Alinto

Livre blanc

Novembre 2022

SOUVERAINETÉ NUMÉRIQUE : QUELS ENJEUX POUR LES E-MAILS PROFESSIONNELS ?

Sommaire

Introduction

La souveraineté numérique est plus que jamais au cœur des préoccupations des entreprises. **Elle pose les questions de la protection des données, de leur confidentialité et de l'indépendance des entreprises face aux fournisseurs américains (GAFAM notamment).**

Un enjeu non négligeable dans un contexte géopolitique tendu (guerre en Ukraine, crise de Taïwan...), et où les cyberattaques proviennent pour la majorité de pays autocratiques comme la Russie ou la Chine (selon le rapport de Carbon Black[1]). Les entreprises européennes ont plus que jamais besoin de protéger leurs datas et de miser sur la souveraineté.

Les technologies open source apportent des éléments de réponse. Grâce à l'ouverture du code, les entreprises disposent d'une vue sur le fonctionnement des applications et donc sur l'hébergement, le stockage et l'exploitation des données produites. De plus, plusieurs initiatives nationales et européennes voient le jour pour contrer les géants mondiaux du secteur : réglementations (RGPD), sensibilisation à la souveraineté, évangélisation autour des technologies open source…

Les messageries professionnelles sont également concernées. Leur exposition aux cyberattaques en font une priorité sur le plan de la sécurité, alors que leur fonctionnement, en termes d'acheminement et de stockage des données demeure complexe. C'est pourquoi, dans ce Livre Blanc, nous faisons le point sur la souveraineté numérique, les initatives européennes et le rôle de l'open source pour la sécurité des messageries professionnelles.

[1] https://www.developpez.com/actu/216086/La-Russie-et-la-Chine-sont-les-deux-principales-origines-des-cyberattaques-dans-le-monde-entier-d-apres-un-rapport-de-Carbon-Black/

Les enjeux de la souveraineté numérique

Les débats sur la souveraineté numérique sont au cœur des stratégies digitales des entreprises. La souveraineté n'est pas uniquement une lubie protectionniste destinée à combler le retard de l'Europe dans le domaine du numérique. Elle vise à **assurer la prospérité et l'indépendance des entreprises**, en protégeant leurs données, celles de leurs clients et de leurs concitoyens.

Concrètement, pour les entreprises, opter pour une solution numérique souveraine permet de répondre à trois enjeux majeurs. Explications.

La souveraineté pour garder le contrôle de ses données

La confidentialité des données s'est invitée à l'agenda de la majorité des entreprises. C'est encore plus le cas depuis l'entrée en vigueur du RGPD en 2018, qui a accéléré la prise de conscience en Europe. En effet, tous les pays, toutes les législations n'offrent pas la même protection des données. Il est donc primordial de **les cartographier, de s'assurer qu'elles sont protégées et inaccessibles aux personnes malveillantes.**

Pour protéger leurs données, plusieurs solutions s'offrent aux organisations :

- Les héberger sur un **cloud souverain**, localisé en Europe et géré par des sociétés de droit européen. Cela peut être certifié par différents labels (comme SecNumCloud, la certification la plus exigeante en matière d'hébergement en France)
- Opter pour des **logiciels open source** et/ou des logiciels européens
- Former les salariés aux différentes réglementations en matière de **protection de la data**
- **Sensibiliser les collaborateurs** quant à l'importance d'une bonne gestion de la donnée

La souveraineté de l'hébergement protège légalement les données de tout accès hostile. C'est le socle d'une bonne stratégie de contrôle pour les entreprises qui souhaitent tirer de la valeur de leurs données, tout en assurant leur confidentialité à leurs clients.

La souveraineté pour contrer le cloud act

Depuis 2018, le Cloud Act est en vigueur aux États-Unis. Il stipule que les autorités américaines peuvent demander aux fournisseurs de services de communication soumis à la juridiction américaine de leur fournir des données sous leur « possession, garde ou contrôle », et ce **indépendamment de la localisation des dites données**. C'est une véritable menace pour les données des entreprises européennes qui sont hébergées par des prestataires américains, y compris dans des datacenters basés en Europe. En effet, au titre du Cloud Act, ces prestataires peuvent exploiter les données, même confidentielles, au-delà des usages initialement prévus.

La souveraineté numérique européenne a pour but de mettre en place des **garanties contre ces accès illicites de la part de certains pays**, d'encadrer les demandes d'accès par des autorités étrangères et les transferts de données non personnelles.

