Vous avez dit souveraineté ?

Alain BOUILLÉ
Expert Cybersécurité

Les propos de cet article reflètent l'opinion de son auteur et n'ont aucunement vocation à représenter la position de quel qu'organisme ou quel que groupe de travail que ce soit dans lesquels l'auteur est par ailleurs impliqué.

Le sujet de la souveraineté en matière de numérique devient une sorte de marronnier qui s'apparente à une mauvaise série où à la fin de chaque épisode, on a l'impression que c'est toujours le même qui gagne ou plutôt le même qui perd à savoir notre souveraineté numérique !

Les batailles perdues du 20ème siècle

L'histoire hoquète depuis 40 ans où toutes les batailles (mais au fait s'est-on vraiment battus ?) ont été perdues ou presque. Ce fut d'abord le cas du hardware remporté de main de maître par les Américains qui font depuis longtemps travailler les Chinois pour la fabrication de leurs matériels. Puis, ce fut le software également gagné par les Américains avec cependant quelques poches de résistance dont SAP reste sans doute la plus notable en Europe. Entre temps, il n'est pas besoin de s'appesantir sur l'épisode Minitel / Internet, l'histoire a mille fois été contée.

L'émergence des GAFAM et… des premiers Clouds Souverains

À l'avènement du Cloud Computing au début des années 2000, l'Europe est restée coi et s'est laissée submerger par ceux qui n'étaient pas encore les géants de la Californie et que l'on n'appelait pas encore les GAFAM ! Sans doute piquée par l'hégémonie de ces derniers qui se répandaient comme une traînée de poudre dans les entreprises françaises et dans le reste du monde, la France sort de sa torpeur 12 ans plus tard, autrement dit un siècle à la vitesse du numérique et lance avec panache le cloud souverain à la française sous l'impulsion du Président Sarkozy ! Comme on ne pouvait pas faire simple, deux sociétés voient le jour, Cloudwatt et Numergy avec un investissement initial de 150 millions d'euros qu'il a fallu partager en deux soit 75 millions d'euros chacune. Ce montant peut sembler trop élevé quand on connait la fin de l'histoire, mais représente une infime goutte d'eau comparée aux milliards de dollars investis de l'autre côté de l'Atlantique par les géants californiens parfois en pure perte. Mais en France on ne supporte pas l'échec et les détracteurs de la souveraineté se délectent dès qu'ils le peuvent de ces « débâcles » pour justifier qu'il vaut mieux aller en Californie chercher les solutions à nos besoins numériques.

La Data et le RGPD

Du coup, lorsque les datas ont commencé à jaillir dans les années 2010 tel l'or noir au 19ème siècle, on s'est dit que là peut-être quelqu'un allait se réveiller pour faire en sorte que nos gisements de données ne traversent pas l'Atlantique par les pipelines de l'Internet. C'est alors qu'on a sorti l'arme absolue, à savoir le RGPD qui devait mettre au pas, entre autres, les grands acteurs du cloud qui commençaient à

malmener les données privées des usagers en toute impunité. Les GAFAM n'ont pas tremblé longtemps, car ce fut eux paradoxalement qui ont affiché d'insolentes conformités au RGPD avant tout le monde tandis que les entreprises françaises ramaient pour être « compliant » à la date fatidique du 25 mai 2018.

Certes le RGPD représente une avancée indéniable en matière de protection des données à caractère personnel, mais n'aide aucunement les RSSI à protéger les données critiques de l'entreprise qui ne sont justement pas « à caractère personnel » ! Ce règlement a aussi contribué à ce que les GAFAM construisent des data centers en France pour éviter des flux de données trop problématiques vers les USA ou l'Irlande ou encore les Pays-Bas, mais on s'est bien gardé d'imposer dans le règlement une quelconque étanchéité de ces données pourtant stockées en France, aux lois extraterritoriales américaines (Patriot Act, Cloud Act…). On rencontre encore pourtant quelques naïfs ou pire des incompétents qui ne voient pas le problème et qui s'imaginent que parce que les données sont en France, tout baigne !

