires afin d'encadrer l'accès transfrontalier aux données : ces accords fixent un cadre procédural et des garanties, et peuvent ouvrir des mécanismes permettant de s'opposer à certaines demandes ou d'en contester la portée, notamment lorsqu'elles entrent en conflit avec le droit de l'État partenaire.

À ce jour, il n'existe pas d'accord entre les États-Unis et l'Union européenne sous l'égide du *CLOUD Act*. Dans cette situation, les entreprises ne peuvent donc, en théorie, pas contester la demande des autorités américaines.

[12] Rapports Google : https://transparencyreport.google.com/user-data/us-national-security
[13] Rapport Microsoft : https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data

FISA Act, États-Unis

Le *Foreign Intelligence Surveillance Act (FISA)* est une loi adoptée en 1978 aux États-Unis qui sert de principal cadre légal à l'administration américaine pour la collecte d'informations de renseignement extérieur.

La section 702 du FISA constitue un outil de surveillance permettant aux autorités américaines d'accéder aux données hébergées par des entreprises américaines en dehors des États-Unis, sans avoir besoin de recourir à un mandat et leur permet également d'accéder à toutes les données transitant sur le sol américain. Elle a été au cœur des décisions Schrems I[14] et Schrems II[15] rendues par la Cour de justice de l'Union européenne (CJUE), qui ont conduit à l'invalidation des accords Safe Harbor[16] et Privacy Shield[17].

À l'occasion des débats sur la prolongation de la loi FISA, l'article 504 a été durci. Désormais, il ne vise plus uniquement les fournisseurs de services : il s'étend également aux fournisseurs d'équipements, tels que les fabricants et/ou opérateurs de routeurs, de switches et, plus largement, d'infrastructures et équipements réseau).

Executive Order 12333, États-Unis

L'*Executive Order 12333*, signé en 1981, est un décret présidentiel destiné à étendre les pouvoirs et les responsabilités des agences de renseignement des États-Unis et à ordonner aux dirigeants des agences fédérales américaines de coopérer pleinement avec les demandes d'information de la CIA.

Ce texte définit ainsi avec précision les missions, les pouvoirs et les limites des services de renseignement tels que la CIA, la NSA et le FBI, en matière de collecte, d'analyse et de partage d'informations. Il est par exemple inscrit dans ce décret que « la Central Intelligence Agency est chargée de recueillir, d'analyser, de produire et de diffuser des renseignements étrangers et du contre-espionnage » et que l'on entend par « renseignement étranger » : « toute information relative aux capacités, aux intentions ou aux activités de gouvernements étrangers ou de leurs composantes, d'organisations étrangères ou de personnes étrangères[18].»

À ce titre, ce décret constitue l'un des fondements juridiques permettant aux États-Unis d'accéder à certaines données.

CALEA Act, États-Unis

Adoptée aux États-Unis en 1994, la loi *CALEA (Communications Assistance for Law Enforcement Act)* est une loi relative aux interceptions de communication. Son objectif est de renforcer la capacité des forces de l'ordre à procéder à des interceptions légales de communications, en exigeant des opérateurs de télécommunications et des fabricants d'équipements de télécommunications qu'ils modifient et conçoivent leurs équipements, infrastructures et services de manière à intégrer des capacités natives de surveillance ciblée.

[14] Eur-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362
[15] InfoCuria : https://curia.europa.eu/juris/liste.jsf?num=C-311%2F18&utm_
[16] Eur-Lex: https://eur-lex.europa.eu/eli/dec/2000/520/oj
[17] Eur-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016D1250&utm
[18] USA government : https://www.odni.gov/files/NCSC/documents/Regulations/EO_12333.pdf?utm_

Cybersecurity Law, Chine[19]

Adoptée en 2016, la *Cybersecurity Law (CSL)* entend renforcer la protection des données, la localisation des données et la cybersécurité, dans l'intérêt de la sécurité nationale. Elle s'applique à toute entreprise opérant en Chine, y compris les entreprises étrangères.
À titre d'exemple, celles-ci sont tenues de fournir un support technique et une assistance aux autorités de sécurité publique et de sécurité nationale lorsqu'elles mènent des activités de protection de la sécurité nationale ou des enquêtes pénales.

