L'auto-hébergement comme pratique professionnelle

Un serveur n'est rien de plus qu'un ordinateur. La question n'est pas de savoir s'il faut en avoir un, mais où vivent les données de vos clients, qui les maintient et qui assume la responsabilité quand quelque chose échoue.

Pour s'entendre : Vos données vivent toujours dans l'ordinateur de quelqu'un : dans celui d'un géant à qui vous confiez tout, dans un ordinateur loué que vous gérez, ou dans le vôtre propre. Plus vous voulez de contrôle, plus vous assumez de responsabilité. Déléguer à un grand tiers rassure, mais n'exonère pas : l'information est la vôtre —et celle de vos clients—, et le responsable, c'est vous.

La question entre le cloud et la cave

Il est bon de commencer par désactiver un mot qui fait peur sans raison : serveur. Un serveur n'est pas une machine mystérieuse dans une salle réfrigérée. C'est, simplement, l'ordinador d'une autre personne —ou le vôtre — qui conserve des informations et les livre à celui qui les demande. Pendant des décennies, nous avons conservé les informations de nos clients dans un dossier, dans un classeur, sur le bureau et personne ne perdait le sommeil pour cela. L'information n'était pas effrayante parce qu'elle était sur papier ; elle n'a pas à l'être non plus parce qu'elle est sur un disque.

Le « cloud » n'est pas non plus éthéré. C'est l'ordinateur d'une entreprise, presque toujours loin et presque toujours celui d'un autre. Je l'ai appris involontairement le jour où, confiant que mes fichiers étaient en sécurité dans Google Drive, j'ai découvert que le dossier de mon ordinateur ne contenait pas mes documents, mais des raccourcis vers des documents qui vivaient ailleurs. Si cet autre endroit décidait de fermer, de changer de prix ou d'annuler le service, ma tranquillité s'en irait avec lui. Je ne possédais pas mes affaires ; j'avais la permission d'y accéder.

C'est de là que naît la question de ce Cahier, plus simple à formuler qu'à résoudre : où devraient vivre les données de vos clients ? Et les vôtres ? Le débat public la pose comme s'il n'existait que deux réponses opposées — le nuage des grandes plateformes ou se débrouiller soi-même —, presque une question de camp. Mais il n'y a pas deux chemins : il y en a trois, et aucun n'est un acte de foi. Lus posément, ils comportent plus de nuances et exigent plus qu'il n'y paraît.

Cela vous concerne, peu importe ce que vous vendez

Il est facile de penser que la confidentialité est l'affaire des avocats, des médecins ou des journalistes, et que le reste n'a rien à cacher. C'est une erreur, et une erreur coûteuse. Presque n'importe quelle entreprise conserve des données de ses clients soumises à la loi, et beaucoup conservent, sans le savoir, des informations bien plus sensibles qu'il n'y paraît.

Un magasin de canapés note le nom, l'adresse et le téléphone de qui achète ; s'il y a un financement, ses données économiques aussi. Une entreprise de rénovation ou de décoration conserve des photos de l'intérieur des maisons de ses clients et les plans complets de leurs logements. Une entreprise de nettoyage manie les plans des bureaux qu'elle nettoie, souvent annotés de couleurs et de chiffres indiquant quel employé entre où, à quelle heure et avec quelle clé. Rien de tout cela ne semble grand-chose jusqu'à ce qu'on se demande pour qui d'autre cela aurait de la

valeur : ces plans de nettoyage sont, vus avec d'autres yeux, la carte parfaite pour quiconque voudrait s'introduire pour voler.

Le fait qu'une entreprise soit petite, ou qu'elle vende des canapés au lieu de défendre des litiges, ne rend pas ses données sans valeur ni ne fait que la loi cesse de s'y appliquer. Cela fait seulement que son propriétaire a tendance à moins y penser. Et penser peu à quelque chose qui est votre responsabilité est précisément là où les problèmes commencent.

Où vivent vos données ?

À cette question, il y a, en substance, trois réponses. Et il convient de rappeler que « les données » ne sont pas seulement le dossier d'un client ou le bloc de factures et de devis : ce sont aussi vos conversations avec lui — par WhatsApp, par un service de messagerie professionnel, par Solo2. Les trois réponses qui suivent ne sont pas des degrés de pureté ni une échelle des bons aux mauvais : ce sont trois manières de répartir une même chose, le contrôle et la responsabilité.

