Ce qu'une signature ne peut pas réparer

Lorsqu'un canal technique ne convient pas aux données sensibles, aucune autorisation signée ne le rend adéquat. La seule chose qu'une signature change, c'est la fausse tranquillité de celui qui la recueille ; les données suivent exactement le même chemin.

Pour bien se comprendre : En réunion, quelqu'un dit avec la meilleure intention du monde : « tout le monde utilise WhatsApp ; on fait signer une autorisation aux clients et c'est réglé ». Cela ressemble à de la diligence — il y a un papier, une signature, une date. Mais cette signature ne déplace pas les données, et celui qui signe n'est presque jamais la seule personne dont l'intimité voyage sur ce canal. Et même s'il l'était, aucune signature ne légalise une illégalité.

L'issue qui semble de bon sens

La scène se répète dans les bureaux, les consultations et les conseils — et aussi dans des lieux beaucoup moins solennels. Le peintre qui envoie des photos de l'appartement d'un client. Le plombier qui transfère une facture avec le nom, l'adresse et le téléphone. Le chauffeur de taxi qui garde sur son mobile l'adresse de celui qu'il récupère chaque matin. L'indépendant qui transmet par chat le numéro de sécurité sociale de celui qui l'a embauché. Pas besoin d'un scénario de film judiciaire pour que des données de personnes tierces circulent sur un téléphone.

Et dans n'importe lequel de ces lieux apparaît, tôt ou tard, la même issue élégante. Quelqu'un soulève le doute — est-ce correct d'envoyer ceci par ici ? — et, avant que la conversation ne devienne embarrassante, arrive la réponse facile : que le client signe une autorisation. S'il donne son accord, c'est bon.

C'est une issue attrayante car elle résout l'embarras sans obliger à changer d'outil, sans rien apprendre de nouveau, sans coût. Elle a la forme de la diligence : un document, une signature, une date. Et pourtant, elle ne résout pas le problème qu'elle prétendait résoudre. Elle le cache.

Une signature ne déplace pas les données

Il convient de commencer par le plus simple, car c'est précisément ce qu'on oublie. Une autorisation est un papier. Elle ne change pas le trajet du message, ni le serveur sur lequel une copie est conservée, ni qui peut la lire si une injonction arrive ou s'il y a une faille. Le document du client continuera de passer par la même infrastructure, dans le même pays, gérée par la même entreprise, avec ou sans signature.

La seule chose qui change avec la signature, c'est l'état d'esprit du professionnel : il passe du doute à une fausse tranquillité qui ne correspond à aucun changement réel dans le parcours des données. La signature est un permis que l'on s'accorde à soi-même pour continuer à faire exactement la même chose.

Le permis que personne dans la salle ne pouvait donner

C'est ici que se trouve le nœud du problème. Pensons à un divorce. Le client signe l'autorisation : d'accord, que ses données passent par où il faut. Mais par ce canal, ce ne sont pas seulement les données du client qui voyagent. Le nom de l'autre partie y circule. Les données du mineur dont la garde est discutée y circulent. Le rapport de l'expert, le témoignage d'un tiers, le numéro de compte du conjoint y circulent.

Aucune de ces personnes ne s'est assise dans le bureau. Aucune n'a rien signé. Le professionnel a obtenu l'accord de la seule personne qui n'était pas tout le problème, et a continué à traiter les données de toutes celles qui l'étaient sans rien leur demander — parce qu'il ne pouvait pas leur demander.

Il en va de même pour un dossier de travail qui mentionne d'autres employés, un rapport clinique qui parle de membres de la famille, ou une déclaration qui regroupe les fournisseurs et clients du client lui-même. L'information d'un tiers ne cesse pas d'être protégée parce que la personne qui la fournit a signé un papier. Elle n'était pas à elle pour pouvoir l'autoriser.

Il y a des choses qu'une signature n'atteint pas

Il y a une limite que nous ne testons presque jamais : une signature ne va que jusqu'où va ce qui est à vous. Ce qui est à vous, vous pouvez le céder. Ce qui est à autrui, non — même si vous signez avec votre plus belle plume.

Un père ne peut pas signer un permis pour que l'on fasse du mal à son fils. Ce papier ne vaut rien, et pas parce qu'il lui manque un sceau : parce que ce permis n'a jamais été entre ses mains pour le donner. L'autorisation du client fonctionne de la même manière — elle couvre ce qui est à lui et s'arrête là.