Data Security Law, Chine[20]

Entrée en vigueur le 1er septembre 2021, la *Data Security Law (DSL)* élargit la notion de « données sensibles » en incluant toute information pouvant avoir un impact sur la sécurité nationale, la stabilité économique ou les intérêts publics. Cette loi s'applique aux organisations opérant sur le territoire chinois, ainsi qu'à celles situées à l'étranger lorsque leurs activités de traitement de données sont jugées susceptibles d'affecter des intérêts stratégiques.
Les flux de données transitant par des infrastructures ou services soumis à ce cadre peuvent faire l'objet d'exportations et d'analyses.

Personal Information Protection Law, Chine[21]

Souvent comparée au RGPD européen, la *Personal Information Protection Law (PIPL)*, impose des obligations de consentement, de transparence et de limitation des finalités.
Elle contient une exception majeure : les données peuvent être transmises aux autorités pour des raisons de sécurité nationale ou d'intérêt public.

Cadres extra-européens visant à protéger l'accès aux données externalisées

Au-delà des frontières de l'Europe, de nombreux textes visent également à protéger les données des citoyens, des entreprises et des organisations publiques.

Act on the Protection of Personal Information, Japon

La loi japonaise sur la protection des données, l'Act on the Protection of Personal Information (APPI), a été adoptée en 2003 et a depuis été révisée, notamment en 2020, pour renforcer la sécurité des données personnelles des citoyens japonais. Avec sa portée extraterritoriale, elle s'applique aux entreprises étrangères manipulant les informations de résidents japonais. L'APPI impose des exigences strictes en matière de consentement et de transparence, garantissant aux individus des droits tels que l'accès, la correction et la suppression de leurs données. De plus, des sanctions sévères peuvent être imposées en cas de non-conformité, tandis que les amendements récents introduisent des obligations de notification en cas de violation de données.

Digital Personal Data Protection Act, Inde

La loi sur la protection des données personnelles numériques (Digital Personal Data Protection Act – DPDPA), adoptée par le Parlement indien le 11 août 2023, établit un cadre juridique pour le traitement des données personnelles numériques, en affirmant le droit des individus à la protection de leurs informations. Le texte présente une portée extraterritoriale, s'appliquant aux entités, indiennes ou étrangères, qui traitent les données en Inde. Cette loi autorise le transfert de données personnelles hors de l'Inde, uniquement vers les pays non interdits par le gouvernement indien.

[19] China Law Translate : https://www.chinalawtranslate.com/en/2016-cybersecurity-law/
[20] China Law Translate : https://www.chinalawtranslate.com/en/data-security-law-draft-2/
[21] China Law Translate : https://www.chinalawtranslate.com/en/pipl-draft-2/

Privacy Act, Australie

L'Australie s'est dotée dès 1988 d'une réglementation sur la protection des données avec le Privacy Act. L'article 14 prévoit un ensemble de droits relatifs à la protection de la vie privée, connus sous le nom de principes australiens de protection de la vie privée (Australian Privacy Principles). Ces principes s'appliquent aux organismes du gouvernement australien et du Territoire de la capitale australienne, ainsi qu'aux organisations du secteur privé qui sont sous contrat avec ces gouvernements, aux organisations et aux petites entreprises qui fournissent des services de santé, et aux organisations privées dont le chiffre d'affaires annuel dépasse 3 millions de dollars australiens (sous réserve de certaines exceptions spécifiques). La section 5B confère à la loi une portée extraterritoriale qui s'applique aux entités ayant un « lien australien », défini par la constitution ou l'exercice d'activités commerciales dans le pays, qui collectent ou détiennent des données personnelles australiennes.

Lei Geral de Proteção de Dados, Brésil

La loi générale sur la protection des données (Lei Geral de Proteção de Dados - LGPD) du Brésil est entrée en vigueur le 18 septembre 2020 et constitue le cadre principal de protection de la vie privée des consommateurs dans le pays. Cette législation impose des exigences strictes en matière de collecte, de traitement et d'utilisation des données personnelles, tout en garantissant des droits aux individus, tels que l'accès, la correction et la suppression de leurs informations. La LGPD possède une portée extraterritoriale, ce qui signifie qu'elle s'applique également aux entreprises situées en dehors du Brésil qui traitent des données de personnes résidant dans le pays.

Personal Information Protection and Electronic Documents Act, Canada

La loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), ou, Personal Information Protection and Electronic Documents Act (PIPEDA)[22] du Canada, entrée en vigueur en 2000, encadre la collecte, l'utilisation et la communication de renseignements personnels dans le cadre d'activités commerciales. Elle a une portée extraterritoriale puisqu'elle s'applique aux organisations canadiennes comme étrangères. Cette législation s'applique également à une organisation à l'égard des renseignements personnels qu'elle communique, utilise ou recueille dans le cadre d'une activité commerciale et qui circulent à l'étranger.

