Olfeo

LIVRE BLANC

Souveraineté :
Pourquoi choisir des solutions souveraines de sécurité en SaaS ?

Souveraineté

SOMMAIRE

Les solutions de sécurité en SaaS :
la nécessité d'une vigilance accrue

Les éditeurs SaaS accèdent à l'ensemble des données sensibles

Historiquement, les données confidentielles ou sensibles des entreprises étaient stockées sur des serveurs hébergés physiquement dans leurs locaux (sur des logiciels On-premise). Dans certains cas, ces données étaient déplacées vers des Datacenters propres sécurisés aussi bien pour l'accès que le stockage.

Désormais, les logiciels On-premise laissent la place aux solutions SaaS, hébergées sur des serveurs mutualisés dans le Cloud. Les données se déplacent massivement des serveurs internes vers des applications SaaS métiers externes. Le SaaS devient alors un prolongement du Système d'Information des entreprises sans qu'elles soient parfaitement conscientes des conséquences.

Les données ainsi déversées vers le Cloud sont extrêmement diverses et souvent sensibles :

- Commerciales : fichiers clients et prospects, contrats, propositions, politiques tarifaires…
- R&D : secrets industriels, projets de recherche, innovation…
- RH : informations sur les collaborateurs (rémunération, santé, évaluation…)
- Financières : comptes, situation de trésorerie, opération M&A en cours…

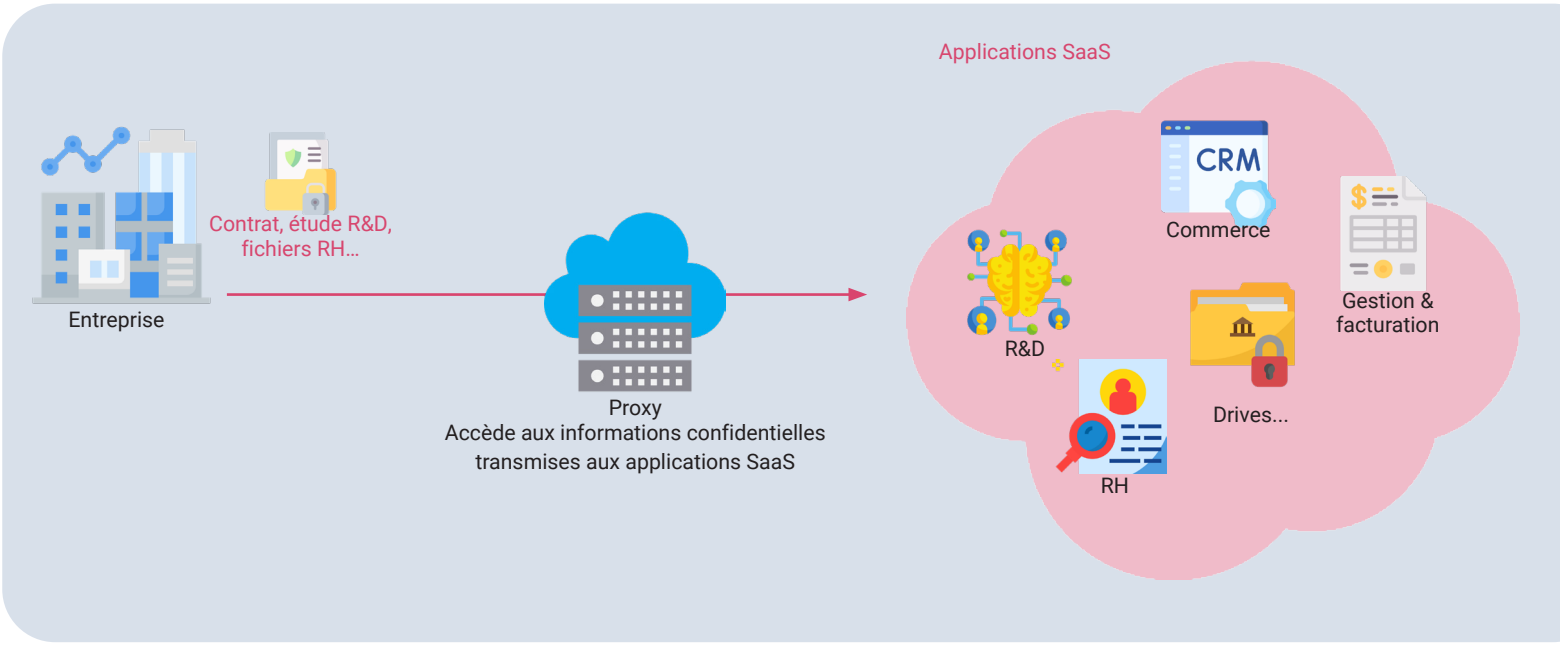
Lorsque les données étaient stockées sur les serveurs internes, leur sécurisation faisait l'objet d'une analyse de risques et de méthodes de protection avancées. Paradoxalement, cette nécessité de contrôle semble complètement disparaître lorsque les données quittent l'entreprise.