Pour cela, deux règlements européens sont envisagés :

- **Le data governance act :** adopté en mai 2022, il sera applicable en septembre 2023. Il vise à favoriser le partage des données personnelles et non personnelles en mettant en place des structures d'intermédiation.

- **Le data act :** présenté en février 2022, il a pour objectif d'assurer une meilleure répartition de la valeur issue de l'utilisation des données personnelles et non personnelles entre les acteurs de l'économie de la donnée, notamment liées à l'utilisation des objets connectés et au développement de l'Internet des objets.

La souveraineté pour contrer l'expansion des GAFAM

Les GAFAM[1] menacent fortement la souveraineté numérique. Le poids économique de ces géants du numérique américaines est considérable : "la valorisation boursière cumulée des GAFAM a atteint « 5 853 milliards de dollars » en 2020, soit une valeur supérieur au PIB du Japon, 3ème économie au monde"[2].

Cette domination n'est pas uniquement économique, mais concerne aussi la dépendance numérique. En effet, ces entreprises sont capables de traiter et stocker les données de citoyens et d'entreprises du monde entier (datacenters, messageries, clouds…), qui leur sont "confiées" de manière plus ou moins conscientes lors de l'utilisation de services ou d'applications. Rappelons au passage que les GAFAM relèvent de la législation américaine. Ils sont soumis au Cloud Act, ce qui signifie que les données en leur possession sont susceptibles d'être transmises à des tiers.

Le reste du monde, et notamment l'Europe, se doit donc de contrer cette puissance en créant un véritable écosystème souverain. Comment ? En faisant évoluer les réglementations à ce sujet, en favorisant l'utilisation de logiciels open source et en communiquant sur les enjeux de la souveraineté numérique.

[1] Google, Amazon, Facebook, Apple, Microsoft

[2] https://fr.countryeconomy.com/gouvernement/pib

Souveraineté numérique : les initiatives européennes

Pour tendre vers une souveraineté numérique européenne, réglementer l'usage, le stockage et la collecte des données s'avère indispensable. Cette nécessaire protection des données continue de susciter un débat complexe entre pays membres. Ce qui n'a pas empêché l'Union Européenne de prendre plusieurs initiatives à ce sujet. Décryptage.

Le Règlement général la protection des données (RGPD) : le point de départ

Entré en vigueur en mai 2018, le RGPD est le premier pas vers la souveraineté numérique. Il réglemente l'accès, le stockage et l'utilisation des données personnelles des citoyens européens. Pour cela, les entreprises qui détiennent de telles données doivent répondre à plusieurs exigences (suppression des données, consultation sur demande, nomination de DPO…). Ce même règlement stipule que les données personnelles de l'UE ne peuvent être transférées que vers des pays qui offrent une protection similaire et que l'UE considère comme pays "adéquats"[1].

Or, la législation américaine, par exemple, est bien moins stricte que le RGPD. Le Cloud Act donne la possibilité au gouvernement américain d'accéder aux données détenues par des sociétés américaines. Et culturellement, les Américains considèrent la donnée comme un actif dont on peut faire commerce. **Malgré ces différences, de nombreuses entreprises européennes confient leurs data aux grands fournisseurs de services numériques américains, notamment pour leur hébergement.** Cela a poussé l'UE à prendre d'autres initiatives pour réguler le marché des données.

[1] Voir https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Le Data Governance Act et le Data Act : pour aller plus loin

Ces deux textes complètent le RGPD. Ils visent à développer un marché unique de la donnée en soutenant l'accès, le partage et la réutilisation des données, dans le respect des valeurs de l'UE.

Le Data Governance Act entrera en vigueur en septembre 2023. Il a pour objectif de favoriser le partage des données personnelles et non personnelles en mettant en place des structures d'intermédiation. Ces dernières définiront clairement les conditions dans lesquelles les données détenues par le service public pourront être réutilisées, et ainsi lutter à armes égales avec les acteurs du marché international.

Le Data Act, quant à lui, vise à établir des règles harmonisées quant à l'accès aux données générées par les objets connectés et les différents services liés. Il s'agit de faciliter l'accès, la gestion et le partage de ces données.

