Chine : cadre légal cloud et SaaS

Ce que tout architecte doit savoir

Stéphane FOSSE
fosse.fr

24 mars 2026

Résumé

La Chine a bâti depuis 2017 un cadre réglementaire qui rend impossible l'opération d'un cloud ou d'un SaaS étranger sans partenaire local, sans données hébergées sur le sol chinois et sans certification de sécurité délivrée par la police. Ce n'est pas une contrainte parmi d'autres : c'est la condition d'entrée. Pour un architecte qui conçoit des systèmes d'information à portée mondiale, ignorer ce cadre revient à découvrir en production que l'instance chinoise de son système ne peut pas synchroniser avec le siège.

Quelles lois chinoises s'appliquent aux fournisseurs cloud et SaaS étrangers ?

Trois lois fondamentales forment la colonne vertébrale du dispositif. La **Cybersecurity Law** (CSL), entrée en vigueur le 1er juin 2017, pose les premiers jalons : elle impose à l'article 21 un schéma de protection multiniveau pour tout opérateur de réseau, et à l'article 37 une obligation de localisation des données sur le territoire continental pour les opérateurs d'**infrastructures d'information critiques** (Critical Information Infrastructure, CII). La liste des secteurs concernés — télécommunications, énergie, finance, transports, services publics — est plus large qu'il n'y paraît.

La **Data Security Law** (DSL), effective depuis le 1er septembre 2021, étend le régime de localisation au-delà des CII. Elle introduit une classification tripartite des données : données générales, données importantes (*important data*) et données nationales essentielles (*core national data*). Pour chaque catégorie, les obligations de protection croissent. L'article 36 de la DSL produit l'effet le plus structurant pour les architectes : il interdit formellement à toute organisation ou individu présent en Chine de transmettre des données stockées sur le territoire à des autorités judiciaires ou policières étrangères sans approbation préalable des autorités chinoises compétentes. C'est une réponse directe et délibérée au *CLOUD Act* américain de 2018.

La **Personal Information Protection Law** (PIPL), en vigueur depuis le 1er novembre 2021, complète le tableau en calquant sur les données personnelles des citoyens chinois des règles proches du RGPD européen — collecte fondée sur le consentement, droit à la portabilité, limitation de la durée de conservation — mais avec des conditions de transfert transfrontalier bien plus restrictives. Transfert hors de Chine ? Il faut soit une évaluation de sécurité par l'Administration du cyberespace de Chine (Cyberspace Administration of China, CAC), soit la signature de clauses contractuelles types, soit une certification tierce.

Ce triptyque a été consolidé début 2025 par le **Règlement sur la sécurité des données réseau** (*Network Data Security Management Regulations*), adopté en conseil d'État le 30 août 2024 et entré en vigueur le 1er janvier 2025. Ce texte précise notamment les obligations des grandes plateformes réseau — définies comme celles dépassant 50 millions d'utilisateurs inscrits ou 10 millions d'utilisateurs actifs mensuels — et introduit des exemptions limitées aux transferts transfrontaliers pour des motifs légaux ou d'urgence sanitaire.

Un fournisseur SaaS étranger peut-il opérer directement en Chine ?

Non, et c'est là que le droit chinois se distingue fondamentalement de n'importe quelle autre réglementation. Le cloud computing — IaaS, PaaS et SaaS — est catégorisé dans le catalogue des télécommunications comme un service à valeur ajoutée (*Value-Added Telecommunications Service*, VATS). Opérer un tel service en Chine nécessite une **licence VATS spécifique pour les activités de centre de données internet** (IDC). Or, depuis 2015 au moins, les entités étrangères ne peuvent pas détenir directement cette licence : elles doivent obligatoirement s'associer à un partenaire local agréé qui, lui, la détient et en porte la responsabilité juridique.