Cadres européens et français visant à protéger les données externalisées

RGPD, Union européenne

Entré en application en mai 2018, le Règlement général sur la protection des données (RGPD) constitue le socle de la régulation européenne en matière de traitement des données à caractère personnel. Il s'applique à toute entité, européenne ou étrangère, qui traite des données relatives à des personnes se trouvant sur le territoire européen. Son objectif principal est de donner aux citoyens européens le contrôle de leurs données, tout en encadrant de manière stricte leur traitement, notamment lorsqu'il implique des transferts hors de l'Union.

Ces transferts ne sont autorisés que si le pays destinataire assure un niveau de protection des données « adéquat », reconnu par une décision d'adéquation de la Commission européenne[23]. À défaut, ils ne peuvent avoir lieu que moyennant des garanties appropriées[24], telles que des clauses contractuelles types.

À titre d'exemple, afin d'encadrer les transferts de données entre l'Union européenne et les États-Unis, plusieurs mécanismes ont été mis en place au fil des années. Il en existe notamment avec les États-Unis.

L'accord actuel avec les États-Unis, le *Data Privacy Framework (DPF)*[25] est en vigueur depuis 2023. Ce nouveau cadre introduit un système de certification pour les entreprises américaines, un principe de proportionnalité dans l'accès aux données par les agences de renseignement, ainsi qu'un mécanisme de recours via la *Data Protection Review Court (DPRC)*.

Data Privacy Framework

À ce jour, le DPF fait l'objet de vives critiques, à commencer par Max Schrems et son organisation NOYB (None of Your Business). En juillet 2023, Max Schrems a annoncé[26] son intention de contester à nouveau la validité du cadre devant la CJUE. Selon lui, le DPF ne résout pas les failles identifiées dans les deux arrêts précédents : les programmes de surveillance de masse américains restent largement inchangés, le principe de proportionnalité invoqué dans le DPF est interprété de manière unilatérale par les autorités américaines, la Data Protection Review Court est une instance administrative dépendante de l'exécutif – ce qui contreviendrait à l'exigence d'un recours effectif devant une autorité indépendante, prévue par l'article 47 de la Charte des droits fondamentaux de l'UE.

Par ailleurs, le Privacy and Civil Liberties Oversight Board (PCLOB), l'autorité américaine chargée de veiller à ce que les dispositifs de surveillance gouvernementaux respectent les libertés civiles et la vie privée, a été considérablement affaibli lorsque, en janvier 2025, l'administration Trump a demandé la démission de ses trois membres démocrates – dont sa présidente. Cette décision a privé le conseil du quorum nécessaire à son fonctionnement, le paralysant de fait. Elle a ainsi suscité une vive inquiétude en Europe : de nombreux acteurs ont alerté sur le risque que ce coup porté au PCLOB compromette le cadre de transfert de données entre l'Union européenne et les États-Unis, lequel repose précisément sur l'existence d'un contrôle indépendant.

En parallèle, le député français Philippe Latombe a déposé un recours[27] en septembre 2023 devant le Tribunal de l'Union européenne pour demander l'annulation de la décision d'adéquation relative au DPF. Le recours de Philippe Latombe visant à invalider la décision d'adéquation sur les flux de données UE-US a été rejeté le 3 septembre 2025 par le Tribunal de l'UE. Ainsi, le DPF reste en place à ce jour, dans l'attente d'un appel.

[23] Article 45
[24] Article 46
[25] EUR-Lex : https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj
[26] Noyb : https://noyb.eu/fr/european-commission-gives-eu-us-data-transfers-third-round-cjeu
[27] InfoCuria : https://curia.europa.eu/juris/documents.jsf?num=T-553/23

Data Act, Union européenne

Adopté en 2023 et entré pleinement en application le 12 septembre 2025, le *Data Act*[28] s'inscrit dans la stratégie numérique européenne visant à construire un marché unique de la donnée.