Séduites par les facilités qu'offrent les applications SaaS, les responsables de services métier des entreprises (marketing, commerce, finance, rh…) souscrivent directement des abonnements auprès d'éditeurs SaaS sans l'aval de la DSI (shadow IT). Les RSSI, DSI et DPO des entreprises européennes prennent tout juste conscience de ces risques et s'équipent, depuis peu, de solutions pour exercer un meilleur contrôle de leur parc applicatif (CASB).

Les applications SaaS de sécurité : un cas encore plus sensible

Les logiciels de sécurité accèdent à l'ensemble des données d'entreprises y compris les plus secrètes.

Les solutions de sécurité, notamment les firewalls et les proxys, déchiffrent les flux web afin d'analyser les contenus et bloquer ceux considérés comme suspects (malwares, contenus illégaux, dangereux ...). Elles interceptent l'ensemble des connexions entre le SI interne, les utilisateurs et les applications SaaS externes et ont donc accès à tous les fichiers échangés.



Pour préserver ses données, il est donc nécessaire :

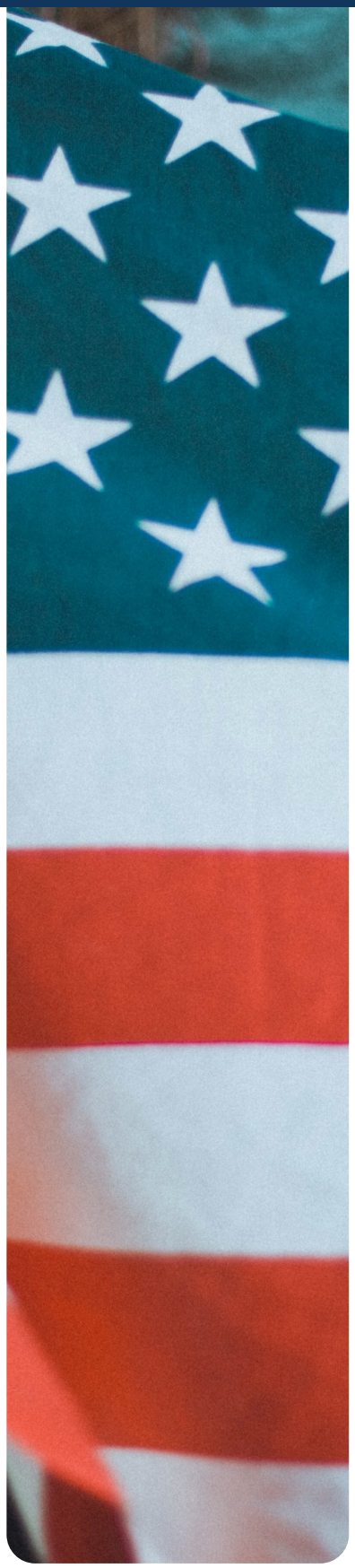
- d'utiliser des applications SaaS provenant de partenaires de confiance,
- de sélectionner un partenaire proxy lui-même de confiance car il accède à tous les contenus échangés avec toutes les applications SaaS, l'enjeu est donc encore bien plus fort.

Les applications SaaS de sécurité occupent une place particulièrement sensible dans la chaîne de confiance.

La confiance a été longtemps perçue comme antagoniste avec la notion de SaaS. Cela explique l'arrivée tardive du SaaS dans le domaine cyber.

Opter pour un mauvais prestataire de sécurité SaaS, fait pourtant courir des risques majeurs et multiples qui vont bien au-delà d'une simple réponse à des attentes fonctionnelles. L'objectif de ce Livre Blanc est d'identifier ces risques. Si le vol de données est le premier d'entre eux, il en existe d'autres aux lourdes conséquences et ils concernent tous les acteurs : Entreprise, Administration, DSI, RSI, distributeur, intégrateur…

RISQUES	CIBLES	ENJEUX
Intelligence économique : captation de données	Entreprise, Administration	Fuite d'informations confidentielles de toute nature
Espionnage industriel : captation de données	Entreprise, Administration	Fuite d'informations confidentielles de toute nature
Non-respect du RGPD	Entreprise, Administration	• Amendes (20 M€ ou 4% du CA) • Remplacement de solution à la demande d'un employé ou un client • Perte de notoriété
Devenir une US Person	Entreprise	• Soumission aux lois américaines : régime des sanctions, lois sur la corruption… • Amendes • Déstabilisation…
Négligence fautive des personnels informatiques	DSI, RSSI, DPO	Sanctions disciplinaires pouvant aller jusqu'au licenciement pour faute
Diffusion de solutions non conformes à la loi	Intégrateur, Distributeur	Poursuite pour concurrence déloyale



Les risques de choisir des solutions américaines de sécurité en SaaS

Préambule : nous choisissons ici de simplifier l'analyse aux seules solutions américaines car :

- ce sont largement les plus présentes en dehors des solutions européennes,
- les États-Unis se sont dotés de réglementations particulièrement contraignantes (Cloud Act, Fisa…) et un droit extensif (extra-territorialité juridique) qui entraîne des risques particuliers.

Les risques légaux de captation de données : l'intelligence économique

L'environnement juridique américain permet de très nombreuses dérives sur l'accès légal aux données qui sont confiées à des prestataires américains (hébergeurs ou éditeurs de solutions SaaS).