Tout déléguer à un prestataire. C'est le plus courant, et pour la plupart c'est la seule chose qu'ils connaissent. Je mets tout dans Google Workspace ou dans Microsoft 365 et je le confie entièrement au prestataire. Je paie mon abonnement et je cesse d'y penser. La forme la plus extrême de cela, ce sont les services où vous n'avez même pas vos propres données : certains logiciels de facturation dans le nuage, par exemple, conservent vos factures et vos devis — et fonctionnent très bien —, mais l'information vit dans leur système, pas dans le vôtre. Tant que vous payez, vous accédez ; le jour où vous partez, vous découvrez qu'emporter votre propre historique est difficile ou impossible. Garder vos données à moitié en otage est, pour plus d'un prestataire, justement ce qui vous empêche de partir à la concurrence. En échange de la commodité, je cède le contrôle et — sans le dire à voix haute — le sentiment que la responsabilité n'est plus la mienne. Ici tient une nuance qu'on ne fait presque jamais : déléguer n'est pas synonyme d'américain. Je peux tout déléguer tout aussi commodément à un prestataire européen — Infomaniak, par exemple — et résoudre d'un seul coup une bonne partie des doutes sur les transferts internationaux que nous avons vus dans « Schrems II », sans rien auto-héberger. Ce n'est pas les États-Unis contre le reste de l'univers : au sein même de la pure délégation, il y a déjà des décisions qui comptent.

Louer et gérer votre propre serveur. J'ai la même chose que ce que Microsoft ou Google me donneraient, mais je l'installe moi-même. Je loue un serveur chez un fournisseur européen —Hetzner, OVH, Scaleway—, j'installe des logiciels libres (Nextcloud pour les fichiers, par exemple) et j'administre moi-même le résultat. Je gagne un contrôle réel : je sais ce qui tourne, où et pourquoi. Mais la machine se trouve toujours dans le centre de données d'un tiers et, surtout, celui qui en supporte les conséquences change. En déléguant, si quelque chose échoue, vous avez quelqu'un à blâmer. En gérant vous-même, il est fort probable que la faute soit vôtre.

L'avoir sur votre propre ordinateur. C'est l'option que presque personne ne raconte, et c'est le cœur de ce Cahier. Vous n'avez pas besoin d'un énorme serveur allumé vingt-quatre heures sur vingt-quatre à l'intérieur d'un macro centre de données pour héberger vos affaires. L'ordinateur de votre bureau est déjà un serveur : il vous sert. Vous le laissez allumé au bureau et vous vous y connectez depuis votre ordinateur portable chez un client, ou depuis votre mobile quand vous êtes à la maison. Nous l'appelons « l'ordinateur du bureau », pas « le serveur », mais il fait exactement la même chose que les deux options précédentes. Le contrôle est maximum et la proximité aussi : vos données sont là où vous êtes. La contrepartie, dite sans fioritures, est que la responsabilité est aussi maximum. S'il y a une coupure de courant, il n'y a pas de technicien de garde à Nuremberg : c'est à vous de relever le disjoncteur. Et pour que cet ordinateur soit accessible de l'extérieur, il faut quelque chose qui jette le pont entre votre portable et lui. Ce n'est pas de la magie, et il est bon de le savoir avant de choisir cette voie.

Et il n'est même pas nécessaire de réutiliser l'ordinateur du bureau : il existe un appareil conçu précisément pour cela, le NAS (fabriqué par Synology, QNAP et d'autres). Comme presque tout ce que nous avons vu dans ces Cuadernos, il n'y a aucune magie à l'intérieur : c'est un ordinateur spécialisé, le même type de machine que vous loueriez dans un centre de données, mais conçu pour stocker des données et les servir sur le réseau, sans écran ni clavier au milieu. Branchez-y un écran et un clavier et vous obtenez un ordinateur ordinaire ; installez le logiciel adéquat sur votre PC et vous obtenez un NAS. La différence, c'est que le NAS arrive prêt à l'emploi. Vous

l'achetez, vous le branchez chez vous ou au bureau, et il est à vous. Vous ne payez pas d'abonnement mensuel ; vous le payez une fois et il vous appartient, comme n'importe quel outil de votre entreprise. Vous l'allumez, vous l'éteignez, vous l'emportez ailleurs si vous le souhaitez. Et comme il est à vous, rien ne vous empêche d'en avoir deux —un à la maison, un au bureau— ou trois, en ajoutant un dans un lieu sûr, synchronisés entre eux : votre propre redondance, sans dépendre d'un tiers pour la maintenir. L'auto-hébergement, au fond, n'est pas une seule chose : c'est une combinaison de machines, de propriété, d'emplacements et de logiciels.