Le *Data Act*[29] aborde les enjeux liés à l'application de législations extraterritoriales dans son article 28, à travers une obligation de transparence concernant l'accès et le transfert internationaux de données. Cet article impose aux fournisseurs de services de traitement de données de publier et tenir à jour, sur leur site internet, les juridictions dont dépend l'infrastructure TIC déployée pour le traitement des données de leurs différents services, ainsi qu'une description générale des mesures techniques, organisationnelles et contractuelles mises en place pour empêcher l'accès, par des autorités publiques extra-européennes, aux données à caractère non personnel détenues au sein de l'Union européenne, ou leur transfert international, lorsque cet accès ou ce transfert risque de contrevenir au droit de l'Union ou au droit de l'État membre concerné. Cette disposition introduit ainsi un devoir de transparence applicable à l'ensemble des fournisseurs de cloud opérant sur le territoire de l'Union européenne. Elle les oblige à indiquer clairement s'ils sont soumis à des législations extraterritoriales susceptibles de les contraindre à transférer les données qu'ils stockent ou traitent. Par ailleurs, la description des mesures mises en œuvre pour empêcher l'accès aux données par des autorités venant de pays tiers à l'UE vise à inciter les fournisseurs de cloud à faire le nécessaire pour prévenir tout accès illicite[30].

Cette disposition du *Data Act* permet, en conséquence, aux clients de choisir en pleine connaissance de cause leur prestataire de services cloud, en étant informés de manière explicite sur le risque que leurs données puissent être transférées à des autorités situées en dehors de l'Union européenne.

Loi « Sécuriser et réguler l'espace numérique », France

La loi visant à sécuriser et réguler l'espace numérique (SREN), adoptée en 2024, vise à renforcer la protection des citoyens dans l'environnement numérique tout en encadrant les grandes plateformes et les services essentiels. Elle constitue une anticipation en droit français du *Data Act*, y compris les obligations de transparence de l'article 28 du *Data Act* (article 33 de la loi SREN).

L'article 31[31] de cette loi va plus loin en disposant que les administrations de l'État, certains de ses opérateurs et certains groupements d'intérêt public doivent porter une attention toute particulière au service de cloud utilisé lorsque des données d'une sensibilité particulière sont traitées. Ces données sont définies et l'article prévoit que les services cloud utilisés doivent répondre à des critères de sécurité strictement définis et « garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers non autorisés par le droit de l'Union européenne ou d'un État membre. ».

Cette loi s'inscrit dans une démarche de transparence accrue pour les utilisateurs de services cloud tout en imposant un cadre plus strict de protection de la donnée sensible pour certaines organisations publiques.

Loi de blocage (loi n°68-678 du 26 juillet 1968), France

La loi de blocage[32], promulguée en 1968 et modifiée en 1980, interdit à toute personne physique ou morale établie en France de transmettre à une autorité étrangère des informations d'ordre économique, commercial, industriel, financier ou technique lorsque la demande est susceptible de porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public ou tend à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères.

[28] EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32023R2854
[29] EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202302854
[30] Basé sur le considérant 102 du *Data Act* : *Afin de prévenir tout accès illicite des pouvoirs publics de pays tiers aux données à caractère non personnel, les fournisseurs de service de traitement de données soumis au présent règlement, tels que les services d'informatique en nuage et en périphérie, devraient prendre toute mesure raisonnable pour empêcher l'accès aux systèmes dans lesquels sont stockées des données à caractère non personnel, y compris, s'il y a lieu, par le chiffrement des données, la sujétion régulière à des audits, le respect vérifié de dispositifs de certification pertinents en matière de réassurance de sécurité et par une modification de leurs politiques d'entreprise.*
[31] Légifrance : https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000049563610
[32] Légifrance : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326

La loi a pour double objectif de préserver les intérêts fondamentaux de la Nation et d'encadrer la coopération judiciaire avec les États tiers à travers les dispositifs formels existants comme les traités bilatéraux. Elle empêche ainsi qu'une autorité étrangère contraigne directement une entreprise française à lui remettre des informations sensibles sans passer par les voies légales prévues à cet effet.

Quand elles mettent en exergue un possible manquement à la loi dite de blocage, les législations extraterritoriales ont pour effet de placer les entreprises françaises face à un conflit juridique, entre la nécessité de répondre aux sollicitations étrangères et obligation à se conformer à la loi française. Pour pallier cette insécurité juridique, un décret[33] et un arrêté[34] d'application ont été publiés en février et mars 2022. Les entreprises destinataires de demandes d'informations émanant d'autorités étrangères doivent désormais en référer au *Service de l'Information Stratégique et de la Sécurité Economiques (le SISSE)*. Ce dernier dispose d'un mois pour évaluer si la loi de blocage s'applique et pour formuler un avis officiel. Cet avis peut ensuite être communiqué par l'entreprise à l'autorité requérante pour justifier son refus de transmission.

