Confidentialité réelle vs apparente : les questions qu'il convient de se poser

Synthèse opérationnelle du cycle 2 : les questions qui distinguent un service à confidentialité architecturale d'un service à confidentialité déclarative. Un questionnaire pour le professionnel européen avant d'adopter tout outil numérique destiné à des données sensibles.

Pour être clairs : Deux services ayant la même mention légale peuvent se comporter de manière très différente. L'un protège par conception technique. L'autre protège par promesse contractuelle. La différence ne se lit pas dans la mention — elle se découvre en posant les questions concrètes. La qualité des réponses en dit autant sur le produit que leur propre contenu.

La différence entre confidentialité architecturale et confidentialité déclarative

Au fil des sept articles précédents de ce cycle, nous avons parcouru des couches différentes d'un même sujet. Le droit des transferts internationaux avec Schrems II. L'idée mathématique du hachage cryptographique qui scelle chaque Cuaderno. Le choix architectural du kill switch et la capture institutionnelle qui l'accompagne presque toujours. Le mécanisme du chiffrement de bout en bout et la question opérationnelle de l'endroit où résident les clés. L'alignement des incitations selon le modèle économique. L'identité cryptographique auto-souveraine. L'auto-hébergement comme stratégie proportionnée. Chaque article a traité un angle. Celui-ci, le dernier du cycle, les réunit dans un questionnaire.

La distinction qu'il convient de retenir est simple : il y a des services dont la confidentialité est *architecturale* et il y a des services dont la confidentialité est *déclarative*. La première est incrustée dans la conception technique : certaines violations de l'engagement de confidentialité sont techniquement difficiles ou impossibles parce que l'architecture ne les permet pas. La seconde est déposée dans le texte de la mention légale : certaines violations seraient contractuellement sanctionnables si elles surviennent, mais techniquement rien ne les empêche. Les deux modèles peuvent respecter le RGPD ; mais l'un protège par construction et l'autre protège par promesse, et la différence est opérationnellement énorme.

Les questions qui suivent sont conçues pour distinguer un cas de l'autre. Ce ne sont pas des questions techniques avancées. Ce sont les questions auxquelles tout fournisseur honnête peut répondre dans sa documentation publique. La qualité et la précision de la réponse en disent autant sur le produit que la réponse elle-même. Les questions se regroupent en six couches ; il convient de les poser toutes avant d'adopter le service pour des données sensibles, et non seulement celles que le premier instinct identifie.

Couche 1 : architecture

Fixons un terme avant de poursuivre. Par *opérateur*, nous entendons l'entreprise qui fournit le service : l'entité qui contrôle les serveurs et le logiciel, et non une personne en particulier. Cela étant précisé, la question architecturale fondamentale est : que fait l'opérateur du contenu entre l'expéditeur et le destinataire ? Il existe

trois réponses possibles et il convient de savoir les distinguer, car toutes trois sont parfois présentées avec un vocabulaire similaire.

- La première : le contenu passe par un serveur de l'opérateur en clair, où l'opérateur peut le lire même s'il promet de ne pas le faire.
- La deuxième : le contenu passe par un serveur de l'opérateur chiffré, où l'opérateur ne peut pas le lire si les clés résident exclusivement sur les appareils des utilisateurs.
- La troisième : le contenu ne passe par aucun serveur de l'opérateur, parce qu'il n'existe aucun serveur de l'opérateur dans ce flux précis.

La différence entre ces trois n'est pas de degré : elle est de nature.

La question complémentaire —déjà formulée dans le Cuaderno sur le chiffrement— est : qui détient les clés cryptographiques qui permettent de lire le contenu ? Si c'est l'utilisateur et seulement l'utilisateur qui les détient, le chiffrement est réel. Si l'opérateur les détient en outre sous quelque forme que ce soit —même sous le nom de « récupération de compte » ou de « synchronisation entre appareils »—, le chiffrement est nominal. La question n'admet pas de réponse intermédiaire honnête.

