

Un cadre légal unique pour la protection des données

Pierre Van Wambeke, CEO de SeeZam

Propos recueillis par Sébastien Lambotte



Crédit: Luc Deflorenne

51

Le Luxembourg nourrit l'ambition de devenir un centre d'excellence en matière de gestion des données sensibles. SeeZam, dans ce contexte, a développé une solution de coffre-fort virtuel®, profitant notamment d'une législation unique pour offrir à ses clients un niveau de confidentialité inégalé.

DANS L'ÈRE DIGITALE QUE NOUS TRAVERSONS, ALORS QUE LES MÉDIAS FONT RÉGULIÈREMENT ÉTAT DE FAILLES DE SÉCURITÉ INFORMATIQUE, COMMENT PEUT-ON AUJOURD'HUI GARANTIR QUE DES YEUX INDISCRETS RESTENT PARFAITEMENT ÉCARTÉS DE VOS DONNÉES LES PLUS SENSIBLES ?

Les questions relatives à la sécurisation des données sont à la fois complexes et importantes. Il est essentiel, et ce pour un

nombre considérable d'acteurs, de pouvoir disposer de garanties relatives à la préservation de données sensibles. Face aux enjeux actuels, il faut en effet pouvoir proposer des solutions innovantes de protection de l'information. Le Luxembourg est bien positionné pour permettre à des acteurs de développer des solutions répondant à ces besoins. C'est pour cette raison que nous avons choisi cet État pour développer, depuis six ans, notre solution de coffre-fort numérique.

EN QUOI LE LUXEMBOURG SE DIFFÉRENCIE-T-IL DES AUTRES ?

Grâce à un contexte législatif unique. Il nous offre l'opportunité de proposer un véritable coffre-fort numérique, dans lequel le client peut déposer des informations et des documents dont il est le

seul à connaître la nature, à pouvoir en gérer les accès, indépendamment des prestataires qui font tourner la solution. Comme un banquier ne sait pas forcément ce qu'un client entrepose dans son coffre-fort physique, en tant que fournisseur de cette solution, je suis personnellement dans l'incapacité de dire ce que mes clients entreposent à l'intérieur de l'espace numérique sécurisé que nous mettons à leur disposition.

POUVEZ-VOUS NOUS EN DIRE PLUS SUR CE CONTEXTE LÉGISLATIF UNIQUE ?

Oui. Le Luxembourg permet un cryptage libre. On peut donc crypter l'information à un très haut niveau, sans contrainte. Ensuite, il n'y a pas d'obligation d'avoir une porte dérobée vers les coffres, de disposer de passe-partout ou de soumettre

les clés de cryptage à une quelconque autorité. Très médiatisées, les limitations imposées par le Patriot Act américain (facilitant la surveillance mondiale de la NSA) sont un exemple. Dans d'autres Etats européens, la France par exemple, pour des cryptages au-delà de 128 bits, il est obligatoire de soumettre les clefs de cryptage à la Défense. Cette contrainte n'existe pas au Luxembourg. Le fait de pouvoir crypter sans limite et de ne pas exiger du prestataire d'avoir accès aux clefs du client permet d'établir des niveaux de sécurité considérés inviolables en l'état de la technologie actuelle.

COMMENT VOTRE CLIENT PEUT-IL S'ASSURER QUE VOUS-MÊME N'AUREZ PAS ACCÈS À CE QU'IL ENTREPOSE DANS LE COFFRE ?

La confiance est effectivement ce qu'il y a de plus difficile à créer à l'égard des clients. C'est vrai à l'échelle de notre activité comme ça l'est pour l'ensemble de la Place, dans la mesure où l'ambition de cette dernière est de se positionner comme un hub de confiance en matière de gestion de la donnée sensible. La législation contribue à l'établissement de cette confiance. Au-delà, la technologie et le modèle mis en œuvre constituent d'autres leviers permettant de la renforcer. Avec SeeZam, nous fournissons à nos clients un espace de stockage et les outils pour générer eux-mêmes, sans être un « rocket scientist », les clés de cryptage permettant de sécuriser leurs fichiers et d'y accéder. A aucun moment, SeeZam n'a les moyens d'accéder au contenu des coffres dans la mesure où nous ne disposons tout simplement pas des clés de décryptage que seul le client peut libérer.

IL DOIT CEPENDANT FAIRE CONFIANCE À CE DISCOURS. DANS UN ENVIRONNEMENT « DIGITAL » OÙ DES FAILLES SONT DÉCOUVERTES CHAQUE JOUR, COMMENT PEUT-IL EN ÊTRE SÛR ?