De nombreuses lois et réglementations ont été produites depuis 40 ans. Les plus connues sont :

- L'Executive Order 12333[1] (1981)
- Patriot Act[2] (2001)
- Foreign Intelligence Surveillance Act (FISA) notamment article 702 et 1881a[3] (2008)
- Le Cloud Act[4] (2018)

La plus récente, le Cloud Act, permet ainsi aux organes gouvernementaux américains (qui réunissent tant les départements fédéraux, tels que la CIA, la NSA ou le FBI, que les services locaux des états et leurs sous-divisions politiques) de requérir la transmission de données hébergées aux États-Unis ou en dehors du sol américain auprès de prestataires de services de communications électroniques ou de services informatiques à distance.

[1] *https://www.archives.gov/federal-register/codification/executive-order/12333.html*
[2] *https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act*
[3] *https://www.congress.gov/bill/110th-congress/house-bill/6304*
[4] *https://www.congress.gov/bill/115th-congress/senate-bill/2383/text*

Même si les données sont hébergées en France, elles sont accessibles par les organes gouvernementaux américains car c'est la nationalité de l'éditeur ou de l'hébergeur qui les soumet au Cloud Act, non leur localisation.

Cette transmission d'informations peut se faire sans prévenir l'entreprise qui en est victime.

Il existe une possibilité de recours (encore faut-il être averti…) mais 99% des demandes sont acceptées par les juges américains, il agit donc ici plutôt comme une chambre d'enregistrement.

Le motif d'application de cette loi est très large « sécurité publique, défense et sûreté de l'État ». Elle n'est pas limitée aux enquêtes pénales ou aux actions contre le terrorisme. Pour rappel, dans le cadre du Patriot Act, moins de 1% des requêtes concernaient le terrorisme qui était pourtant à l'origine de la loi.

	Localisation des serveurs US	Localisation des serveurs européens
Éditeur ou hébergeur non US	Soumis au Cloud-Act	Confiance !
Éditeur ou hébergeur US	Soumis au Cloud-Act	Soumis au Cloud-Act

Exemples :

- Un éditeur US qui héberge des données en France est soumis au Cloud Act
- Un éditeur français qui héberge des données sur AWS ou Azure est soumis au Cloud Act

Outre l'obligation légale qui s'impose aux éditeurs SaaS américains, ceux-ci n'hésitent pas à inclure dans leurs Conditions Générales par défaut des clauses autorisant expressément l'exploitation des données qui leur sont confiées, à l'instar de ce que font les GAFAM. Ces conditions ne sont que très rarement analysées par les services juridiques.

Opter pour un prestataire de sécurité SaaS américain c'est donc accepter que ses données puissent être accessibles sans même en être averti. Aucune clause contractuelle (CCT, BCR) signée avec un acteur américain ne peut l'affranchir de respecter la loi à laquelle il est soumis.

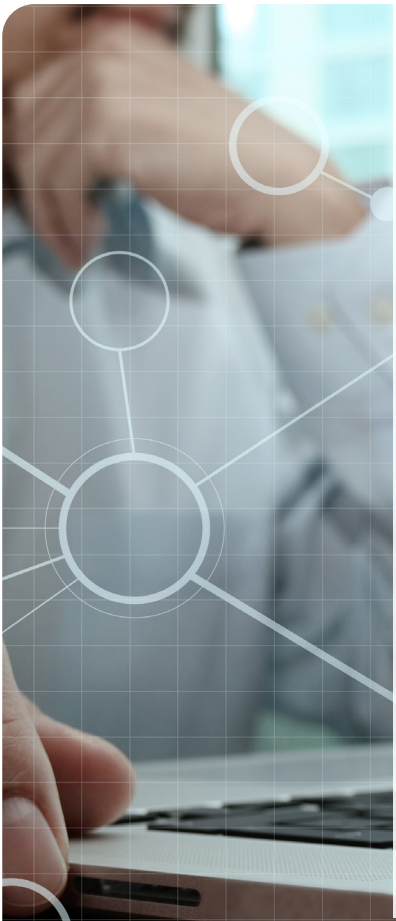
Les risques illégaux de vol de données : l'espionnage industriel

Les révélations Snowden : le recours massif à l'espionnage industriel

À partir du 6 juin 2013, Edward Snowden rend publiques des informations classées top-secrètes sur des agences de renseignement américaines (NSA, CIA…) concernant notamment les systèmes d'écoute sur Internet du gouvernement américain et des programmes de surveillance PRISM, XKeyscore, Boundless Informant, Bullrun…. Il publie en 2019 son autobiographie « Mémoires vives » et révèle de nombreuses informations sensibles sur son gouvernement.