Couche 2 : modèle économique

La question sur le modèle économique importe autant que la question architecturale, et pour la même raison de fond : les incitations produisent, au fil du temps, des produits systématiquement différents même avec des objectifs déclarés identiques. Comment l'opérateur gagne-t-il de l'argent aujourd'hui ? Une seule source, deux, un mélange ? Si le financement inclut la publicité ou la monétisation des données, quelles données sont monétisées et sur quelle base juridique du RGPD cela se fait-il ? La finalité déclarée dans la mention légale couvre-t-elle les données de tiers que le professionnel entend confier au service ?

Et la question de second ordre, pas toujours formulée : quelle est la situation financière de l'opérateur à un horizon de trois à cinq ans ? Une entreprise en phase de capital-risque opère sous des pressions différentes de celles d'une entreprise en rentabilité stable. Le changement de modèle de financement est, à plusieurs reprises, le moment où le contrat implicite avec les utilisateurs est réécrit sans négociation.

Couche 3 : juridiction

Pour le professionnel européen, la question de la juridiction n'est pas rhétorique. Dans quelle juridiction l'opérateur est-il constitué ? Dans quel pays les serveurs qui traitent les données sont-ils physiquement situés ? La réponse aux deux questions précédentes est-elle la même ou différente, et si elle diffère, quelle législation s'applique ? Une région européenne exploitée par une entreprise américaine n'est pas, aux fins de Schrems II, une réponse européenne : l'entreprise est soumise à FISA 702 indépendamment de l'endroit où se trouvent les serveurs.

La question complémentaire opérationnelle est : si arrivait demain une ordonnance de renseignement valide dans la juridiction de l'opérateur exigeant la remise de mes données ou de celles de mes clients, que se passerait-il ? Si la réponse honnête commence par « l'entreprise serait tenue de les remettre », le service ne protège pas contre cette ordonnance, quoi que la publicité suggère du contraire. Si la réponse honnête commence par « l'entreprise ne pourrait pas les remettre parce qu'elle ne les détient pas en clair », le service protège bel et bien ; et la différence dépend presque entièrement des deux premières couches, non de la qualité de la politique de confidentialité.

Couche 4 : opérateur et kill switch

Quelle capacité technique l'opérateur conserve-t-il pour suspendre, bloquer, supprimer ou dégrader le service à distance ? La question n'est pas paranoïaque : elle est opérationnelle. Les plateformes numériques ont exercé cette capacité à plusieurs reprises ces dernières années, parfois de leur propre initiative, parfois sur ordre de gouvernements, parfois après des changements de propriété ou de politique. Si la capacité existe, il convient de savoir sous quelles hypothèses contractuellement déclarées elle s'exerce, et de réserver une marge pour les hypothèses non déclarées que la pratique de ces dernières années a montrées tout aussi pertinentes : ordonnance judiciaire inattendue, sanction internationale, changement de gouvernance d'entreprise, acquisition par une entité ayant une autre politique.

La question sœur est celle du plan de continuité : si l'opérateur exerçait la capacité contre le professionnel —pour quelque raison que ce soit, juste ou non—, quel temps d'activité resterait disponible, quelle procédure d'exportation des données existe, et vers quel fournisseur alternatif pourrait-on migrer ? Si la réponse commence par « cela ne devrait pas arriver », ce n'est pas une réponse opérationnelle ; c'est une promesse.

Couche 5 : identité et accès

Qui contrôle les identifiants d'accès au service ? Si l'opérateur peut réinitialiser l'accès de l'utilisateur sans la participation de l'utilisateur —procédure habituellement appelée « récupération de compte »—, l'opérateur est, techniquement, le dépositaire du compte et peut aussi le céder à quiconque le demande au moyen de la procédure appropriée. Si l'opérateur ne peut pas réinitialiser l'accès parce que l'identité réside cryptographiquement sur l'appareil de l'utilisateur, l'opérateur ne peut pas non plus la céder, pas même sous ordonnance. Les deux modalités sont légitimes selon le contexte ; mais, une fois de plus, elles sont différentes, et il convient de savoir laquelle on adopte.

Qu'advient-il des données du professionnel si le professionnel perd l'accès ? Existe-t-il des mécanismes de récupération —de compte, de fichier, de session— qui dépendent de l'opérateur ? Ces mécanismes sont-ils compatibles avec la déontologie professionnelle du secteur si l'opérateur est contraint de les utiliser ?