Doctrine « cloud au centre », France

La doctrine d'utilisation de l'informatique en nuage par l'État, dite « cloud au centre », définie en 2021 par la Direction interministérielle du numérique (DINUM)[35] et actualisée en 2023, fixe les orientations stratégiques de l'État en matière de cloud. Elle impose que tout nouveau projet numérique de l'administration soit conçu en priorité sur le cloud, avec pour enjeux de moderniser les infrastructures, de garantir la sécurité et la résilience des services tout en assurant la souveraineté numérique de l'État. Dans ce cadre, les services numériques des administrations doivent être hébergés sur l'un des deux cloud interministériels internes de l'État (Nubo, PI) ou sur les offres de cloud proposées par les industriels satisfaisant des critères stricts de sécurité.

Notamment, pour chaque produit numérique manipulant des données d'une sensibilité particulière et dont la violation est susceptible d'engendrer une atteinte à l'ordre public, à la sécurité publique, à la santé et à la vie des personnes ou à la protection de la propriété intellectuelle, l'offre de cloud commerciale retenue devra impérativement respecter la qualification SecNumCloud (ou une qualification européenne garantissant un niveau au moins équivalent, notamment de cybersécurité) et être immunisée contre tout accès non autorisé par des autorités publiques d'États tiers.

Compatibilité entre le droit local et les législations à portée extraterritoriale

Les législations ayant une portée extraterritoriale viennent se superposer au droit local. L'analyse des textes montre qu'un risque d'incompatibilité existe entre ces deux types de réglementations.

D'un côté, certaines réglementations interdisent tout accès à des données, notamment personnelles, sans un consentement éclairé des utilisateurs, à l'instar du RGPD. D'un autre côté, des textes imposent aux entreprises d'un pays donné d'accéder aux données qu'elles détiennent pour le compte de leurs clients, alors que lesdits clients ainsi que leurs clients finaux n'ont pas consenti de manière explicite à de tels accès. Par exemple, le *CLOUD Act* ne prévoit aucune obligation d'information des personnes concernées par la collecte ou la transmission des données, ni aucune obligation d'information des autorités des pays tiers lorsque les données concernent des ressortissants ou des entités situées hors des États-Unis.

Par ailleurs, ces lois imposant un accès aux données des utilisateurs par les prestataires assujettis créent une problématique de nature contractuelle. En effet, prestataires et clients ont pour usage de définir le droit applicable au contrat dans des clauses contractuelles types (CCT). Toutefois, même si une entreprise européenne utilise des CCT pour encadrer le transfert de données vers des fournisseurs cloud non-européens, ces garanties peuvent être remises en cause par une autorité européenne de protection des données.

En conséquence, dans l'Union européenne, une entité privée ou publique devrait s'assurer que le fait d'externaliser ses données auprès d'un prestataire de cloud ne l'expose à une incompatibilité juridique.

[33] Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045190519?utm
[34] Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045358485?utm
[35] Circulaire Premier ministre n°6282/SG : https://www.transformation.gouv.fr/files/ressource/Circulaire-n6282-SG-5072021-doctrine_utilisation-informatique-en-nuage-Etat.pdf

3 Adaptation des pratiques juridiques aux enjeux d'externalisation

Méthode d'évaluation de l'exposition à des réglementations extraterritoriales

La maîtrise du risque lié aux réglementations à portée extraterritoriale suppose une démarche structurée, progressive et documentée. L'évaluation de l'exposition d'une organisation à ces cadres juridiques ne peut se limiter à une analyse ponctuelle ou déclarative ; elle doit s'inscrire dans un processus global et itératif intégrant la nature des données, les obligations réglementaires applicables au détenteur, ainsi que les caractéristiques juridiques et opérationnelles des prestataires envisagés.

La méthode présentée ci-après vise à proposer un cadre opérationnel permettant d'identifier, d'analyser et de maîtriser les risques juridiques liés à l'externalisation des données, en particulier dans des environnements cloud potentiellement soumis à des lois étrangères incompatibles avec le droit français ou européen. Elle repose sur une approche en plusieurs étapes, allant de l'identification des exigences propres à l'entité et aux données traitées, jusqu'à la mise en place de garanties contractuelles et le recours à des dispositifs de confiance reconnus.

Auto-évaluation initiale

Avant tout projet d'externalisation des données, une organisation privée ou publique doit définir le régime auquel elle est soumise, en particulier dans les cas suivants :

- Être une administration, un opérateur de l'État ou un groupement d'intérêt public ;
- Détenir des documents ou des renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public ;
- Détenir des données personnelles ;
- Détenir des données de santé.