Ce serait faire preuve de candeur, que d'imaginer que les gouvernements ne mènent pas d'opérations d'espionnage industriel. Ce qui frappe dans les révélations Snowden c'est :

- l'étendue des actions d'espionnage
- leur durée de conservation (rien n'est jamais effacé)
- la connivence avec les éditeurs de sécurité



Les révélations de Snowden ont été confirmées et complétées par d'autres lanceurs d'alertes. On apprend notamment que :

- Le budget du renseignement américain atteint 71 Milliard US $ et compte 129.000 personnes. La lutte anti-terroriste représente « seulement » 35% de l'activité du service.
- La communauté du renseignement a recours à l'espionnage industriel pour améliorer les avantages concurrentiels des sociétés américaines.
- La CIA organise des rencontres régulières avec les entreprises US pour partager les « informations recueillies ».
- La collaboration étroite entre la NSA et 100 éditeurs US dont les GAFAM leur permet l'accès direct aux bases de données de leurs clients.
- L'existence notamment du programme, BULLRUN[5], dont l'objectif est l'implantation de portes dérobées « Backdoor » dans les logiciels de sécurité en collaboration avec les éditeurs américains.

Les révélations de Microsoft

Tom Burt, le responsable de la sécurité des clients de Microsoft a apporté, le 30 juin 2021, un témoignage capital devant la commission judiciaire de la Chambre des représentants.*

Il a déclaré que Microsoft reçoit régulièrement des ordres secrets de demandes d'informations, de la part du département de la Justice, sans une analyse juridique ou factuelle significative (« boilerplate secrecy orders unsupported by any meaningful legal or factual analysis »). Microsoft a transmis confidentiellement des enregistrements d'appels et de SMS concernant même des échanges ou des conversations de journalistes.

Les statistiques sont parlantes : Microsoft reçoit entre 2400 et 3500 ordres secrets par an sur environ 11200 demandes. Il sous-entend qu'il en est de même pour Google, Apple, etc ...

La France, un des pays le plus écouté

Pays européen le plus écouté pour l'industrie, capacités d'espionnage et de contre-espionnage.

70,3 millions

Communications interceptées par mois : métadonnées, enregistrement, sms pour la lutte anti-terroriste et la surveillance du monde des affaires. *Entre 10/12/2012 et le 8/01/2013*

Programme de ciblage des administrateurs des systèmes d'information pour implantation de logiciels espion.

Rapport de la DGSI de novembre 2018 « Panorama des ingérences économiques américaines en France » : le service de contre-espionnage français indique l'existence d'une stratégie d'envergure de conquête des marchés et dans laquelle la France est particulièrement exposée.

[5] *https://fr.wikipedia.org/wiki/Bullrun*
**source : https://siecledigital.fr/2021/07/05/etats-unis-donnees-microsoft/*

Le cas particulier du proxy

Comme nous l'avons vu en introduction, les firewalls et les proxys interceptent et déchiffrent tous les échanges avec les applications SaaS extérieures. Si un éditeur de proxy en SaaS avait des intentions malignes, les informations recueillies seraient particulièrement abondantes. Il pourrait aisément obtenir :

- Les données de connexions qui permettent de définir un profil numérique individuel précis notamment des équipes de direction : sites consultés, recherches effectuées dans les moteurs de recherche,…
- Mais aussi tous les fichiers échangés via les applications SaaS métier y compris ceux stockés sur des espaces sécurisés : contrats clients, secrets de fabrications, données financières…

Les révélations Snowden ont créé un choc mondial et de nombreux états ont mis en œuvre des mesures pour se protéger des points de vulnérabilité les plus essentiels. Les DSI, les RSSI et les DPOs ont en charge la sécurité de leurs organisations et la défense de leurs intérêts. Ils doivent aussi préserver les données qui leur sont confiées par leurs employés, leurs clients et leurs partenaires.

Il n'est dorénavant plus possible de faire preuve d'angélisme et d'adopter une posture de victime consentante à la captation de données. Faire le choix de solutions souveraines particulièrement pour des services SaaS de sécurité plutôt que des solutions américaines susceptibles de disposer de backdoor, permet déjà de limiter le risque.

Les risques juridiques RGPD

Le risque RGPD suite à l'invalidation du Privacy Shield

Le RGPD protège le transfert des données personnelles en dehors de l'Union Européenne. Un tel transfert n'est possible qu'avec le consentement explicite et individuel des personnes ou si les lois applicables sur la protection des données locales ont un niveau substantiellement équivalent à celui de l'Union.

Le Privacy Shield était un processus d'auto-certification dérogatoire accordée par la commission européenne en 2016 aux éditeurs et hébergeurs américains. Elle avait considéré, de manière surprenante, que la protection des données personnelles assurée par les lois américaines était équivalente à celle de l'Europe. Pas moins de 4.200 entreprises américaines ont utilisé cette auto-déclaration pour héberger des données personnelles d'Européens.

Le 16 juillet 2020, la cour de Justice de l'Union Européenne a invalidé le Privacy Shield. Elle estime dans son arrêt[6] que :

- Les différentes lois américaines liées aux renseignements (Patriot Act, FISA, Cloud Act…) permettent l'accès par les autorités publiques américaines, aux données personnelles transférées de l'UE vers les États-Unis, de façon particulièrement large et sans ciblage, entraînaient des limitations de la protection des données personnelles qui ne sont pas circonscrites de manière à satisfaire à des exigences équivalentes à celles requises par le droit de l'UE.