Et même dans cette limite, elle ne couvre pas tout. Une signature ne rend pas licite ce que la loi ne consent pas, peu importe qui la signe. Le consentement n'est pas un passe-partout : c'est une clé qui n'ouvre qu'une seule porte — la sienne —, et même cette porte ne donne pas accès à ce qui est interdit.

Et il faut le dire sans détour, car c'est la partie que l'on ne dit presque jamais : demander — ou donner — une signature pour blinder ce que la loi ne permet pas n'est pas un geste neutre qui n'aurait simplement pas d'effet. Selon le cas, tenter de le faire est, en soi, une nouvelle infraction. Cela ne règle pas le problème : cela l'aggrave.

La signature qui se retourne contre soi

Et il y a un revirement qu'il convient de regarder en face. Recueillir l'autorisation ne laisse pas le professionnel tel qu'il était : cela le laisse dans une pire situation.

Parce que ce papier est, avant tout, la preuve que quelqu'un s'est posé la bonne question — est-ce adéquat ? — et y a répondu par un placebo au lieu d'une solution. Le jour où il faudra expliquer pourquoi les données d'un tiers ont fini là où elles ne devaient pas, l'autorisation signée ne sera pas le bouclier imaginé : ce sera le document qui démontre que l'on connaissait le risque et que l'on a choisi de le masquer avec une signature. La diligence apparente laisse une trace. La signature n'archive pas le problème ; elle le date.

La seule chose qui le répare vraiment

Si une signature ne répare rien, qu'est-ce qui le fait ? Une seule chose : que les données n'aillent pas là où elles ne doivent pas aller.

Quand le canal ne délivre pas de copie du document à un tiers — parce qu'il va directement de l'appareil de celui qui l'envoie à celui de celui qui le reçoit, sans serveur intermédiaire qui le conserve — il n'y a rien à autoriser, personne à qui demander la permission, ni trace embarrassante à justifier après coup. Le problème ne se gère pas avec un formulaire : il disparaît parce que l'architecture ne permet pas de le créer.

Ceci n'est pas la propriété d'un seul outil — c'est une propriété de la conception, et il y a plus d'une façon de l'avoir. Ce qui distingue ces outils du reste n'est pas une promesse mieux rédigée dans les mentions légales, mais le fait qu'ils n'ont besoin de la signature de personne pour être en règle.

Une signature est la forme civilisée de demander la permission. Mais on ne peut demander la permission qu'à celui qui est présent. Et dans presque toutes les données sensibles qu'un professionnel manipule, les personnes dont l'intimité est réellement en jeu ne sont pas dans la salle, ne signeront pas, et n'auraient aucune raison de faire confiance à quelqu'un qui signe pour elles. C'est pourquoi la bonne question n'a jamais été « comment faire pour que ceci soit autorisé ? », mais « pourquoi ai-je besoin d'une autorisation pour quelque chose qu'un canal bien choisi ne m'obligerait pas à demander ? ».

Note éditoriale : quand ces Cuadernos nomment des entreprises ou des produits, ce n'est pas pour accuser. Ceux qui les construisent font un travail que des millions de personnes utilisent et apprécient. Ce que nous soulignons est structurel — le modèle, pas la marque. Les marques apparaissent comme exemples car ce sont celles que le lecteur reconnaît.

Pour aller plus loin

- Ce Cuaderno laisse de côté, à dessein, le détail normatif — les articles et les sentences —, car l'argument qu'il démonte n'est pas juridique : c'est une issue de confort. L'armature légale expliquant pourquoi le canal importe se trouve dans les deux Cuadernos suivants.
- *RGPD et messagerie professionnelle : pourquoi la plupart enfreignent les règles sans le savoir* — transferts internationaux, responsable du traitement et trace numérique rétroactive.
- *Le secret professionnel à l'ère numérique* — pourquoi la confidentialité doit être garantie par l'architecture et non par une promesse.

← PrécédentConfidentialité réelle vs apparente : les questions à se poser

Lectures recentes

- Analyse · 26 mai 2026 Confidentialité réelle vs apparente : les questions à se poser
- Analyse · 25 mai 2026 Self-hosting comme pratique professionnelle
- Concept · 23 mai 2026 Les 24 mots : qu'est-ce qu'une identité cryptographique

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 84322d539e39156f15fc8b60beed49439db9866ba395d8b681a26930fca2e35e

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