Pour chaque cas, des obligations s'imposent :

Contexte	Obligations	Actions à mener
Être une administration, un opérateur de l'Etat ou un groupement d'intérêt public	Recourir à un prestataire de services cloud qui répond à des critères de sécurité strictement définis et « garantissant notamment la protection des données traitées ou stockées contre tout accès par des autorités publiques d'États tiers non autorisé par le droit de l'Union européenne ou d'un État membre. »	Analyse technique et juridique des prestataires envisagés et exclusion des prestataires assujettis à des législations permettant l'accès aux données par des autorités d'États tiers non autorisées par le droit de l'Union européenne.
Détenir des documents ou des renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public	Interdiction de transmettre à une autorité étrangère des informations d'ordre économique, commercial, industriel, financier ou technique lorsque la demande est susceptible de porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public ou tend à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères.	Analyse rigoureuse des données hébergées et traitées et sélection méthodique des fournisseurs de services cloud, de sorte que ceux-ci ne soient pas en mesure d'accéder aux données dont il est question, lorsqu'un tel accès est susceptible de porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public ou tend à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères.

Contexte	Obligations	Actions à mener
Détenir des données à caractère personnel	Autorisation de transferts de données uniquement si le pays destinataire assure un niveau de protection des données « adéquat », reconnu par une décision d'adéquation de la Commission européenne. À défaut, autorisation de transferts de données moyennant des garanties appropriées, telles que des clauses contractuelles types.	Analyse rigoureuse des données hébergées et traitées et analyse juridique des prestataires envisagés, pouvant donner lieu à l'exclusion d'un prestataire soumis à des obligations de transferts de données auprès de pays ne garantissant pas un niveau de protection des données adéquat ou à la négociation de clauses contractuelles types adaptées.
Détenir des données de santé	Obligation d'avoir recours à un prestataire certifié HDS.	Imposer que le prestataire soit qualifié HDS.

De manière générale, une analyse de la sensibilité et de la criticité des données doit être menée afin d'évaluer les conséquences d'un accès par un tiers aux données.

Analyse du cadre juridique applicable aux fournisseurs

L'analyse du cadre juridique applicable au fournisseur est nécessaire pour déterminer les obligations auxquelles il est soumis.

Il s'agit ici avant tout de déterminer l'origine du fournisseur, qui détermine à priori le régime juridique auquel il doit obéir.

Afin de connaître la nationalité d'une entreprise, il conviendra de connaître par exemple les éléments suivants :

- La localisation du siège social de la maison mère de l'entreprise,
- Le pays d'immatriculation,
- La composition du capital social déterminant l'appartenance de l'entreprise,
- La nationalité des actionnaires,
- La relation d'appartenance avec une société mère.

En fonction de la nationalité de l'entreprise et/ou de sa gouvernance, l'entreprise est assujettie aux législations de ce pays et ne peut s'y soustraire.

Exiger des garanties contractuelles spécifiques

Même si les prestataires ne sauraient s'affranchir du droit qui s'applique à eux, en tout lieu et à tout moment, il est nécessaire construire un cadre contractuel adapté aux contraintes réglementaires et surtout aux attentes du client, dans un souci de transparence.

Il apparait ainsi important de disposer des éléments suivants :

1. Le droit applicable et juridiction ;
2. La déclaration par le prestataire du cadre juridique auquel il est assujetti, énumérant toutes les normes et précisant pour chacune si un accès aux données est possible, et si oui
   i. les modalités d'information et de demande d'autorisation au propriétaire de la donnée,
   ii. les modalités de notification et, le cas échéant, d'autorisation auprès de l'autorité compétente en France le délai de prévenance et les cas d'ordonnance de confidentialité,
   iii. les conditions techniques d'accès, y compris le recours à des tiers,
3. Les modalités de mise à jour périodique de la déclaration prévue au [1], considérant que tout changement législatif, réglementaire, de contrôle ou de sous-traitant critique, doit faire l'objet d'une mise à jour sans délai ;
4. La localisation des données : localisations autorisées des données, métadonnées, journaux, sauvegardes et environnements de secours ;
5. Engagement de confinement géographique et interdiction des transferts non autorisés ;
6. Déplacement et réversibilité technique : conditions de déplacement des données et des traitements, y compris politiques de cycle de vie, réplications et basculements ;

7. Les conditions de restitution des données : conditions de restitution intégrale dans un format ouvert ou documenté, avec assistance raisonnable. En cas de modification de la déclaration prévue au [1], demander la restitution des données, d'un effacement complet et vérifiable chez le prestataire et ses sous-traitants, avec certificat d'effacement et logs ;
8. La sous-traitance : liste nominative et à jour des sous-traitants, localisation et rôle. Droit d'audit en cascade, clauses équivalentes imposées à tout sous-traitant, notification préalable à tout changement ;
9. Le changement de contrôle : notification préalable de tout projet de fusion, acquisition, cession d'actifs ou changement de contrôle. Modalité de résiliation si le changement accroît l'exposition juridique, modifie les localisations ou la loi applicable.