Au-delà de la solution technologique, c'est aussi un engagement contractuel établi avec l'ensemble des clients. J'aime à rappeler un autre aspect de la législation luxembourgeoise : le vol de données

personnelles est particulièrement sanctionné. Une condamnation au pénal à une peine allant jusqu'à 10 ans de prison dissuadera les escrocs et vient donc aussi rassurer le client.

PERMETTRE DE CACHER DES DONNÉES À L'ÉGARD DES AUTORITÉS NE CONSTITUE-T-IL PAS UN NOUVEAU RISQUE POUR LE LUXEMBOURG DE SE VOIR À NOUVEAU POINTER DU DOIGT EN FAVORISANT UNE CERTAINE OPACITÉ ?

Le Luxembourg a la volonté d'offrir des garanties réelles en matière de confidentialité et de secret. Je pense que, à l'heure où on évoque des opérations d'espionnage à grande échelle, menées par les Etats eux-mêmes, c'est un excellent positionnement. Le législateur, avant toute chose, doit être le garant des libertés et des droits de chacun. Or, la Charte des Droits de l'Homme consacre le droit au secret des échanges et des communications. Au regard de l'actualité, on devrait au contraire regretter que ce droit soit bafoué au quotidien, piétinant le fondement d'une démocratie édiflée sur le vote secret, faut-il le rappeler.

A QUELS BESOINS RÉPOND AUJOURD'HUI UNE SOLUTION DE COFFRE-FORT VIRTUEL COMME CELLE QUE VOUS PROPOSEZ ?

Nous avons identifié plusieurs fonctions principales. La première réside dans la protection des informations. Chaque entreprise a des informations à protéger, on parle de capital numérique. Elles peuvent concerner des décisions du conseil d'administration, relatives à des fusions ou acquisitions par exemple. La deuxième fonction est celle du partage de l'information. Le coffre-fort permet de centraliser l'information et de n'en accorder l'accès qu'à des personnes autorisées. Cette fonction est aussi intéressante dans le cadre d'un conseil d'administration, pour porter à la connaissance des administrateurs et des parties prenantes les informations sensibles sans avoir à les faire circuler sur des réseaux non sécurisés. Enfin, le coffre-fort électronique offre aussi des fonctionnalités de dépôt.

Il peut fonctionner comme une boîte aux lettres blindée. Vous pouvez autoriser des acteurs tiers à y déposer des documents que vous seul pourrez décrypter. Cette fonction est utile, par exemple, au niveau des secrétariats sociaux, pour la distribution des fiches de salaire, documents qui revêtent aussi un caractère confidentiel. Cela peut encore être utile pour des assureurs ou des banques. L'avantage est que ce mode de distribution est irrémédiablement moins onéreux que le traitement papier.

QUÉ RÉPONDEZ-VOUS À CEUX QUI VOUS PROCHERAIENT QUE VOTRE SOLUTION PERMET DE CACHER DES DOCUMENTS RELATIFS À DES OPÉRATIONS MALVEILLANTES ?

Dans la mesure où je ne peux accéder aux contenus entreposés dans les coffres, je ne peux pas préciser si oui ou non des documents de telle nature existent. Au moment où il veut accéder au service, cependant, l'utilisateur est invité à adhérer à une charte, précisant que la solution ne peut pas être utilisée à des fins qui contreviendraient à la loi. Je répondrai aussi que le secret n'est pas quelque chose de sale et de tabou et que de nombreuses professions sont heureusement liées à un secret (PSF, avocats, médecins,...). Enfin, nous n'avons pas le monopole du cryptage. Nous mettons simplement à disposition une interface intuitive offrant des technologies de pointe sans requérir l'expertise.

QUE SE PASSE-T-IL LE JOUR OÙ LA POLICE SOUHAITE ACCÉDER AU COFFRE DE L'UN DE VOS CLIENTS ?

Comme précisé, je ne dispose ni de clefs ni de pied de biche qui me permettent d'entrer dans les coffres. Avec une injonction de justice luxembourgeoise, mon obligation de moyens (pas de résultat) me permettra tout au plus de bloquer l'accès au compte ou de fournir le contenu crypté. Mais je ne dispose pas des moyens de le décrypter. Accéder aux clés de cryptage, qui permettent la lecture du contenu, nécessite de disposer des données permettant l'authentification du client et qui lui sont personnelles.