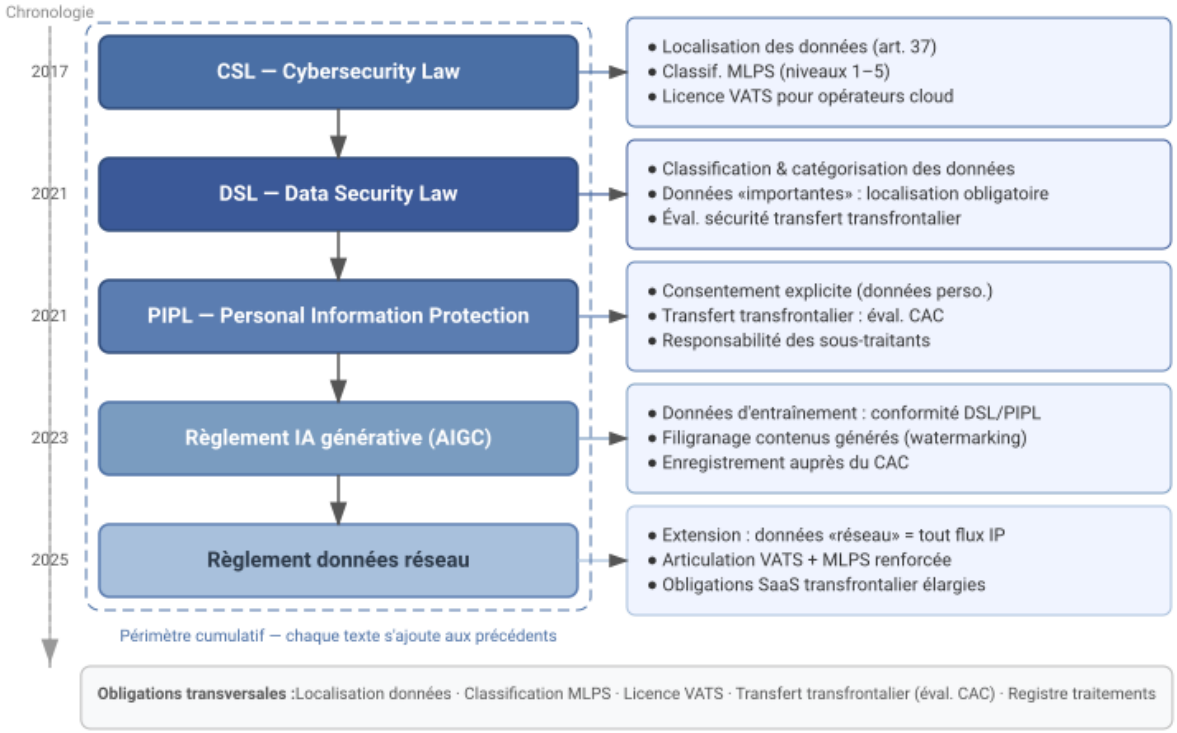

FIGURE 1 – Pile législative chinoise – Données cloud & SaaS

Les cas les plus emblématiques illustrent la mécanique. Azure de Microsoft opère en Chine via la société **21Vianet**, qui détient et gère physiquement l'infrastructure, facture les clients et assure la conformité réglementaire. AWS opère via **Sinnet** (Beijing Sinnet Technology). Ces entités ne sont pas de simples filiales : ce sont des opérateurs légaux distincts qui exploitent les technologies sous licence. La conséquence est architecturale et immédiate : au 31 décembre 2025, l'instance Azure China via 21Vianet propose 104 services, soit 52 % des 199 services disponibles sur Azure Global. La moitié du catalogue SaaS standard n'existe tout simplement pas dans l'instance chinoise.

En avril 2024, le Ministère de l'industrie et des technologies de l'information (MIIT) a publié un avis permettant à des entités étrangères d'investir à 100 % dans des entreprises VATS situées dans quatre zones pilotes — Beijing, Shanghai, Hainan et Shenzhen. Ce signal mérite d'être mesuré. L'ouverture est géographiquement circonscrite, ne remet pas en cause l'obligation de localisation des données et ne modifie pas la doctrine de fond. Les autorités chinoises ont par ailleurs indiqué elles-mêmes anticiper un renforcement des exigences de localisation à mesure que l'économie numérique mûrit.

Qu'est-ce que le MLPS 2.0 et quelles obligations impose-t-il aux entreprises étrangères ?

Le **Multi-Level Protection Scheme 2.0** (MLPS 2.0) est le schéma de protection multiniveau révisé en 2019 et rendu obligatoire par l'article 21 de la CSL. Il s'applique à toute organisation — étrangère ou nationale — qui opère un réseau en Chine, sans exception de taille ni de secteur. Son principe : chaque système d'information doit être classifié sur une échelle de cinq niveaux selon l'impact potentiel d'un incident sur les citoyens, les organisations, l'ordre social ou la sécurité nationale. Le dossier de classification est déposé auprès du Bureau de sécurité publique local (PSB), c'est-à-dire la police.