La Directive NIS2 : souveraineté et cybersécurité

La directive européenne Network Internet Security, dite NIS 2, a pour objectif de renforcer le niveau de préparation des entreprises et organisations aux risques cyber. Elle va se traduire par de nouvelles obligations : mesures de sécurité, règles de supervision, obligation de notifier toute attaque à l'ANSSI…

Chaque pays pourra dresser la liste des organisations concernées par cette directive, en fonction d'une analyse de risque. On estime que plusieurs milliers d'entités liées aux services numériques, à l'industrie spatiale ou la recherche vont ainsi être soumises à cette directive, qui est en cours d'adoption.

Les autorités locales : la CNIL et l'ANSSI pour veiller au respect des législations en France

En France, deux organismes se chargent de veiller à l'application des réglementations sur la protection des données et d'aider entreprises et citoyens à faire face à la menace cyber.

La Commission nationale de l'informatique et des libertés (CNIL), parfois appelée le gendarme du numérique, est le régulateur des données personnelles. Elle a plusieurs missions :

- **Informer et protéger les droits :** elle répond aux demandes d'information des professionnels et particuliers en matière de protection des données. Elle traite également leurs plaintes.
- **Accompagner la conformité :** elle propose une boîte à outils pour aider les entreprises à se mettre en conformité.
- **Anticiper et innover :** elle participe aux développements de solutions protectrices de la vie privée, conseille les entreprises et participe à la constitution d'un débat sur les enjeux éthiques de la donnée.
- **Contrôler et sanctionner :** elle contrôle la mise en application concrète de la loi.

L'ANSSI (Agence nationale de la sécurité des systèmes d'information), de son côté, apporte son expertise et son assistance technique aux organisations concernant la cybersécurité. Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

L'action des gouvernements européens : de véritables prescripteurs

Pour tendre vers la souveraineté numérique, les gouvernements jouent un rôle important. Ils sont prescripteurs dans le choix de solutions technologiques. Leurs décisions aident à mettre en avant le savoir-faire des acteurs numériques européens. Depuis quelques années, **les gouvernements poussent ainsi les collectivités et les entreprises à se tourner vers des solutions open source ou des logiciels produits par des éditeurs locaux.**

Le développement de l'écosystème numérique européen permet ainsi de proposer une véritable alternative face aux GAFAM, et de garder le contrôle sur les données.

La prise de conscience des enjeux liés à la souveraineté numérique est bien réelle en Europe. Des règlements comme le RGPD ont éveillé l'attention des citoyens. Les médias se font l'écho de scandales liés à des fuites de données ou à la manne que représentent les données de santé. Des initiatives ont bien été prises à l'échelle européenne, mais elles ne sont pas encore suffisantes pour contrer la puissance des géants américains. Mais, **ces règlements montrent la voie pour tendre vers des solutions plus respectueuses des données de nos concitoyens.**

Souveraineté et cybersécurité : intimement liés ?

À l'heure où les cyberattaques sont toujours plus nombreuses et sophistiquées, la cybersécurité est un prérequis à la souveraineté numérique. Les systèmes d'information gagnent en complexité, avec des interconnexions public/privé aux frontières souvent poreuses. Dans le même temps, les volumes d'échange par email augmentent jour après jour, offrant autant de portes d'entrée pour les cybermenaces.

En matière de protections de données, **la cybersécurité et la souveraineté sont indissociables**. Voici pourquoi.

La souveraineté numérique, première marche pour la protection des données

Comme évoqué dans l'article "Souveraineté numérique : les initiatives européennes", la souveraineté vise à mieux protéger les données des organisations et des concitoyens européens. En effet, en utilisant les services d'un partenaire qui se dit souverain, on s'attend à ce qu'il n'utilise les données que pour les usages spécifiés, et qu'il ne les divulgue pas. Cette garantie est évidemment assurée par les processus de contrôle, de stockage et de traitement mis en place, le respect des réglementations… mais aussi par les solutions technologiques utilisées (hébergement souverain, logiciels open source…).

Les menaces de cyberattaques ou de divulgation des données sont donc moins importantes en faisant appel à un prestataire européen.

La cybersécurité : protection contre les menaces externes

Par définition, la cybersécurité est un ensemble de mesures visant à assurer la sécurité des systèmes et données informatiques contre des actes malveillants. Une cyberattaque peut affecter gravement les entreprises. Elles doivent donc être capables de faire face à un tel événement, et mettre en place des mesures de sécurisation du SI.

Cela passe, entre autres, par le déploiement de logiciels de protection (antivirus par exemple), par des plans de mise à jour des systèmes (patches), de systèmes d'authentification, mais aussi la formation des collaborateurs aux bonnes pratiques de cybersécurité.

