

# Souveraineté numérique : les retours de Talkspirit, Yousign et Reverso

La France et l'Europe ambitionnent de disposer d'alternatives solides aux offres cloud des GAFAM et BATX\*. Silicon.fr s'est entretenu avec trois entrepreneurs, Philippe Pinault, co-fondateur et président-directeur général du réseau social d'entreprise [Talkspirit](#), Théo Hoffenberg, fondateur et dirigeant de [Reverso](#), fournisseur de technologies linguistiques à base d'IA, et Antoine Louiset, co-fondateur et CTO du fournisseur de logiciel de signature électronique [Yousign](#), pour aborder la thématique de la souveraineté numérique.

**Silicon.fr – Un ministère régalien peut promouvoir la souveraineté numérique et, dans le même temps, imposer une « boucle WhatsApp » pour interagir avec ses services lors d'une présentation en ligne. Y a-t-il discordance ?**

Philippe Pinault : Bien sûr. Imposer un outil soumis au [Cloud Act](#) et dans le même temps prôner plus de souveraineté numérique crée de la confusion. L'Etat se doit d'être exemplaire et joindre les paroles aux actes pour plus de cohérence.

Théo Hoffenberg : En partie. Il ne faut pas imposer du « tout » français, quand il n'y a pas de bonne solution, même s'il est problématique de communiquer officiellement sur certains outils. En outre, il n'y a pas vraiment de concurrence française à WhatsApp ou Facebook. En revanche, dans les serveurs/l'hébergement web, on a [OVHcloud](#) ou d'autres, et dans la vidéoconférence, on a des solutions comme Livestorm, et pas uniquement [Zoom](#) ou Teams...

Antoine Louiset : Il n'y a pas forcément discordance. Ici, nous sommes dans le cas d'une conférence publique. Il eût certes été préférable de faire appel à une solution européenne pour des raisons au moins politiques, mais l'usage de cet outil ne présente pas de risque en matière de sécurité ou de souveraineté au sens où nous l'entendons. Cependant, il ne faut pas perdre de vue que la cohérence est un élément clé pour crédibiliser ce genre d'initiative, il s'agirait donc de montrer l'exemple en cherchant systématiquement une alternative française ou européenne aux solutions utilisées.

**La labellisation de services cloud « de confiance » va-t-elle dans le bon sens ?**

T.H. : Pas sûr, car Microsoft, Google et Amazon se positionnent sur ces créneaux.

P.P : Oui, selon moi, la mesure est positive. C'est la reconnaissance, enfin, de l'importance et du caractère stratégique du Cloud dans les choix d'infrastructures pour bâtir le « [futur du travail](#) ». La prise en compte du Cloud first et la certification d'[opérateurs cloud](#) comme partenaires « de confiance » vont donc dans le bon sens pour emmener l'ensemble du marché vers l'adoption du cloud, avec un niveau de sécurité optimal.

A.L. : Nous sommes en effet sur une bonne voie. Le stockage et la gestion des données sont au cœur de tous les processus des entreprises aujourd'hui. Qu'elles éditent les logiciels ou les utilisent. Créer des solutions européennes n'a pas d'intérêt si elles n'ont pas d'autre choix que de dépendre, à un moment ou à un autre, d'un acteur étranger. En valorisant les acteurs français du Cloud et leur

développement, cette initiative ouvre la voie à une souveraineté numérique complète des produits français. Il serait cependant intéressant de penser cela au niveau européen, sur le modèle d'[eIDAS](#) et des services de confiance qualifiés, pour se donner davantage de moyens de développer des géants du numérique capables de rivaliser face aux acteurs chinois et américains.

**Sous l'angle des solutions et services de sécurité, c'est le « zero trust » qui l'emporte. Qui supporte le risque, l'utilisateur ou le fournisseur ?**

A.L. : Les deux supportent des risques. Le fournisseur tente de protéger l'utilisateur. Celui-ci doit être conscient des actions qu'il entreprend pour pouvoir détecter des anomalies. Or, il reste encore beaucoup de pédagogie à faire sur la sécurité côté utilisateurs.

P.P : Les [deux parties](#) sont impliquées dans la mise en œuvre d'une politique de sécurité [zero trust](#). Le fournisseur dans le design de sa solution et les choix de paramétrage qu'il rend possible. Les utilisateurs dans leur usage des solutions et dans l'adoption de pratiques cohérentes avec la politique de sécurité de l'entreprise. Quels que soient les outils, le risque le plus élevé aujourd'hui apparaît surtout du côté des utilisateurs.

T.H. : Les grands groupes ont aussi intérêt à participer, car souvent les contraintes de sécurité coûtent très cher en regard des solutions achetées.

\* GAFAM : Google, Amazon, Facebook, Apple, Microsoft | BATX : Baidu, Alibaba, Tencent, Xiaomi.

(crédit photo de une © beugdesign - Adobe Stock)