Ici, il est inévitable de nommer ce que nous faisons, et nous le faisons sans déguisement : chez Solo2, ce pont, c'est l'application elle-même qui le tend. L'ordinateur de votre bureau reste accessible uniquement à vos appareils de confiance, et toujours sous chiffrement, et vos autres appareils s'y reconnectent tout seuls. Quand un client vous parle, c'est votre ordinateur — pas celui d'un tiers — qui parle au client. Nous ne résolvons pas la coupure de courant ; nous résolvons le pont. Et nous ne sommes pas les seuls : pour presque chaque besoin il existe aujourd'hui des programmes — libres ou propriétaires — qui permettent justement cela, avoir les données sur votre matériel et y accéder depuis l'extérieur. Le nôtre est un exemple ; l'important, c'est l'idée, pas la marque.

La redondance n'est pas un super-pouvoir

Ici surgit l'objection immédiate, et elle est raisonnable : si j'ai tout sur l'ordinateur du bureau, que se passe-t-il s'il tombe en panne ? La question est bonne. La réponse est que le filet de sécurité que nous imaginons chez les grands fournisseurs est plus modeste —et plus imitable— qu'il n'y paraît.

Quand je laisse mes données dans le centre de données d'une multinationale, j'ai confiance qu'elle ait des copies à plusieurs endroits. Et probablement qu'elle les a : dans un second emplacement, peut-être dans un troisième. Mais cette redondance n'est pas infinie et surtout elle n'est pas mienne : cela reste un disque dur dont je ne suis pas le propriétaire, géré par quelqu'un en qui je place une foi que je ne vérifie presque jamais.

Ce même réseau, je peux le tisser moi-même, et avec un avantage décisif. Mon service quotidien vit sur l'ordinateur du bureau. De là, je garde une copie cryptée sur l'ordinateur d'une entreprise amie —un confrère, un autre bureau de confiance— et une autre copie cryptée, si je le veux, chez ce même fournisseur européen dont nous parlions. La différence est tout : ce que je laisse à l'extérieur n'est pas mon service ni mes données en clair, mais une copie cryptée que seul moi peux ouvrir. Le fournisseur externe garde un coffre fermé dont il n'a pas la clé. Je ne lui confie pas mon information : je lui confie quelques octets qui, sans moi, ne signifient rien.

C'était en sécurité jusqu'à ce que ça ne le soit plus

Permettez-moi une histoire personnelle, car elle illustre cela mieux que n'importe quel argument. Pendant plus de dix ans, j'ai été un client dévoué de CrashPlan, un service de sauvegarde techniquement extraordinaire. Je sauvegardais dans leur cloud tous mes ordinateurs et ceux de ma famille —ceux de l'entreprise et ceux de la maison, tout—, avec des versions que je pouvais récupérer à la fréquence que je voulais, en remontant le temps jusqu'à un fichier spécifique d'il y a plusieurs mois. Après la première copie, il ne transmettait que les différences, cryptées et compressées, de sorte que je maintenais à jour une énorme sauvegarde avec presque aucun effort. Cela m'a sauvé maintes fois, d'un simple document à un disque entier. Le prix a augmenté au fil des ans et je m'en fichais : je payais avec plaisir.

Ce que je ne savais pas, c'est que CrashPlan avait commis une erreur de calcul : ils avaient promis par contrat un stockage illimité, en espace et en temps. Et l'espace multiplié par le temps —des années d'historique, des versions toutes les quelques minutes— croît jusqu'à devenir insoutenable. Un jour, ils nous ont tous informés que le service prenait fin. Ils l'ont fait avec élégance et avec un délai généreux, presque un an, et nous ont donné les moyens de télécharger nos données. Mais où va-t-on avec plus de dix ans de copies versionnées de tous ses disques ? C'est là que vous découvrez que vous n'avez ni le moyen de tout télécharger ni l'endroit où le mettre, et que, même si vous le pouviez, le nouvel entrepôt coûterait une fortune.

J'ai sauvé quatre choses indispensables. Le reste est parti quand ils ont coupé l'interrupteur. J'étais tranquille, mes informations étaient à l'abri... jusqu'à ce qu'elles ne le soient plus. Et non par une trahison : CrashPlan s'est comporté de façon impeccable — contrairement à Evernote, qui des années plus tard s'est comporté de façon honteuse — ; tout simplement, mon ange gardien dans le nuage a décidé, en toute légitimité, de cesser de l'être. Le résultat, pour moi, fut identique : ce que je croyais en sûreté a disparu.