En pratique, la plupart des entreprises internationales opérant des systèmes orientés utilisateurs chinois se retrouvent en **Niveau 3**. Ce niveau déclenche un audit annuel obligatoire conduit par un expert agréé (tiers indépendant, reconnu par le cadre MLPS). Le score minimum pour passer l'évaluation est de 75 sur 100. Pour les systèmes de Niveau 4, les réévaluations sont semestrielles. Les standards techniques qui définissent les contrôles attendus — GB/T 22239-2019, GB/T 25070-2019 et GB/T 28448-2019 — couvrent non seulement la technique (authentification, chiffrement, détection d'intrusion, journalisation) mais aussi la gouvernance : politique de sécurité documentée, plan de réponse aux incidents, formation du personnel.

Pour les SaaS étrangers, le MLPS 2.0 introduit une contrainte de chaîne d'approvisionnement souvent sous-estimée : le niveau de certification MLPS du fournisseur cloud hébergeant le service ne peut pas être *inférieur* au niveau de certification du système client. Les renouvellements de licences commerciales ont commencé à être conditionnés à l'obtention d'une certification MLPS valide.

Comment la Chine contrôle-t-elle les flux transfrontaliers de données ?

La Chine opère un triple mécanisme. Premier niveau : l'obligation de **localisation physique**. Toutes les données cloud doivent être hébergées dans des datacenters situés sur le territoire continental. Ces datacenters ne peuvent pas être interconnectés avec des sites situés hors de Chine, même si ces derniers appartiennent au même fournisseur. La règle est absolue et ne souffre pas d'exception technique.

Deuxième niveau : l'**évaluation de sécurité avant export**. Tout transfert hors de Chine de données classifiées comme « importantes » doit passer par une évaluation organisée par le CAC. Pour les données personnelles, trois voies alternatives existent : l'évaluation CAC, des clauses contractuelles types approuvées par le CAC, ou une certification de protection des informations personnelles délivrée par un organisme agréé. Le seuil déclenchant l'évaluation obligatoire — traitement de données personnelles de plus d'un million de personnes, ou transfert cumulé dépassant 100 000 personnes sur un an — concerne directement tout SaaS RH, CRM ou e-commerce de taille significative.

Troisième niveau : l'**interdiction de transmission aux autorités étrangères**. L'article 36 de la DSL est sans ambiguïté : aucune organisation ou individu opérant en Chine ne peut fournir à une autorité judiciaire ou policière étrangère des données stockées sur le territoire sans autorisation préalable des autorités chinoises compétentes. Cette disposition est la réponse législative explicite au *CLOUD Act* américain de 2018. La contradiction est structurelle : une multinationale dont le SaaS est une filiale américaine hébergeant des données en Chine se retrouve simultanément soumise à deux obligations légalement incompatibles.

Quels impacts concrets sur l'architecture des systèmes d'information ?

L'ensemble de ce cadre converge vers un pattern architectural unique que l'on peut appeler le modèle ***bi-stack***. L'entreprise occidentale présente en Chine doit maintenir deux stacks applicatifs distincts, étanches et non synchronisables sans procédure réglementaire : un SI global opéré sur les hyperscalers classiques (AWS, Azure, GCP), et un **SI China** hébergé chez un partenaire local agréé — Alibaba Cloud, Huawei Cloud, Tencent Cloud — ou via les instances locales cloisonnées des hyperscalers (Azure China/21Vianet, AWS China/Sinnet).

Le pattern hybride le plus couramment observé consiste à maintenir un **plan de contrôle global** (gouvernance, monitoring, identité) sur le SI principal, couplé à un **plan de données local** étanche pour toutes les données chinoises. Les outils de gouvernance IAM, SIEM, DLP doivent donc être soit répliqués dans l'instance chinoise, soit remplacés par des équivalents locaux. La réduction fonctionnelle est réelle : les instances chinoises des hyperscalers proposent systématiquement un sous-ensemble des services disponibles globalement, avec des écarts pouvant dépasser 50 %.

Cette fragmentation a des conséquences directes sur quatre dimensions architecturales. La gouvernance des données : le registre de traitement de l'entreprise doit intégrer une classification à trois niveaux conforme à la DSL/PIPL, avec des workflows distincts pour les données chinoises. L'identity fabric : les systèmes d'identité et d'accès (IAM/PAM) doivent opérer de manière indépendante sur l'instance chinoise, sans délégation vers un tenant global hébergé hors de Chine. La chaîne d'approvisionnement logicielle : chaque composant tiers intégré au SI China doit être vérifié au regard des certifications MLPS de son hébergeur. Enfin, la conformité SaaS IA : depuis août 2023, le Règlement provisoire sur les services d'IA générative impose aux fournisseurs de LLM ou de services IA à « attributs d'opinion publique » une évaluation de sécurité auprès du CAC avant mise en service — les chatbots d'entreprise et assistants IA entrent dans ce périmètre s'ils servent le public chinois.

