

Jabber/XMPP

25 years of Digital Independence



Daniel Gultsch - August 24, 2026

Infrastructure

« Nos infrastructures devraient nous appartenir. » Beaucoup de gens approuvent par instinct cette affirmation. Pourtant, l'identité de ce « nous » varie selon le type d'infrastructure. Les autoroutes, les voies ferrées, les ponts et les ports nécessitent des efforts à l'échelle d'une Nation. La gestion des réseaux d'eau est généralement confiée aux municipalités. Et ce désir d'autonomie s'exprime aussi à une échelle bien plus réduite : être propriétaire de son logement est un rêve pour beaucoup — mais cette propriété ne doit pas nécessairement être individuelle. Les coopératives d'habitation ou le logement social¹ peuvent offrir des avantages similaires.

Le néocolonialisme de la Chine, qui se manifeste notamment par la construction et le rachat d'infrastructures dans des États souverains, est légitimement critiqué. Refuser de vendre ses sources d'eau à Nestlé est une position universellement admise, et les propriétaires immobiliers figurent parmi les classes les plus détestées.

Pendant longtemps, l'Europe n'a pas appliqué les mêmes exigences aux services numériques. Cela s'explique en partie par le fait que l'Europe incluait implicitement les entreprises américaines dans un « nous » collectif — une hypothèse qui s'est officiellement effondrée sous l'administration Trump, mais qui aurait dû être accueillie avec scepticisme bien avant cela. Les entreprises ne sont pas nos amies. Plus largement, l'Europe n'avait tout simplement aucune considération pour les infrastructures de services numériques. Si l'antiaméricanisme revient à la mode et alimente une grande partie du mouvement pour la souveraineté numérique, l'Europe ne doit pas se contenter de remplacer les entreprises américaines par des entreprises européennes, mais s'orienter vers des propriétés collectives.

Sous le système capitaliste, les entreprises auront toujours un rôle dans la construction ou l'exploitation de nos infrastructures, mais doivent rester interchangeable. Si une entreprise construit une route, l'entretien et la réparation 50 ans plus tard doit pouvoir être confiée à un autre prestataire. Il est acceptable qu'une entreprise construise et exploite les lignes à haute tension, mais elle ne doit pas en être propriétaire. Nous voulons que de plus petits acteurs puissent s'interconnecter au réseau et y participer. C'est là

¹https://en.wikipedia.org/wiki/Housing_in_Vienna

qu'interviennent les standards² ouverts.

Internet a été — et l'est encore, dans une certaine mesure — bâti autour de standards. Un datacenter peut acheter des serveurs auprès d'un fournisseur, des switchs auprès d'un autre, des routeurs auprès chez un troisième, et les connecter à un fournisseur d'accès qui utilise du matériel d'un autre constructeur encore. Si l'une de ces entreprises fait faillite ou déçoit ses clients par ses pratiques, on peut commander chez une autre. Les avantages de cette indépendance d'approvisionnement sont évidents, même pour ceux dont ce n'est pas le métier. Pourtant, dès qu'on parle d'outils de communication, même les personnes les plus renseignées oublient d'appliquer ce même raisonnement.

Communiquer est sans doute la quatrième activité la plus importante pour les êtres humains après respirer, manger et se reproduire. Pourtant, on considère rarement nos outils de communication comme des infrastructures.

Les activistes citent souvent Signal, Wire et Threema comme exemples de chats développés et gérés par des organisations un peu plus éthiques que les géants de la tech. Mais au-delà de la confidentialité, ces entreprises continuent d'entretenir des écosystèmes fermés dont on ne peut s'extraire. Elles ne sont pas interopérables. Signal n'a pas agi de manière intrinsèquement malveillante — bien que verser près d'un million de dollars par an à son PDG et héberger ses serveurs sur AWS soient des choix discutables — le problème est que nous ne disposons d'aucun plan B si cela devient le cas.

La question du logiciel libre est orthogonale à ce problème. La liberté permet de garantir que le logiciel n'est pas un logiciel espion — contrairement à WhatsApp et aux autres produits de Meta³ — et que le chiffrement de bout en bout est fiable, mais n'empêche pas Signal de fermer ses serveurs ou de cesser ses activités dans l'UE⁴). Le logiciel libre ne suffit pas, à lui seul, à répondre aux exigences que nous devrions avoir pour notre infrastructure.

Pour être à la hauteur, nous devons concevoir des systèmes où l'auto-hébergement est structurellement possible, mais n'est pas nécessaire. Tout comme il est possible d'être propriétaire de son logement, il devrait être possible de gérer son propre serveur ; il en va de même pour la propriété

² **NdT:** *standard* en anglais est traduit par *norme* ou *standard* de façon interchangeable

³ <https://localmess.github.io/>

⁴ https://mastodon.world/@Mer__edith/112535616774247450

collective. Les systèmes numériques devraient offrir les avantages de la propriété individuelle et de la propriété collective.