Une attention toute particulière doit être apportée à la mise en place d'une révision régulière afin de mettre à jour les conditions contractuelles en fonction des potentielles évolutions des caractéristiques juridiques et économiques du prestataire. En effet, le dynamisme du secteur du numérique implique très souvent des opérations de fusion, acquisition ou changement de contrôle qui sont susceptibles d'affecter le cadre juridique applicable et la chaîne de sous-traitance.

Outils facilitant l'évaluation des prestataires

Il existe des dispositifs de qualification et de certification qui prévoient des exigences relatives à l'exposition à des réglementation extraterritoriales. Ces dispositifs faisant l'objet d'un audit par un tiers indépendant et de contrôles sur place et sur pièce permettent de faciliter l'analyse des prestataires et de disposer d'éléments d'analyse factuels et objectifs.

La qualification SecNumCloud

Le référentiel SecNumCloud, élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), définit un ensemble rigoureux de règles de sécurité visant à garantir un haut niveau d'exigence sur les plans technique, opérationnel et juridique. À ces mesures de sécurité s'ajoutent des dispositions relatives au risque d'exposition extraterritorial. Ces dispositions sont disponibles au chapitre 19.6 « Protection vis-à-vis du droit extra-européen ».

Afin d'assurer cette protection, plusieurs exigences sont imposées aux fournisseurs de services cloud[36]:

- Leur siège statutaire, administration centrale et principal établissement doivent être établis au sein d'un État membre de l'Union Européenne.
- Leur capital social et droits de vote doivent être majoritairement détenus par des entités possédant leur siège, administration centrale ou principal établissement au sein d'un État membre de l'Union européenne.
- Les services fournis doivent respecter la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'État de droit.

La transparence est au cœur du dispositif : le prestataire doit documenter les risques résiduels liés à l'existence de lois extra-européennes ayant pour objectif la collecte de données ou métadonnées des commanditaires sans leur consentement préalable.

La certification HDS

La Code de la santé publique, art. L1111-8 impose des conditions de sécurité particulières à tous les détenteurs de données de santé, pour eux-mêmes au bénéfice d'un tiers. Le respect de ces exigences peut être démontré au moyen d'une certification dite HDS.

La certification Hébergeur de Données de Santé (HDS) a pour objectif de renforcer la protection des données de santé à caractère personnel et de construire un environnement de confiance autour de l'e-santé et du suivi des patients. Le dispositif impose le respect d'un référentiel exigeant en matière de sécurité, de confidentialité et de traçabilité, couvrant aussi bien l'hébergement d'infrastructure physique que l'hébergement applicatif ou l'administration des systèmes, avec des exigences inspirées notamment des normes ISO27001 Iet ISO20000.

[36] Référentiel d'exigences SecNumCloud : https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf

Le référentiel HDS[37], actualisé en 2024, contient des règles visant à encadrer les risques liés aux législations extraterritoriales. Il impose que tout transfert de données de santé en dehors de l'Union européenne ne puisse se faire qu'avec l'accord explicite du client et dans le respect des mécanismes de transfert autorisés par le RGPD. Cette exigence se décline de manière opérationnelle dans plusieurs points du référentiel. Ainsi :

- L'exigence 29 prévoit que lorsqu'une prestation implique un accès à distance depuis un pays extérieur à l'Espace Économique Européen, cet accès doit reposer sur une décision d'adéquation de la Commission européenne au sens de l'article 45 du RGPD, ou, à défaut, sur une garantie appropriée prévue à l'article 46. Si aucune décision d'adéquation n'existe, l'hébergeur doit en informer son client et lui préciser les garanties mises en place pour protéger les données.
- L'exigence 30 complète ce dispositif en ciblant directement le risque d'application d'une législation étrangère. Lorsque l'hébergeur ou l'un de ses sous-traitants est soumis à une loi d'un pays tiers n'assurant pas un niveau de protection adéquat, il doit en faire état dans le contrat, lister les réglementations extra-européennes susceptibles d'imposer un accès aux données de santé en dehors du cadre prévu par le droit de l'Union, décrire les mesures prises pour limiter ce risque et préciser les risques résiduels qui pourraient subsister malgré ces précautions.
- L'exigence 31 introduit un principe de transparence renforcée : l'hébergeur doit publier et tenir à jour une cartographie des transferts de données de santé vers des pays hors EEE, y compris les accès visés par l'exigence 29, et y intégrer la description des risques d'accès non autorisés identifiés dans l'exigence 30.