Quelle est la trajectoire réglementaire chinoise d'ici 2030 ?

La direction est sans ambiguïté. Le marché chinois du cloud a atteint 828,8 milliards de CNY en 2024, soit une croissance de 34,4 % par rapport à 2023. La Chine occupe désormais une position de leadership dans les organismes de normalisation internationaux — ISO, UIT, IEEE — sur les standards cloud et IA, avec un agenda explicite d'influence sur les normes mondiales. Cette montée en puissance normative s'accompagne d'un durcissement technique du contrôle.

Trois tendances dessinent le paysage 2030. La première est le **cloud souverain domestique** : au sein des CII, la doctrine évolue vers une propriété exclusivement domestique des infrastructures. Les hyperscalers étrangers, même via des partenaires locaux, pourraient voir leur périmètre se réduire aux seules entreprises étrangères implantées en Chine. La deuxième tendance est la **bifurcation technologique sino-américaine**.

Les restrictions d'exportation américaines sur les semi-conducteurs accélèrent la construction d'une stack technologique chinoise autonome qui n'a pas vocation à être interopérable avec les standards occidentaux. La troisième tendance est l'**instrumentalisation stratégique de la régulation** : l'article 26 de la DSL dote la Chine d'une clause de réciprocité lui permettant de prendre des contre-mesures contre tout État imposant des restrictions discriminatoires sur les données chinoises. La réglementation de la donnée est devenue un outil de politique étrangère.

Pour l'architecte qui doit concevoir un SI à portée mondiale avec une présence en Chine, la conclusion pratique est que la complexité de ce bi-stack ne se réduira pas. La question n'est plus « comment connecter » l'instance chinoise au SI global, mais « comment concevoir un SI modulaire dont le composant chinois peut fonctionner en autonomie complète, avec des points de synchronisation réglementairement conformes et juridiquement sûrs des deux côtés ».

Conclusion

La Chine ne cherche pas à bannir les SaaS étrangers. Elle les domestique : licence locale, partenaire agréé, données sur le sol national, accessibles aux autorités, déconnectées des instances globales. Ce modèle est cohérent, stable dans sa doctrine depuis 2017, et de moins en moins négociable au fil des ans. Comprendre ses mécanismes — CSL, DSL, PIPL, MLPS 2.0, VATS, règlement réseau 2025 — n'est pas un exercice de conformité juridique. C'est une condition préalable à toute décision d'architecture pour une organisation qui opère ou prévoit d'opérer en Chine continentale. Les entreprises qui l'ont intégré tôt ont conçu leurs SI en conséquence. Les autres découvrent en production que leur architecture globale ne passe pas la frontière.

Références

[1] AppInChina. Regulation on Network Data Security Management. Anglais. 2024.

[2] Cheung Kong Graduate School of Business. Crossing Borders: How China's Data Laws Are Affecting Businesses. Anglais. 2022.

[3] Covington Inside Privacy. China Released Core National Standards Updating Mandatory Cybersecurity Requirements under the Cybersecurity Multi-level Protection Scheme. Anglais. 2019.

[4] Jia Dai et al. China's emerging data protection framework. Anglais. In : *Journal of Cybersecurity* 8.1 (2022).

[5] DigiChina, Stanford University. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). Anglais. 2022.

[6] Hogan Lovells. China finalizes generative AI regulation. Anglais. 2023.

[7] IAPP. China issues the Regulations on Network Data Security Management: What's important to know. Anglais. 2024.

[8] Giulia Interesse. China Issues New Regulations on Network Data Security Management, Effective January 1, 2025. Anglais. 2024.

[9] Latham & Watkins. China Clarifies Privacy and Data Security Requirements in Network Data Security Management Regulations. Anglais. 2024.

[10] Mayer Brown. PRC Network Data Security Management Regulations. Anglais. 2024.

[11] Morgan Lewis. What China's New Data Security Law Means for Multinational Corporations. Anglais. 2021.

[12] Pekingnology. On cross-border data access: a Chinese summary. Anglais. 2022.

[13] PwC. How China's PIPL rules can impact your business. Anglais. 2021.

[14] Reed Smith LLP. MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates. Anglais. 2019.