Couche 6 : futur

Cette dernière couche est souvent négligée parce qu'elle exige une projection. Que se passerait-il si le service était acquis par une autre entreprise ? Presque toutes les acquisitions s'accompagnent d'une révision des conditions de service dans les mois qui suivent. Que se passerait-il si les exigences réglementaires changeaient ? Le droit européen a accru les obligations de retrait et de blocage depuis 2022, il ne les a pas réduites. Que se passerait-il si l'opérateur disparaissait ? Une part importante des services cloud n'a pas de plan de sortie documenté pour le scénario de fermeture de l'opérateur ; le professionnel découvre le problème lorsqu'il n'y a plus le temps de le préparer.

Il y a une formulation qu'il convient de retenir pour cette couche : les architectures qui dépendent moins de l'opérateur sont plus résilientes face aux changements de l'opérateur. L'auto-hébergement sous l'une quelconque de ses modalités, l'identité cryptographique auto-souveraine, les communications sans serveur intermédiaire, toutes réduisent la surface de risque future par le procédé consistant à réduire la surface de dépendance présente. Elles ne l'éliminent pas ; elles la réduisent.

La différence entre structure et promesse

S'il fallait distiller le cycle en une seule phrase, ce serait celle-ci : les réponses structurelles se maintiennent même si l'opérateur, l'administration ou la législation changent ; les réponses par promesse se maintiennent tant que celui qui promet peut et veut les tenir. Les deux peuvent être correctes au moment de leur adoption. Une seule des deux tient indépendamment du passage du temps et du changement des circonstances.

Cela ne signifie pas que chaque professionnel doive exiger des réponses structurelles de tous les services qu'il adopte. La proportionnalité demeure légitime : un tableur pour la comptabilité interne n'a pas besoin de la même réponse que le dossier clinique d'un patient. Cela signifie, oui, que le professionnalisme consiste à savoir quel type de réponse a été accepté dans chaque cas, et à avoir décidé consciemment que ce type de réponse est proportionné à la donnée concrète.

Le questionnaire, ordonné

Douze questions concrètes qui synthétisent le cycle, ordonnées pour que la réponse à chacune éclaire la suivante :

1. Le contenu passe-t-il par un serveur de l'opérateur ? Si oui : en clair, chiffré avec les clés de l'opérateur, ou chiffré avec des clés exclusives de l'utilisateur ?
2. Si un chiffrement de bout en bout est invoqué, où résident les clés cryptographiques ? L'opérateur connaît-il ou conserve-t-il une partie d'entre elles sous quelque forme que ce soit, y compris la « récupération » ?
3. Quelles métadonnées le service génère-t-il et conserve-t-il ? Pendant combien de temps ? À qui sont-elles visibles ?
4. Comment l'opérateur se finance-t-il ? Si le financement inclut la publicité ou la monétisation des données, la finalité déclarée couvre-t-elle les données de tiers confiées par le professionnel ?
5. Quelle est la situation financière de l'opérateur à un horizon de trois à cinq ans ? Y a-t-il des facteurs suggérant un changement imminent de modèle (introduction en bourse imminente, levée de fonds s'épuisant, acquisition probable) ?
6. Dans quelle juridiction l'opérateur est-il constitué ? Dans quel pays les serveurs sont-ils physiquement situés ? S'ils diffèrent, quelle législation nationale s'applique au traitement ?
7. Que se passerait-il si une ordonnance de renseignement valide dans la juridiction de l'opérateur exigeait la remise de mes données ? L'entreprise pourrait-elle s'y conformer techniquement ?
8. Quelle capacité technique l'opérateur conserve-t-il pour suspendre, bloquer ou supprimer le service ? Sous quelles hypothèses contractuelles ? Sous quelles hypothèses non contractuelles historiquement documentées ?
9. Quel plan de sortie existe-t-il si l'opérateur exerçait cette capacité contre moi, à juste titre ou non ? Existe-t-il une procédure documentée d'exportation des données vers un fournisseur alternatif ?
10. Qui contrôle les identifiants d'accès ? L'opérateur peut-il les réinitialiser sans ma participation ? Cela me protège-t-il ou m'expose-t-il ?
11. Existe-t-il une alternative européenne, auto-hébergée ou sans serveur intermédiaire pour cette fonction précise ? Quel est son coût réel, comparé au risque évalué ?
12. Si la décision d'aujourd'hui était examinée dans cinq ans par un inspecteur, un auditeur ou un client affecté par une violation, le choix actuel serait-il défendable avec les arguments disponibles aujourd'hui, ou faudrait-il s'excuser de ne pas avoir posé de questions raisonnables ?