Ce que cette histoire enseigne réellement a plus à voir avec la nature humaine qu'avec la technologie. Quand quelqu'un sent que quelque chose est sa responsabilité, il agit de manière préventive : il fait des copies, assure ses arrières, se méfie avec bon jugement. Quand il croit —à tort— que la responsabilité est portée par un tiers grand et solvable, il se relâche et laisse faire. Cette tranquillité déléguée n'est pas de la prudence : c'est, sans maquillage, une forme d'irresponsabilité.

Payer n'est pas la même chose que se conformer

Cette irresponsabilité tranquille ressemble beaucoup à celle de parents qui inscrivent leur fils dans l'école la plus chère, lui paient ensuite un master, et croient ainsi avoir accompli leur devoir. Ils ne l'ont pas accompli. Être parent, c'est s'inquiéter de ce qu'il a appris aujourd'hui, de ce qu'il ne comprend pas, de ses valeurs, de sa confiance en soi. Si à vingt-cinq ans ce fils ne sait ni travailler ni se comporter, la faute n'est pas à l'école qui a encaissé l'argent : elle est à celui qui a délégué et payé en croyant que cela suffisait. Payer un tiers n'exempte pas de responsabilité. Cela ne l'a jamais fait.

Avec les données, c'est pareil, et l'histoire récente le confirme. Il y a cinquante ou cent ans, un professionnel rangeait les affaires de ses clients dans des dossiers, à son cabinet ou chez lui, et s'en sentait responsable. Il était rare que quelque chose se perde. Nous sommes passés au monde numérique et, avec une facilité stupéfiante, nous téléversons tout vers « le nuage » — qui n'est rien d'autre que l'ordinateur d'une multinationale — et cessons de nous en soucier. Et il y a souvent des accidents, et il y a des entreprises qui perdent tout, et alors on dit : la faute à Google, la faute à Microsoft. Non. L'information est la vôtre, ou celle de vos clients, mais le responsable, c'est vous.

Héberger vos propres données n'est pas un caprice technique : c'est récupérer cette sérénité d'il y a des décennies, celle de savoir où est chaque chose et pourquoi. La protection des données, entre-temps, a connu un brusque balancement de pendule —de l'absence de toute norme, quand n'importe qui exposait les données d'un client sans réfléchir, à une exigence qui retombe avec une dureté disproportionnée sur le plus petit, le travailleur indépendant qui donne le téléphone d'un client au livreur. Je ne discute pas la finalité ; j'observe le désajustement. Mais le désajustement ne nous absout pas : le jour où l'administration aura les moyens de tracer et de sanctionner à grande échelle, la taille cessera de protéger quiconque, et il est sage de ne pas attendre ce jour avec une maison en désordre. Avoir la donnée sous son propre contrôle aide à se conformer et aide à le prouver. Et surtout, cela remet les choses à leur place : quand l'information est la vôtre, la responsabilité est entièrement la vôtre —il n'y a pas de tiers à blâmer, ni de tiers dont la défaillance vous expose—.

La responsabilité protège aussi

Il serait malhonnête de peindre cela sans ombres. Prendre la place de l'intermédiaire signifie en porter le poids : maintenir les sauvegardes à jour, appliquer les mises à jour, et une responsabilité légale — celle du RGPD — qui, en réalité, n'a jamais tout à fait cessé d'être la vôtre (les références en bas de page détaillent les articles). Il y a du travail, et il y a un jour où quelque chose lâche au mauvais moment. Nous ne le cachons pas.

Mais la peur qui entoure ce mot, responsabilité, est mal calibrée. Il est bien plus facile de perdre vos fichiers dans un service de nuage qui ferme, ou vos photos dans Google Photos, que de perdre ce dossier de documents importants que vous avez sur votre propre ordinateur : celui dont vous savez où il est et dont vous remarqueriez l'absence dès qu'il disparaîtrait. Ce que vous sentez vôtre, vous en prenez soin ; ce que vous croyez à l'abri entre les mains d'un autre, vous le négligez.

Pensez aux albums photo d'autrefois, ceux en papier développé rangés dans un tiroir. Avez-vous jamais entendu quelqu'un dire qu'il a « perdu » son album de famille ? On entend parler de la maison qui a brûlé avec l'album dedans ; le perdre comme ça, non. Et en revanche, des gens qui avaient toutes leurs photos dans Google Photos ou dans Apple Photos et qui se sont retrouvés sans rien : cette histoire revient tous les quelques mois, parce qu'ils croyaient que c'était à l'abri. Google Photos prend soin de vos photos, bien sûr ; mais il n'en prend pas soin comme des parents prennent soin de l'album où se trouvent leurs enfants et leurs petits-enfants. Cette différence, aucun centre de données ne la corrige : la responsabilité, quand elle est vôtre, n'est pas seulement un fardeau ; c'est aussi la meilleure garantie.