Souvent, les entreprises n'ont pas conscience de disposer de données sensibles, ou pensent qu'une attaque n'arrive qu'aux autres. Malheureusement, le nombre d'incidents ne cesse d'augmenter, et les techniques des cyberattaquants sont de plus en plus sophistiquées. **Les conséquences peuvent être dramatiques**.

Par exemple, victime d' une attaque de type ransomware, le centre hospitalier sud-francilien de Corbeil-Essonnes a vu certaines données sensibles (DPI, données personnelles…) divulguées sur Internet[1] suite à son refus de payer une rançon.

[1] https://www.liberation.fr/societe/sante/faute-de-rancon-les-donnees-volees-dans-un-hopital-de-lessonne-se-retrouvent-mises-en-ligne-20220925_PMF2MYWN5NAW3BLNDXF7Q34BZY/

Pas de souveraineté, sans cybersécurité

Cela devient une évidence : **la souveraineté numérique seule ne suffit pas à protéger les données sans inclure le volet cybersécurité.**

La souveraineté numérique permet certes de mieux maîtriser ses données. Cependant, un environnement logiciel ou des applicatifs trop ouverts ou exposés vont faire persister certaines failles. La souveraineté ne peut donc pas être dissociée de la cybersécurité. Cette dernière impose d'insuffler les bonnes pratiques au sein des entreprises, ou encore, de construire une offre cyber européenne qui soit une véritable alternative aux solutions des mastodontes américains.

En attendant qu'un tel dispositif soit déployé, les entreprises ne doivent pas négliger l'usage de solutions de cybersécurité et doivent s'équiper d'antivirus, mettre en place des stratégies de back up, s'entourer d'experts capables de les accompagner, suivre les conseils des organismes de références comme l'ANSSI en France et se tourner le plus possible vers des solutions d'experts métiers de proximité travaillant sur des solutions open source.

Les messageries professionnelles présentent des dangers !

L'évolution du travail à distance, l'adoption de solutions cloud, l'hybridation des systèmes d'information… sont autant de facteurs qui augmentent la vulnérabilité des entreprises face aux cybermenaces. **Si les attaquants visaient les infrastructures il y a quelques années, aujourd'hui, ils ciblent l'humain et misent sur le manque de vigilance des utilisateurs**. Et quel meilleur moyen que l'email pour perpétrer leurs attaques ?

Les messageries professionnelles présentent donc des dangers pour la protection des données des entreprises. Bien heureusement, des solutions souveraines existent et elles permettent une meilleure sécurité. Explications.

Messageries professionnelles : première source des cyberattaques

Avec près de 300 milliards d'emails envoyés chaque jour en 2020 dans le monde, la messagerie est une porte d'entrée privilégiée pour les cyberattaques. Ce canal de communication permet de partager des données et des informations plus ou moins sensibles pour les entreprises. Ces échanges sont des terrains fertiles pour les cybercriminels. Les chiffres en sont témoins :

83 % **des interrogés ont déclaré que leur entreprise avait subi au moins une attaque concluante de phishing par email en 2021.[1]**

Partages de liens frauduleux, envoi de pièces jointes malveillantes, demande de coordonnées bancaires… sont autant de techniques pour piéger les destinataires d'un email. Sans sensibilisation accrue des collaborateurs, ni outils adaptés, les entreprises s'exposent à des risques de violation des données, dont les conséquences peuvent être désastreuses.

[1] Rapport « State of the Phish » 2022

Messageries et souveraineté : mission impossible ?

Comment éviter les cyberattaques ? La réponse n'est pas si simple. Les attaquants sont de plus en plus rusés, **le risque zéro n'existe pas**. Par contre, il est possible de le réduire et de mieux protéger ses données en portant un soin particulier au choix d'un fournisseur de messagerie professionnelle.

Les solutions gérées par les GAFAM ne sont pas souveraines par nature. En effet, elles collectent les données et les stockent dans des datacenters non soumis aux règles de souveraineté européennes. Il n'est donc pas possible de garantir leur confidentialité et d'en garder le contrôle en tant qu'entreprise. De plus, leurs systèmes de messagerie sont des logiciels au code fermé, renforçant la dépendance à un fournisseur, sans transparence sur les traitements, à l'opposé des principes de souveraineté numérique.

Pourtant, des solutions existent et offrent de véritables alternatives : les messageries open source.