Les questions n'attendent pas de réponses parfaites. Elles attendent des réponses honnêtes, que l'opérateur honnête sait donner et que l'opérateur moins honnête évite de formuler avec précision. La différence opérationnelle entre les deux classes d'opérateur, nous le disons sans dramatiser, se perçoit généralement en lisant lentement les réponses qu'ils offrent volontairement, avant même d'avoir à en demander davantage.

Avec cet article nous clôturons le deuxième cycle de Cuadernos Lacre. Nous avons commencé par la dette éditoriale héritée de Schrems II et nous terminons par un questionnaire opérationnel. En chemin, nous avons parcouru des concepts —hachage, chiffrement, identité— et des analyses appliquées —kill switch, modèle économique, self-hosting—. L'intention éditoriale déclarée de la publication n'était pas d'accabler le lecteur avec la liste exhaustive des problèmes, mais de lui remettre des outils pour que, face à tout service nouveau, il distingue quelle sorte de réponse il accepte. Cette distinction —entre architecture et promesse— est l'outil. Le reste, chaque professionnel le mettra au service des données qu'il considère, dans sa pratique, dignes de la question.

Sources et lectures complémentaires

- Cette publication, cycle 2 (mai 2026) — *Schrems II, cinq ans après*, *Ce qu'est réellement SHA-256*, *Kill switch et capture institutionnelle*, *Le chiffrement de bout en bout, enfin expliqué*, *Le modèle économique comme gage de confiance*, *Les 24 mots : qu'est-ce qu'une identité cryptographique*, *L'auto-hébergement comme pratique professionnelle*. Les sept articles sur lesquels repose ce questionnaire.
- Règlement (UE) 2016/679 — Règlement général sur la protection des données. Cadre juridique de référence pour toutes les questions que le questionnaire soulève, en particulier les articles 5, 6, 25, 28, 32, 33 et le chapitre V.
- Comité européen de la protection des données — lignes directrices et avis opérationnels sur Schrems II, les transferts internationaux, les analyses d'impact et la responsabilité proactive (publications 2020-2024).
- Agence espagnole de protection des données — sanctions publiées 2022-2024 contre des responsables du traitement pour des instruments de transfert inadéquats ou pour des analyses d'impact formelles sans contenu substantiel.
- noyb.eu — Centre européen pour les droits numériques, dirigé par Maximilian Schrems. Référentiel public de plaintes, de recours et d'analyses sur le respect réel, et non apparent, des règles européennes de protection des données.

← PrécédentSelf-hosting comme pratique professionnelleSuivant →Ce qu'une signature ne peut pas réparer

Lectures recentes

- Réflexion · 29 juin 2026 Vous n'êtes pas anonyme
- Réflexion · 27 mai 2026 Ce qu'une signature ne peut pas réparer
- Analyse · 25 mai 2026 Self-hosting comme pratique professionnelle

Emportez cet article où vous en avez besoin.

↓ Markdown ↓ Texte brut ↓ PDF

Le fichier est téléchargé sur votre appareil. À partir de là, vous pouvez l'enregistrer, l'importer dans Solo2 ou le partager comme vous le souhaitez. Cuadernos ne décide pas de la destination pour vous.

Cachet de cire · SHA-256 b00e9641ab92b5ee3e89e95b5359615c2f71bc74f045ae74a66e333c0b432202

Cuadernos Lacre · Une publication de Menzuri Gestión S.L. ·
écrite par R.Eugenio · éditée par l'équipe de Solo2.