Les ravages des solutions collaboratives pour la protection du patrimoine informationnel

Là où la situation a commencé à devenir ingérable pour les données des entreprises, c'est lorsqu'on a commencé à s'équiper d'outils dits collaboratifs et que l'on a externalisé les messageries des entreprises et tant qu'on y était les répertoires bureautiques avec, trop contents de se débarrasser de ces boulets qui encombraient les datacenters des entreprises avec un niveau de service de plus en plus décrié. Que celui qui ne s'est pas retrouvé un beau matin obligé de « nettoyer » sa boîte aux lettres pour envoyer le message archiurgent à son chef, mais qui ne pouvait partir parce la boîte aux lettres était pleine lève le doigt ! Alors évidemment quand on annonce une boîte aux lettres de taille quasi illimitée à ces utilisateurs, ils demandent tout de suite la date de la migration !

Lorsqu'on externalise dans le Cloud un service, une base de données, une application métier, bref des données connues et maîtrisées, les RSSI sont suffisamment outillés pour effectuer une analyse de risques appropriée, pointer les données critiques et mettre en œuvre les outils de protection adaptés… et il y en a pléthore ! Seulement lorsqu'il s'agit de migrer son environnement bureautique, effectuer cette analyse relève d'une mission impossible, car on ne sait jamais in fine ce que contient les milliers de boîtes aux lettres d'une entreprise et les milliards de fichiers bureautiques stockés parfois depuis des décennies ! Lorsqu'on est suffisamment kamikaze (j'en connais au moins un !) pour se lancer dans une analyse de ces contenus, on y découvre un énorme foutoir où on y croise un peu de tout : des données RH en pagaille, des notes stratégiques, des plans à 5 ans, des rapports d'audit, des prévisions d'investissement… avec des données certes correctement protégées dans les applications qui les gèrent, mais mises au clair dès qu'elles se retrouvent stockées dans des espaces bureautiques et en pièce jointe de mails.

Alors que deviennent toutes ces données ? Eh bien la plupart du temps, elles sont ni plus ni moins « bennées » dans les Clouds telles quelles, et la plupart du temps sans protection particulière ! Bon débarras et en plus il n'y a que des vieux trucs ! Ben voyons.

La supercherie des solutions hybrides et des systèmes de protection

Hybridation : au début de ces projets collaboratifs, les entreprises se sont lancées dans des analyses de risques plus ou moins sérieuses, plus ou moins complaisantes selon la pression exercée par le porteur du projet (en général le DSI) sur celui chargé de cette analyse (en général le RSSI aux ordres du DSI, cherchez l'erreur !). Il y a même des cas où il n'y a pas eu d'analyse de risques du tout. En général, la grande trouvaille pour les données sensibles a été de considérer que seuls les VIP en manipulaient, donc il suffisait de garder un mini service de messagerie « on premises » pour ces utilisateurs sensibles et le reste

pouvait être externalisé en toute quiétude. Comme si les VIP n'écrivaient jamais à l'étage d'en dessous et n'échangeaient jamais des pièces jointes sensibles avec leurs collaborateurs et comme si les données les plus sensibles n'étaient pas manipulées par des salariés en bas de l'organigramme ? Mais cette option rassurait les COMEX, on leur épargnait une décision douloureuse en les chouchoutant ainsi ! Ces solutions dites hybrides ont très vite fait long feu du fait de la porosité des deux mondes et du surtout du coût qu'elles généraient.

Protection : d'aucuns ont pu se lancer dans des solutions de chiffrement pour protéger leurs données sensibles. Trois écueils à cette option :

- D'abord comme on ne peut pas tout chiffrer, on demande à l'utilisateur de faire le tri en classifiant ses fichiers et ses mails. Mais comment peut-on être certains que l'utilisateur joue le jeu s'il sait qu'une classification élevée est synonyme de dégradation de la fameuse « expérience utilisateur » ?
- Ensuite on a le choix d'utiliser la solution de chiffrement proposée par l'hébergeur qui est parfaitement intégrée à l'ergonomie de la solution… mais qui ne sert à rien, en tous cas pas à se protéger de l'hébergeur, puisque ce dernier garde la clé de chiffrement.
- Vient enfin l'option d'utiliser ses propres clés, mais à ce moment-là le service n'a en effet plus accès aux données et l'expérience utilisateur est dégradée, car ses mails ne sont plus indexés et il est obligé de les classer à la main comme au bon vieux temps !

La dernière possibilité reste l'aiguillage des mails sensibles vers une solution dite de confiance, mais toujours avec l'écueil que cet aiguillage reste à la main de l'utilisateur en fonction de la classification. De telles solutions sont actuellement en développement chez certains offreurs de confiance… à suivre.