- D'autre part, cette législation n'accorde pas aux personnes concernées des droits de recours devant les juridictions contre les autorités etatsuniennes (la CJUE souligne que ces programmes ne prévoient aucune limitation du pouvoir conféré aux autorités étatsuniennes, ni l'existence de garanties pour les personnes potentiellement ciblées non etatsuniennes).

[6] *https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=4802990*

Cette invalidation a entraîné plusieurs recours et saisies de la CNIL.
On notera notamment :

Le cas Health Data Hub

Suite à cette invalidation, un recours a été lancé auprès du Conseil d'État concernant le projet Health Data Hub hébergé chez Microsoft aux Pays-Bas. Dans son ordonnance du 13 octobre 2020[7], le Conseil d'État reconnaît l'existence d'un risque de transfert de données issues du Health Data Hub vers les États-Unis. La CNIL, dans son mémoire en observation sur cette affaire, estime que la Société Microsoft peut être soumise à des injonctions l'obligeant à transférer des données stockées et traitées sur le territoire de l'Union Européenne quelles que soient les clauses contractuelles car la loi américaine l'y oblige. En conséquence, la CNIL a obtenu du Ministère de la Santé la garantie d'un changement de solution technique dans un délai maximum de 18 mois.

Le cas Doctolib

Le 12 mars 2021, le juge des référés du Conseil d'État a rendu son avis[8] sur le stockage des données de prise de rendez-vous pour la vaccination Covid-19 sur la plateforme de droit américain AWS. Elle a considéré qu'elle était conforme car les données personnelles étaient chiffrées par le biais d'une procédure permettant d'empêcher la lecture des données par des tiers. Cette procédure reposait sur un tiers de confiance français.

Le cas Teams

Le 27 mai 2021, la CNIL saisie par les présidents d'Université et la Conférence des grandes écoles sur l'utilisation d'outils collaboratifs américains (Teams…) appelle à une évolution de l'utilisation de ces outils compte tenu du risque d'accès illégal aux données personnelles qui contrevient au RGPD[9].

[7] *https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/440916*
[8] *https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-03-12/450163*
[9] *https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche*

Application aux logiciels de sécurité en SaaS

Les applications SaaS de sécurité stockent toutes des données personnelles puisqu'elles ont un devoir de traçabilité. Parmi les données les plus courantes on trouve :

- des données de sécurité propre : trafic internet nominatif, les connexions horodatées aux différents systèmes, mais aussi les données échangées,
- des données personnelles des employés quand ils se rendent sur des sites personnels en utilisant les accès de l'entreprise : sites de santé, de finance…
- des données potentiellement beaucoup plus sensibles comme les fichiers échangés avec les applications SaaS métiers externes : contrats clients, secrets de fabrications, données financières…

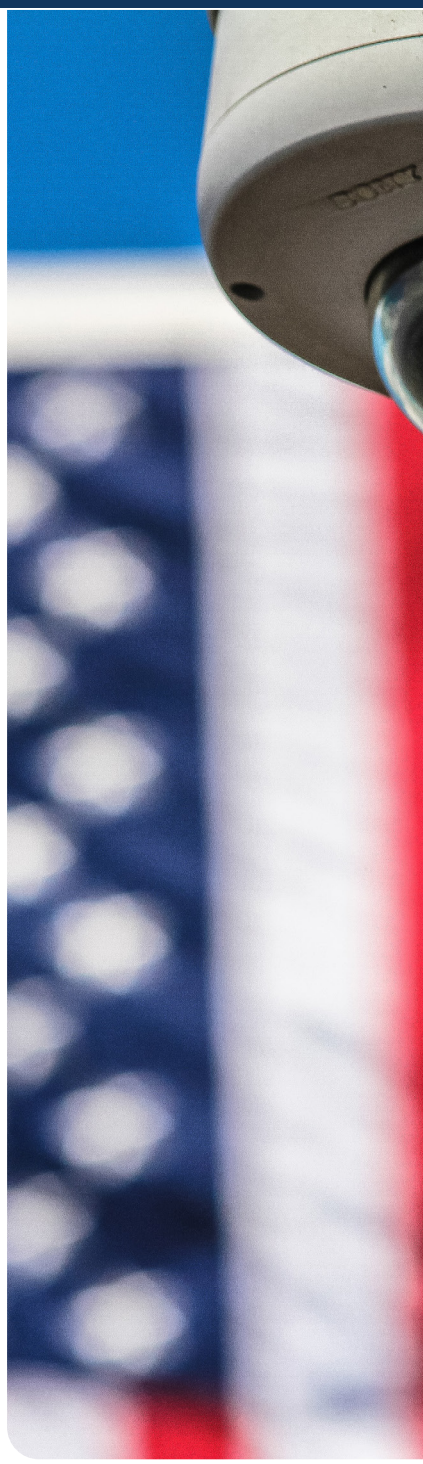
Les logiciels de sécurité en SaaS doivent donc impérativement respecter le RGPD.