Considérer la communication numérique comme une véritable infrastructure ne peut se faire qu'en adoptant et en imposant des normes ouvertes (standards).

Le protocole XMPP (Extensible Messaging and Presence Protocol)⁵⁶ est une norme de communication en ligne. Il n'a pas été conçu pour répondre au climat politique actuel. En réalité, il a plus de 25 ans.

Normes

L'interopérabilité et l'indépendance vis-à-vis des fournisseurs reposent sur l'introduction et le suivi de normes. Afin d'éviter qu'un fournisseur n'impose des normes excluant explicitement ou implicitement ses concurrents, ou lui conférant des avantages déloyaux, des organismes de développement de standards (SDO) ont été créés pour favoriser la coopération mutuelle. Ceux-ci ont généralement des garde-fous pour empêcher une seule entreprise d'acquérir trop d'influence. Parmi les SDO connus, on peut citer l'ISO, l'IETF, le W3C et le Consortium Unicode.

Il est important de distinguer la situation où un fournisseur publie son API en autorisant des tiers à l'utiliser de celle où des individus se réunissent pour élaborer collectivement une norme dans le cadre d'un organisme de développement de standards. Les SDO comme l'IETF fonctionnent parce qu'elles poussent au consensus des personnes avec des besoins différents. Les protocoles ne sont pas dictés par les priorités d'une entreprise ; ils sont au contraire revus et testés par des entités concurrentes, des chercheuses en sécurité et des développeuses indépendant-es.

L'entreprise Element (anciennement Riot et NewVector) développe une messagerie instantanée aux fonctionnalités similaires à XMPP — telles que l'auto-hébergement et la fédération. Mais, au lieu d'adopter XMPP, elle a préféré publier sa propre API baptisée Matrix pour que les autres l'adoptent. Contrairement à un standard traditionnel, Element garde un contrôle étroit sur toute évolution de son API publique. Les postes-clé au sein de la Matrix Foundation sont majoritairement occupés par des employéEs (présent ou

⁵<https://www.rfc-editor.org/rfc/rfc6120.html>

⁶<https://www.rfc-editor.org/rfc/rfc6121.html>

passé) d'Element. Il est notoirement difficile de faire accepter des contributions externes dans la spécification.⁷ En quête de souveraineté numérique, les administrations publiques européennes tombent dans le piège de telles plateformes contrôlées par un fournisseur unique, confondant code open-source et norme ouverte.

C'est naturel que les propositions de standards émergent dans une seule organisation. JMAP — un remplaçant moderne d'IMAP et de SMTP Submission, assez proche de Matrix (une API JSON sur HTTP) — a vu le jour chez Fastmail avant d'être soumis à l'IETF. Jabber a débuté comme un projet communautaire open source avant d'être présenté à l'IETF et rebaptisé XMPP. Les idées démarrent modestement, mais pour créer un standard, il faut des avis extérieurs, de la collaboration et le cadre d'un organisme de développement de standards (SDO).

La différence d'approche entre Fastmail et Element est frappante pour les utilisatrices. Non seulement le protocole JMAP a été considérablement amélioré grâce au groupe de travail de l'IETF, mais il dispose désormais d'au moins trois implémentations de serveurs et beaucoup plus de clients. À l'inverse, Matrix — né à la même époque vers 2014 — n'a toujours qu'une implémentation de référence, tandis qu'une seconde peine à émerger. Cette solution de référence est célèbre pour son usage abusif de ressources, ce qui rend l'auto-hébergement difficile pour les petites organisations et les personnes. Element commercialise des extensions propriétaires pour améliorer les performances.

Le « X » de XMPP

Les origines de XMPP — d'abord nommé Jabber — remontent à plus d'un quart de siècle. La RFC initiale⁸ date d'octobre 2004 et a été légèrement révisée en mars 2011⁵. Or, les besoins en matière de messagerie instantanée évoluent sur une si longue période. Heureusement, le « X » de XMPP signifie « Extensible ». Le protocole peut évoluer grâce à des extensions: les XEP (**XMPP Extension Protocols**). Ces extensions sont gérées par la XMPP Standards Foundation (XSF). La XSF ne les rédige pas, mais fournit plutôt le cadre

⁷<https://github.com/matrix-org/matrix-spec-proposals/pull/4174>

⁸<https://www.rfc-editor.org/rfc/rfc3920.html>

(SDO) permettant aux développeuses de proposer et de standardiser leurs propres extensions.