En combinant ces obligations, la certification HDS impose une forme de transparence vis-à-vis de l'hébergement des données de santé et de leurs transferts extra-européens. Elle n'offre toutefois aucune immunité vis-à-vis de législations à portée extraterritoriale.

Le chiffrement des données

« La protection des données est un élément essentiel d'une stratégie de cybersécurité efficace. Le chiffrement joue un rôle clé : il transforme des informations lisibles en données illisibles, accessibles uniquement grâce à une clé de déchiffrement. Cette technique garantit la confidentialité et l'intégrité des données — qu'il s'agisse d'e-mails, de fichiers partagés, de communications mobiles ou de visioconférences. Elle contribue aussi à sécuriser la mobilité des équipes via le chiffrement des terminaux, à l'usage de VPN et à la protection des accès.

Les données doivent bénéficier d'une protection complète : chiffrement en transit, au repos et en usage, grâce notamment à des modules de cryptographie matérielles sécurisés (HSM), véritables clés de voûte des PKI (Public Key Infrastructure - qui gère les clés cryptographiques). Rien ne sert de chiffrer si les clés sont vulnérables ou duplicables.

Les données ne constituent pas un bloc homogène : chaque enjeu ou niveau de sensibilité appelle un dispositif de protection adapté. Cela va du chiffrement intégré, associé à une supervision par une entité de confiance, à des solutions renforcées, qualifiées et/ou certifiées pour les données soumises à des réglementations spécifiques. En définitive, il est essentiel d'adapter les moyens de protection à la sensibilité des données, tout en garantissant la performance opérationnelle des équipes et une expérience utilisateur la plus fluide possible. »

[37] Agence du numérique en santé, référentiel de certification (HDS) : https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel_certification_hds---fr--v2.pdf

Conclusion

L'externalisation des données dans le cloud, bien qu'elle soit devenue une pratique courante et souvent incontournable dans les stratégies numériques des organisations publiques comme privées, doit **faire l'objet d'une analyse stratégique**. Elle engage des responsabilités profondes, tant sur le plan juridique que sur le plan de la maîtrise et de la gouvernance de l'information.

Ce guide a démontré que **les environnements cloud, par leur nature souvent distribuée et multi-juridictionnelle**, exposent les données à des risques d'accès non autorisés et de pertes de maîtrise.

Les exemples analysés dans ce document sont sans équivoque : **les législations à portée extraterritoriales permettent à des États tiers d'imposer aux organisations, y compris européennes, des obligations d'accès de données, y compris lorsque celles-ci sont hébergées hors de leur territoire**. Ces mécanismes, souvent opaques, contournent les principes fondamentaux du droit européen ou français.

Dans ce contexte, **les organisations françaises et européennes doivent impérativement adopter une posture proactive et éclairée**, afin de s'assurer que les fournisseurs auxquels ils ont recours ne sont pas soumis à ce type de législations à portée extraterritoriale. L'enjeu est d'autant plus crucial pour les organisations publiques et privées qui disposent de données stratégiques voire sensibles.

La sécurité numérique ne peut être garantie que par une gouvernance rigoureuse des données, fondée sur la transparence, la traçabilité et la maîtrise des dépendances. Cela suppose une connaissance fine des cadres juridiques applicables, une capacité à évaluer les risques d'exposition, et une exigence contractuelle renforcée vis-à-vis des fournisseurs de cloud. Cette démarche doit s'inscrire dans une logique de responsabilisation, mais aussi de soutien à la construction d'un écosystème numérique européen fondé sur la confiance, la sécurité et la souveraineté.

En effet, la création et **le développement d'un écosystème européen de prestataires respectueux des cadres, des standards et des valeurs de l'Union européenne doivent être activement soutenus**, encouragés et stimulés pour continuer à renforcer les alternatives européennes performantes, sécurisées et compétitives.

Le futur du cloud ne se subit pas : il se façonne.

Notes

Notes

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

DOCAPOSTE

OUTSCALE

fntc
Fédération des Tiers de Confiance du Numérique

OVHcloud

WIMI

ERCOM
Cyber Solutions by Thales

Numspot

leviia

clever cloud

Janvier 2026