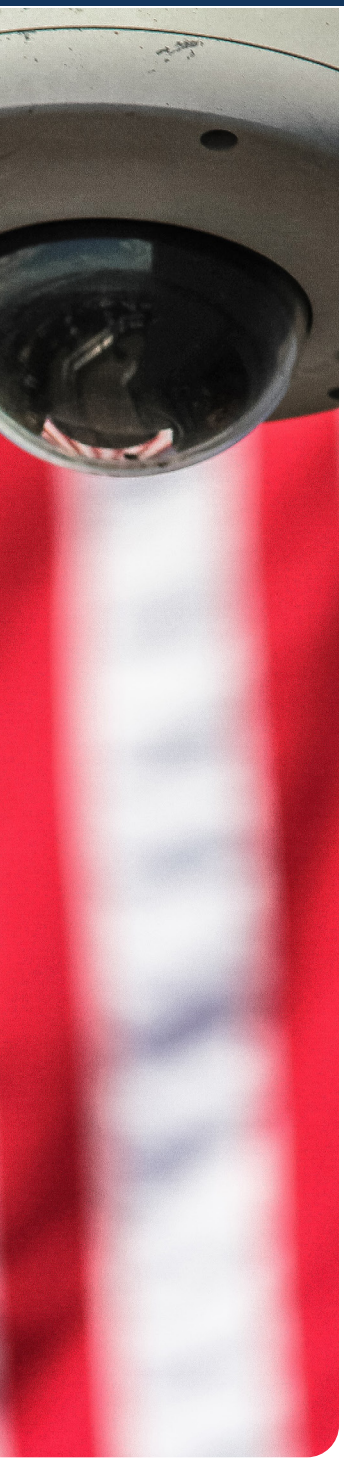
Il n'est pas possible de se mettre en conformité RGPD par l'ajout de simples clauses contractuelles (CCT, BCR) car les lois américaines sont applicables même avec ces clauses et rendent caduques la conformité RGPD. Ce point est réaffirmé dans les différentes jurisprudences

S'ils sont de droit américain, pour être conformes, ils doivent impérativement chiffrer les données collectées et remettre les clés à leur client de manière exclusive.

Les conséquences d'acquérir et d'utiliser des solutions non conformes au RGPD sont de 2 ordres :

- l'obligation d'arrêter le projet et de remplacer la solution par une autre conforme, en cas de saisie de la CNIL (cas Health Data Hub). Dans le cas d'une passerelle de sécurité web, une plainte d'un employé voire d'un client peut suffire.
- Des sanctions pécuniaires : les amendes pour viol du RGPD peuvent aller jusqu'à 20 M€ ou 4% du chiffre d'affaires.





Les risques de devenir une US Person

Comment devient-on une US Person ?

Être une « US Person » soumet des personnes physiques ou morales (entreprises) à la compétence juridictionnelle américaine. Cela signifie que les US Persons peuvent être jugées par une cour américaine et selon les lois votées aux États-Unis quel que soit l'endroit où elles se trouvent.

Cela concernait historiquement les résidents américains et les sociétés de droit américain. Mais l'extraterritorialité du droit américain est devenue de plus en plus extensive.

Au fil des années, devenir US Person s'est appuyé sur des critères de plus en plus étendus :

- L'utilisation du dollar dans les transactions.
- La présence d'une filiale aux États-Unis.
- La nationalité des actionnaires…

L'utilisation de technologies américaines est devenue un nouveau lien pour justifier la compétence juridictionnelle américaine. Le rapport Gauvain[10] de juin 2019 dénonce cette nouvelle dérive :

> Au total, il apparaît que l'interprétation large et mouvante qu'elles font de leur compétence confère aux autorités fédérales américaines, notamment au DoJ (Département de la Justice) ou à la SEC (Organisme de contrôle des marchés financiers), une grande liberté d'action : elles peuvent intervenir dans presque toutes les transactions commerciales ou financières internationales, en vertu de critères de rattachement à leur territoire aussi contestables que l'utilisation d'emails transitant sur des serveurs américains, le stockage de données sur des serveurs américains, ou l'utilisation du dollar dans la transaction.

[10] *https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf*

Le rapport Lellouche de 2016[11] citait déjà le cas de l'affaire Straub et Consorts, société hongroise, dans laquelle le lien invoqué était l'utilisation de Gmail pourtant souscrit en Hongrie au prétexte que les mails transitaient par des serveurs américains. La société a pu ainsi être condamnée par un tribunal américain pour avoir enfreint l'embargo sur le Monténégro…

L'utilisation de technologies américaines dans son système d'information fait donc courir un nouveau risque, celui de devenir une US Person.

Les conséquences d'être une US Person

Les US Person se trouvent soumises à de multiples lois américaines. Celles qui ont été les plus utilisées par la justice américaine sont :

- La lutte contre la corruption dans les transactions internationales : le Foreign Corrupt Practices Act.
- La lutte contre les États soutenant les groupes terroristes : la loi d'Amato-Kennedy (interdiction de ventes à certains pays).
- La fiscalité : le Foreign Account Tax Compliance Act.
- La surveillance comptable et financière et la corruption : la loi Sarbanes-Oxley…

Les amendes infligées aux entreprises françaises ces dernières années représentent plusieurs milliards de dollars (Société Générale, Crédit Agricole, Total, Alcatel, Alstom, Technip…). Le record étant détenu par la BNP avec 9 milliards de dollars d'amende, pour ne pas avoir respecté les embargos américains sur le Soudan, l'Iran et Cuba.