Qu’est-ce qu’une bonne messagerie professionnelle ?

Entre exigences de souveraineté et de cybersécurité, quel est le portrait robot de la messagerie professionnelle idéale ?

La messagerie professionnelle idéale est souveraine

Cela coule de source, c’est une messagerie qui est développée par un éditeur européen, ou open source. Ce dernier critère offre plus de transparence quant au fonctionnement et la réactivité d’une communauté pour corriger d’éventuelles failles . Attention cependant ! Rien ne sert de s’entourer d’un partenaire local si son hébergeur ne coche pas toutes les cases de la souveraineté.

La messagerie idéale est donc composée d’un logiciel édité en Europe, opéré par un prestataire de droit européen qui l’héberge sur des infrastructures en Europe, sécurisées selon les recommandations européennes.

La messagerie professionnelle idéale est sécurisée

Une bonne messagerie professionnelle comprend un arsenal de sécurité complet. Les solutions de sécurité intégrées dans les versions standard des messageries professionnelles (antispam, relais smtp…) sont souvent insuffisantes. Beaucoup d’entreprises ne s’équipent pas de solutions additionnelles. **Jusqu’au jour où elles sont victimes**.

Une bonne messagerie professionnelle doit donc embarquer les meilleures technologies pour assurer le filtrage des emails, mais aussi la bonne délivrance des emails, tout en protégeant la réputation du domaine de messagerie. Ce que peu de systèmes de messagerie proposent par défaut.

Afin de se protéger des cyberattaques par email, la messagerie idéale doit respecter plusieurs critères. D’abord, choisir un hébergeur souverain, puis un fournisseur de messagerie européen. Pour aller plus loin, les entreprises peuvent opter pour l’open source, assurant ainsi la transparence du code. Enfin, il ne faut pas négliger les solutions de sécurité additionnelles pour une protection totale de la messagerie.

L'open source au secours des services de messagerie professionnelle

La messagerie est une application ancrée dans le quotidien en entreprise. Son usage va au-delà des simples échanges d'email. C'est un véritable outil collaboratif et un moyen de communication universel qui permet de gagner du temps et de dématérialiser de nombreux échanges.

Il est donc indispensable de s'équiper d'un outil de messagerie intuitif, ergonomique, fiable et sécurisé. Sur le terrain, les GAFAM dominent le marché avec des messageries intégrées à leurs suites bureautiques comme Office 365 ou Google workspace. Cependant, des alternatives existent. Parmi celles-ci, on retrouve les messageries open source.

Les avantages des messageries open source

Le gros avantage des messageries open source, c'est le libre accès au code. Leur utilisation n'est pas conditionnée à l'achat d'une licence, et **les entreprises ne sont pas dépendantes d'un fournisseur**. Leur intégration dans le système d'information peut être effectuée en interne, ou par un intégrateur, sans engagement avec ce dernier. L'ouverture du code permet également de l'adapter à des besoins bien spécifiques, à moindre coût.

Faire le choix de l'open source, c'est bénéficier d'une communauté d'utilisateurs, qui enrichissent et améliorent la solution en permanence. Que ce soit l'ergonomie, les fonctionnalités, ou la sécurité, les contributeurs regorgent d'idées et apportent leurs compétences pour faire évoluer la solution et l'adapter aux besoins des organisations.

Du côté de la DSI, c'est surtout la pérennité technique qui pèse dans la balance. Pour des informaticiens spécialisés, **les messageries open source sont souvent plus appréciées à mettre en œuvre que celles des géants de la Tech car elles font appel à leur savoir faire métier.**

La messagerie open source et la souveraineté

La sécurité des messageries professionnelles s'aborde à différents niveaux. Du point de vue des données, il convient de se demander : où est-elle stockée ? Comment y accède-t-on ? Les solutions open source n'imposent aucune règle aux entreprises. Ces dernières peuvent donc choisir leur prestataire d'hébergement des données et **s'assurer de leur bon traitement**.

Pour bénéficier d'une continuité de service, les entreprises peuvent souscrire un "plan de reprise d'activité" en cas d'incident, selon des modalités définies avec leur hébergeur.
Opter pour une messagerie européenne et open source, combinée à un hébergement souverain, apporte un socle de sécurité indispensable. Les données de l'entreprise échappent notamment au Cloud Act, la législation américaine qui s'applique de fait aux solutions de messagerie des GAFAM.