Quatre questions avant de décider

Si vous envisagez de franchir le pas, sous l'une de ses formes, il est bon de répondre d'abord à quatre questions avec une honnêteté dépassionnée :

1. Quelle partie de vos données vous ferait mal de perdre, ou de ne pas pouvoir emporter ? Et attention à ne pas écarter le « routinier » : l'historique des factures semble la chose la plus prosaïque du monde jusqu'à ce que vous changiez de logiciel et découvriez que ces factures étaient celles du prestataire, pas les vôtres — que, tout au plus, vous pouvez les imprimer en PDF, sans plus pouvoir chercher dedans. Ce n'est pas seulement une question de sensibilité : c'est de savoir à qui appartient vraiment ce que vous avez besoin de conserver.
2. Quelle option est proportionnée à votre capacité technique réelle ? Un ordinateur à soi, bien entretenu, est à la portée de tous ; administrer un serveur entier, beaucoup moins. Soyez honnête sur ce que vous savez et ce que vous ne savez pas. Et rappelez-vous qu'entre monter un serveur entier et tout déléguer il y a un terrain intermédiaire très raisonnable : des programmes — libres ou propriétaires — qui gardent vos données sur votre propre matériel et vous laissent y accéder depuis l'extérieur. Pour bien des gens, c'est le meilleur équilibre.
3. Quel plan avez-vous pour le pire jour ? Une violation, un disque qui meurt, un fournisseur qui ferme, le technicien en arrêt maladie. Si le plan commence par « cela ne devrait pas arriver », ce n'est pas un plan.
4. Sauriez-vous prouver que vous êtes en règle si demain vous étiez inspecté ? Bien faire et pouvoir prouver que l'on fait bien ne sont pas la même chose. La loi demande la seconde.

Il n'y a pas de réponse universelle. Il y a une réponse proportionnée, adoptée avec honnêteté sur ce qui est gagné et ce dont on hérite. Et au-delà de la technique, une certitude simple : vos données vivent dans l'ordinateur de quelqu'un. La seule question qui compte réellement est de savoir de qui vous voulez que soit cet ordinateur.

L'auto-hébergement n'est ni une vertu ni un vice : c'est un outil avec une empreinte concrète de capacités et de responsabilités. La question n'a jamais été de savoir s'il fallait héberger vos données, mais quelles données, comment et avec quel réseau de soutien. Reprendre le contrôle des données ne signifie pas retourner à la cave ni se méfier de tout : c'est recommencer à se sentir responsable de ce qui nous appartient, comme à l'époque où ces données vivaient dans un dossier sur le bureau. Cette responsabilité, bien comprise, est le véritable service qu'un professionnel rend à ses clients.

Sources et lectures complémentaires

- Règlement (UE) 2016/679 — article 28 (sous-traitant), article 32 (sécurité du traitement), article 33 (notification d'une violation), article 37 (désignation du délégué à la protection des données).
- Agence Espagnole de Protection des Données — *Guide pratique pour l'analyse des risques dans le traitement des données à caractère personnel* (révision en vigueur). Cadre pour les responsables qui assument leurs propres fonctions techniques.
- Comité Européen de la Protection des Données — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Applicable aussi à l'examen de proportionnalité dans les décisions d'infrastructure propre.

- Commission Européenne — répertoire public des fournisseurs de services d'information établis en juridiction européenne. Point de départ administratif pour identifier les options d'hébergement managé européen.
- Nextcloud GmbH (Allemagne) — *Nextcloud Enterprise architecture and compliance documentation*. Cas documenté de logiciel libre avec des modalités auto-hébergées et managées par un fournisseur européen ; utile comme référence technique d'un projet maintenu en juridiction européenne depuis 2016.

← PrécédentLes 24 mots : qu'est-ce qu'une identité cryptographiqueSuivant →Confidentialité réelle vs apparente : les questions à se poser

Lectures recentes

- Réflexion · 29 juin 2026 Vous n'êtes pas anonyme
- Réflexion · 27 mai 2026 Ce qu'une signature ne peut pas réparer
- Analyse · 26 mai 2026 Confidentialité réelle vs apparente : les questions à se poser

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 dd166b6379dca9b4e920070ac9e911abced40981804409beeba50678730c833d

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