Ces amendes sont aussi utilisées comme élément de guerre économique afin de déstabiliser des entreprises dans la perspective de s'en emparer. C'est par exemple le cas d'Alstom rachetée par son rival Général Electric avec la complicité du département de la Justice américain[12].

Elles peuvent servir à d'autres types de représailles : fermeture du marché américain (fournisseurs du Nord Stream 2), arrêt des services délivrés par des éditeurs américains (Huawei perd sa licence Android), peine d'emprisonnement (Frédéric Pierucci cadre dirigeant d'Alstom)…

Pour les entreprises qui ne sont pas déjà de droit américain, il faut éviter à tout prix de devenir une US Person. C'est un nouveau risque entre les mains de la DSI et de la RSSI en cas de choix de solutions entraînant un dépôt de données sur des serveurs de droit américain ou de flux passant par les US.

[11] https://www.assemblee-nationale.fr/14/rap-info/i4082.asp
[12] https://www.youtube.com/watch?v=dejeVuL9-7c

Les risques de négligence fautive du DSI, du RSSI et du DPO

Les personnels des métiers informatiques, qu'ils soient directeurs de la sécurité des Systèmes d'Information, administrateurs ou Responsable de la Sécurité des Systèmes d'Informations, peuvent être responsables en cas d'incompétence professionnelle ou de négligence fautive.

C'est la déclinaison de l'article 1241[13] du Code civil : « *Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence* ».

La responsabilité des personnels peut être recherchée, dans le cadre de leur sphère professionnelle sur 2 axes :

1

Le premier axe de responsabilité peut-être celui de l'incompétence professionnelle ou de la négligence fautive. Dans le cadre du choix d'une solution de sécurité SaaS ne respectant manifestement pas le RGPD et/ou faisant courir des risques majeurs à l'entreprise (soumission au Cloud Act, fuite d'informations, transformation US Person…) la question sera posée, à la première alerte, d'un manquement à ses obligations.

2

Le deuxième axe de responsabilité porte sur l'exécution de demandes formulées par l'employeur (Direction Générale) et qui s'avéreraient manifestement illicites ou risquées quant à la mise en œuvre, au déploiement ou à l'utilisation des données. Exemple : utilisation d'un produit groupe non conforme en Europe.

Les sanctions disciplinaires peuvent aller jusqu'au licenciement pour faute.

Afin de se prémunir, vis-à-vis de ce risque personnel, exposé dans le cadre de son engagement professionnel, les DSI et RSSI ont tout intérêt à informer leur Direction Générale et leur direction juridique, par une note de service, pour les alerter sur les risques de la solution envisagée. L'arbitrage sera ainsi collectif et les libérera d'une potentielle responsabilité par négligence.

[13] *https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032041565/*

Les bonnes pratiques

pour choisir une solution de sécurité en SaaS

Le proxy proposé en SaaS occupe une place particulière dans la chaîne de confiance des équipements de sécurité web. En effet, en tant qu'outil d'interception du flux web, il accède à l'ensemble du contenu web entrant et sortant de l'entreprise. Il convient donc de le sélectionner avec une attention particulière.

La grille d'évaluation des solutions analysées, outre les traditionnels critères techniques, doit permettre d'apprécier les vulnérabilités aux risques décrits dans ce Livre Blanc :

- Quelle est la nationalité de l'éditeur ? (Pour rappel, la localisation des données est sans importance)
- Quelle est la nationalité de l'hébergeur ?
- Quelles sont les données interceptées par le proxy ?
  - Enveloppe de la connexion : domaines, url, horodatage…
  - La traçabilité par utilisateur.
  - Les contenus accédés (supposent le déchiffrement des flux SSL) et notamment les fichiers échangés avec les applications SaaS métiers utilisées par les collaborateurs…
- La solution respecte-t-elle le RGPD ?
- Si la solution est américaine quel est le moyen de chiffrement appliqué sur les données stockées ?

D'autres questions sont liées directement à l'entreprise :

- Mon entreprise est-elle déjà US Person ? Dans le cas contraire, faire évaluer le risque auprès de la Direction Juridique ou Générale pour évaluer le danger d'enfreindre des lois américaines (FCPA, relations commerciales avec des pays sous embargo…)
- Suis-je amené à traiter des données personnelles réglementées : santé, correspondance d'avocats... ? Elles ajoutent des obligations à celles du RGPD dont il faudra s'assurer du respect.

Faire de la confiance un argument de différenciation

L'invalidation du Privacy Shield de juillet 2020, les derniers jugements du Conseil d'État mais aussi les affaires récurrentes montrant que les GAFAM exploitent indûment les données personnelles des européens, accroissent les exigences en matière de protection de données. Les employés des entreprises, ainsi que les clients sont de plus en plus vigilants sur leur exploitation potentielle.