Enfin, **même si le risque zéro n'existe pas en termes de cybersécurité, la priorité des hackers sera toujours de cibler les gros éditeurs**, qui concentrent de grosses parts de marché. Ce risque pourra être réduit avec un arsenal de sécurisation de messagerie complet.

Il est également indispensable de s'assurer que la messagerie soit capable de s'interfacer avec l'architecture IT de l'entreprise et de communiquer avec les autres outils. **L'open source est là encore une alternative intéressante**.

L'exemple du webmail SOGo

SOGo est un webmail open source qui permet de partager calendrier, carnets d'adresses et email au sein d'une entreprise. La solution est totalement ouverte et gratuite, si les organisations choisissent de la déployer par elles-mêmes en interne.

Basée sur AJAX, SOGo est un webmail universel et responsive. Il est le composant front end de l'infrastructure de messagerie qui offre aux utilisateurs une interface complète d'accès aux informations. Il bénéficie d'une communauté de plusieurs milliers de contributeurs qui enrichissent la solution en continu.

Pour les entreprises qui souhaitent bénéficier d'une intégration et d'un accompagnement complets, Alinto propose depuis 2022 une version professionnelle cloud de SOGo, avec un support dédié et une surveillance 24/7. **La solution, totalement sécurisée, s'appuie sur un hébergement souverain.**

Dans le chemin qui mène à la souveraineté numérique, la messagerie a aussi son rôle à jouer. L'open source, combiné à des offres d'hébergement cloud européennes, est un levier pour l'atteindre. Les organisations se tournent de plus en plus vers ces technologies. Même si cette transformation prend du temps à cause de l'inertie due aux cycles de vie des solutions et des renouvellements de marchés, la tendance est bien réelle.

Conclusion

La souveraineté numérique devient de plus en plus une priorité pour les organisations. Leurs motivations sont nombreuses : garder le contrôle des données, encourager l'utilisation de logiciels européens, garder son indépendance face aux grands fournisseurs américains et mondiaux.

Parmi les solutions, les gouvernements européens encouragent les initiatives open source, et les entreprises sont moins réticentes à leur utilisation. Elles ont donc tout intérêt à saisir cette opportunité pour garder le contrôle de leurs données. Et cela commence dès la messagerie professionnelle et sa sécurisation.

À propos

Fondée en 2000, Alinto est une entreprise spécialisée dans les métiers de l'Email : service de messagerie et de sécurité en mode SaaS ou PaaS,... à travers plusieurs produits et principalement :

- **SOGomail** : serveur mail sécurisé, collaboratif tout en un, intégrant le webmail SOGo entièrement responsive.

- **Cleanmail** : le relais de messagerie sécurisé qui protège des cybermenaces en assurant un accès permanent aux emails.

- **Serenamail** : le relais de messagerie SMTP permet à des serveurs ou des applications d'envoyer des emails pour offrir un trafic dit « propre ».

Spécialiste européen de la messagerie sécurisée, Alinto cherche à répondre aux nouvelles attentes du marché en choisissant de se tourner plus activement vers l'open source. Pour cela, l'éditeur reprend en 2022 les rennes du webmail SOGo et de sa communauté et celles de la de filtrage des E-mail.

Mais pourquoi se tourner vers l'open source ? Il s'agit avant tout d'un enjeu de souveraineté numérique. Avec l'open source, le code est à disposition des utilisateurs et les entreprises peuvent ainsi garder le contrôle sur l'hébergement, le stockage, l'exploitation et surtout la réversibilité des données. Pour les équipes d'Alinto, l'open source offre le choix à leurs clients et partenaires de la souveraineté numérique. C'est aussi la volonté de leur proposer une alternative sérieuse et pérenne aux GAFAM.

« À notre sens, l'open source est essentiel pour laisser aux utilisateurs la liberté de choix. C'est un élément important pour la diversité et c'est pour nous un moyen d'offrir aux entreprises des alternatives aux outils de messagerie des acteurs du cloud américains », précise **Philippe Gilbert, CEO d'Alinto**.

Lyon (siège)
15 quai Tilsitt
FR-69002 Lyon
+33 481 09 01 10

Barcelone
Paseo de Gracia,101-4°1
SP-08008 Barcelona
+34 91 005 29 64

Zurich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Lausanne
Rue des Jordils 40
1025 St-Sulpice
Switzerland
Tel: +41 21 695 20 20

Alinto

www.alinto.com