Adapter le protocole à un cahier des charges mouvant n'est pas toujours facile. La XEP-0198 (**Stream Management**), une extension cruciale pour éviter de perdre des messages lors sur mobile, a été stabilisée en 2009, mais n'a été largement déployée que vers 2014-2015. Le premier iPhone est sorti en 2007, et le premier Android (HTC Dream) en 2008. OMEMO (XEP-0384), extension pour le chiffrement de bout en bout, a gagné en popularité à partir de 2016, trois ans après qu'Edward Snowden⁹ a révélé la surveillance massive de la NSA et donc le besoin de chiffrement. Les articles « The (Sad) State of Mobile XMPP in 2014 » de Georg Lukas¹⁰ et « The State of Mobile XMPP in 2016 » de l'auteur de ces lignes¹¹ illustrent cette transition difficile vers l'ère mobile.

Cela montre qu'avoir des standards ne suffit pas. Les normes doivent s'appuyer sur de multiples implémentations, de préférence indépendantes. Aujourd'hui, la XSF assure le suivi de l'état d'implémentation de ses XEP¹². Ces données aident les auteurices et la XSF suivre le cycle des extensions, par exemple pour passer une XEP du statut « Expérimental » à « Stable ». Elles identifient facilement les autres clients et serveurs prenant en charge une extension pour effectuer des tests d'interopérabilité. Enfin, en listant les fonctionnalités des logiciels, elles permettent aux utilisateurices de trouver le client adapté à leurs besoins.

Les clients modernes tels que Dino (Linux) ou Conversations (Android) ne se laissent pas distancer par les alternatives basées sur des protocoles propriétaires. Ils ont par exemple rajouté récemment les réactions par émojis, la synchronisation des confirmations de lecture entre différents appareils, ou encore les indicateurs de fuseau horaire afin d'éviter d'envoyer un message durant la nuit dans un autre pays. Une fonctionnalité unique parmi les solutions de messagerie instantanée auto-hébergées — devenue malheureusement pertinente à la suite d'une attaque soutenue par un État contre un

⁹https://en.wikipedia.org/wiki/Snowden_disclosures

¹⁰https://op-co.de/blog/posts/mobile_xmpp_in_2014/

¹¹<https://gultsch.de/posts/the-state-of-mobile-xmpp-in-2016/>

¹²<https://xmpp.org/extensions/>

¹³<https://notes.valdikss.org.ru/jabber.ru-mitm/>

fournisseur XMPP public¹³ — est le channel binding, un mécanisme visant à empêcher certaines attaques de type man in the middle.

Parmi les projets actuels, la communauté XMPP travaille sur les réponses aux messages, le partage de plusieurs images sous forme de galerie et la prise en charge d'OAuth. Ces fonctionnalités s'appuient déjà sur des XEP expérimentales, mais la communauté attend des retours d'expérience sur leur mise en œuvre avant de faire avancer le processus. Parallèlement, elle étudie les possibilités de mettre à jour la RFC et de soumettre à nouveau le protocole à l'IETF sous l'appellation « XMPP 2.0 ».

La messagerie instantanée n'est pas une expérience utilisateur homogène. Une application pour la collaboration professionnelle n'a pas les mêmes fonctionnalités qu'une pour usage familial ou entre amiEs. Tous les clients XMPP ne visent pas la même expérience, mais les normes permettent de créer des clients spécialisés pour certains besoins sans avoir à inventer un protocole de toutes pièces.

Un avenir ancré dans le passé

La communauté XMPP compte des développeurs plus jeunes que le protocole lui-même, ce qui est fascinant. Il a survécu dans son coin à des startups financées par du capital-risque, à des plateformes propriétaires et à des cycles technologiques entiers. Cette endurance nous fournit la résilience dont nous avons besoins dans ces temps incertains. Elle est l'ancrage, la colonne vertébrale, l'infrastructure.

Matrix a réinventé la roue en concevant un métro sur pneus. Sur le papier, il y a de réels avantages — comme pouvoir gravir des pentes plus raides — arguments utilisés dans une publicité agressive et un lobbying intense pour se vendre auprès des collectivités et gouvernements. Au bout du compte, toutefois, la collectivité se retrouve prisonnière d'un fournisseur unique.

L'évolution de la situation géopolitique et la prise de conscience de la domination excessive des géants de la tech nous poussent à rechercher et à développer des alternatives. Mais et si cette alternative se trouvait sous nos yeux depuis plus de 25 ans ? Il s'agit de la norme de référence en matière de messagerie instantanée : la RFC 6120, ou **Extensible Messaging and Presence Protocol** (XMPP).

À propos de messagerie instantanée standard et fédérée

Dans ce texte, Daniel Gultsch, mainteneur du client XMPP Conversations pour Android, célèbre les 25 ans de la norme RFC XMPP, nous rappelant pourquoi nous ne pouvons pas confier nos communications à un seul acteur.

Malgré ses limites, l'écosystème Jabber/XMPP est encore aujourd'hui animé par des communautés sans but lucratif et des projets à destination des petits hébergeurs indépendants des géants de la tech.

NO SLOP EDITIONS