Plutôt que de se lancer dans des projets manifestement non respectueux du RGPD, en espérant ne pas être pris (cas du Health Data Hub), il est préférable de faire de la conformité un argument de valorisation de son image et de ses offres aussi bien en interne qu'en externe.

La position des distributeurs et des intégrateurs

La sélection de solutions de sécurité concerne en premier lieu les entreprises mais aussi les distributeurs de solutions lorsqu'ils constituent leur catalogue d'offres à proposer à leurs clients.

Ils ont un devoir de conseil éclairé et donc de chercher à minimiser les risques. Par ailleurs, la distribution de solutions manifestement illicites (exemple non-respect du RGPD) sur le territoire européen, les expose à des recours pour concurrence déloyale.

Question
à notre expert

Jean-Noël DE GALZAIN,
PDG Wallix Group, Président HEXATRUST, Pilote du projet cyber de la filière

Pourquoi faut-il privilégier les solutions souveraines et faire le choix clair de la préférence européenne ?

Dans les dix ans à venir, les investissements dans la relance post-Covid, ajoutés à la modernisation de notre industrie, à la transformation des usages des services publics ou de nos territoires vont aller bien au-delà du Plan Marshal de 1947 en termes de dépenses publiques et privées. Selon l'institut IDC, « Les dépenses européennes en technologies et services qui permettent la transformation numérique des entreprises, des produits et des organisations devraient atteindre 378,2 milliards de dollars en 2022[1] » rien qu'en Europe, et 1800 milliards de dollars dans le monde[2]. À la vue des montants qui vont être injectés dans l'économie numérique, une politique industrielle stricte et efficace doit s'imposer en France et en Europe dès que possible. Celle-ci doit accompagner la mise en œuvre d'un numérique de confiance conforme aux réglementations européennes - telles que le RGPD, la Directive NIS, le DGA et le DMA- et assurer un retour sur investissement pour les européens.

Ainsi, nous devons faire le choix clair de la préférence européenne dans nos achats. C'est une priorité aujourd'hui pour nous permettre de développer nos industries technologiques clés (comme la cybersécurité, l'Intelligence Artificielle ou les infrastructures numériques). Il ne s'agit pas ici de tomber dans un protectionnisme qui pourrait ralentir la créativité de l'offre, mais bien, de réduire notre dépendance aux outils et infrastructures étrangères sur lesquelles nous n'avons aucun contrôle, afin de protéger les intérêts des organisations européennes quotidiennement et lors de la survenance d'une crise.

Comment réduire cette dépendance ? Comment faire le choix de la préférence européenne pour bâtir des frontières numériques Wsouveraines ?

Grâce à une politique d'achat que l'on appellerait un European Buy Act où chaque euro investi serait directement fléché auprès de nos entreprises locales en priorité.

Cela doit être le choix de nos gouvernements dans tous les investissements de relance et de modernisation à venir, et aussi celui des directions générales, achats, et informatiques des grands donneurs d'ordres.Ces achats seront décisifs pour alimenter la croissance de nos entreprises de technologies, pour qu'elles se développent, pour diminuer nos importations et créer de l'emploi.

La sécurité web européenne en SaaS

Olfeo SaaS est la première offre de sécurité web européenne en SaaS de confiance.

Une révolution informatique s'opère sous nos yeux : le logiciel devient un service au lieu d'un produit à administrer soi-même. Cette révolution est tellement profonde qu'il semble aujourd'hui archaïque d'installer des produits dans ses datas centers !

La cyber sécurité est plus réticente à suivre cette mutation car les enjeux de confiance y sont particulièrement élevés. Les seules offres disponibles étaient jusqu'à présent américaines ce qui posaient de nombreuses questions sur l'exploitation qui était faite des données, à l'instar des pratiques des GAFAM, ou encore sur le non-respect du RGPD.

Olfeo SaaS s'appuie sur 4 avantages différenciants :

1. Gardez le contrôle sur vos données
2. Sécurisez votre SI grâce à l'environnement de confiance sur Internet
3. Formez et responsabilisez vos collaborateurs à la sécurité
4. Garantissez votre conformité juridique

Olfeo est leader européen de la sécurité web. Ses solutions de passerelles de sécurité, SaaS ou On-premise, protègent le système d'information contre toutes les menaces provenant du web. Sa technologie Trust-Centric qui n'autorise l'accès qu'aux seuls sites de confiance, offre le plus haut niveau de sécurité.

20 ans
d'expertise

99 %
requêtes reconnues

1 000
clients

Olfeo saas
La plateforme web de cybersécurité en toute simplicité

Olfeo on-premise
La solution de cybersécurité qui s'intègre à votre infrastructure IT

Olfeo awareness
Vos collaborateurs deviennent des piliers de votre stratégie de sécurité

Olfeo oem
Les bases de données d'URLs et d'applications Saas d'Olfeo mis à disposition des éditeurs cyber

FRANÇAISES UTILISE PAR LES ARMÉES FRANÇAISES

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

FRANCE CYBER SECURITY

Contactez-nous

contact@olfeo.com

www.olfeo.com

Olfeo

Olfeo - SIRET 450 136 346 - Ne pas jeter sur la voie publique - Juin 2023