La non-réversibilité des solutions, l'enfermement des clients et le verrouillage de la concurrence

Au début de ce nirvana du Cloud, les ROI étaient flamboyants. Bien sûr on pouvait se débarasser de toutes ces machines, de ces coûteux data centers et des informaticiens qui allaient avec ! Enfin pas tous, car il a fallu très vite s'occuper de ces solutions Cloud dont la complexité est la marque de fabrique sans parler des contrats où des armées de juristes doivent être recrutées pour les comprendre et les suivre.

Mais il a fallu très vite déchanter. On a vu des premiers renouvellements de contrat s'accompagner d'une « petite » rallonge de 35 % avec une totale impossibilité de revenir en arrière. On n'avait déjà pas assez de serveurs pour héberger des boîtes aux lettres de taille limitée, alors des boîtes aux lettres de taille illimitées 3 ans après les premières migrations, il faudrait en racheter des serveurs ! Allez à la concurrence ? Chez Monsieur Google ? Alors oui l'irréversibilité (l'enfermement devrait-on dire) est un problème, car cela veut dire qu'aujourd'hui les clients sont pieds et poings liés avec ces fournisseurs et qu'ils ne se gênent plus pour augmenter les tarifs de manière indécente. Il y a belle lurette que les gros clients n'osent plus parler de ROI pour justifier leur basculement dans le Cloud. Il reste bien sûr l'immense richesse de ces offres qui, il faut bien le reconnaître, n'ont pas d'égal à date.

On l'a vu avec la crise COVID, dépendre d'un seul pays, en l'occurrence la Chine, pour la fourniture de tonnes de choses très utiles en cette période de crise était une très mauvaise idée et que rééquilibrer (un peu !) nos capacités de production nationale serait sans doute une bonne idée. Faudra-t-il une crise similaire, les morts en moins il faut l'espérer, pour que la France et l'Europe réalisent que de dépendre que d'une seule nation étrangère pour la fourniture de 80 % de ses services informatiques devenus essentiels pour la bonne marche de l'économie, n'est pas non plus une bonne idée ?

Optimisation ou… fraude fiscale ?

Chacun sait que les GAFAM ne payent pas les impôts qu'ils devraient payer en Europe, la faute à une fiscalité avantageuse organisée par… l'Europe elle-même. Comment alors jouer à égalité quand les offreurs de Cloud français ne font pas signer leurs contrats en droit irlandais à leur client ? Ce sujet est un problème complexe qui semble insoluble, mais qui du coup aggrave la situation qui, si on n'y remédie pas, sera toujours au détriment du cloud souverain.

Les parlementaires s'intéressent au sujet

D'excellents rapports ont été produits par les parlementaires sur le sujet de la souveraineté les années passées. Les deux derniers en date « Le devoir de souveraineté numérique » du Sénat sous l'égide de Gérard Longuet et celui de l'Assemblée nationale sous l'égide du député Raphaël Gauvain « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale » abordent ces questions et donnent des pistes intéressantes en matière de légifération. Le rapport Gauvain en particulier établit la liste de ce qu'il faut faire spécifiquement dans ce domaine… on ne pourra pas dire, je ne savais pas ! Alors qu'attend-on ?

La fausse bonne idée des données sensibles

Quand on parle de Cloud Souverain, automatiquement l'auditoire associe cette notion aux seules informations sensibles. Je ne sais pas d'où vient cette fâcheuse habitude que de ne s'intéresser qu'aux données sensibles quand on parle de Cloud Souverain mais à l'ère du Big Data et de la Data Science, où l'on sait désormais faire « parler » les données qui, individuellement, ne présentent aucun intérêt, mais agglomérées dans des data lakes, représentent souvent une grande richesse à exploiter, il serait temps de reconsidérer cette restriction. Les offreurs de Cloud Souverain seraient donc condamnés à ne ramasser que les miettes laissés par les GAFAM ou du moins les données que les entreprises même les plus aventureuses n'ont pas encore osé externaliser ? Le Cloud Souverain doit aussi s'ouvrir aux données hautement valorisables.

Les bras d'honneur à la souveraineté

Il y a certes des circonstances atténuantes pour les entreprises qui n'ont pas le choix quand il s'agit d'externaliser leur service de messagerie. Car seules deux offres sérieuses sont disponibles sur le marché : Microsoft, leader en la matière, et Google. Et on ne peut tout de même pas leur en vouloir de proposer des solutions performantes !

En revanche, quand des solutions souveraines sont disponibles et concurrentes des GAFAM pour l'hébergement des données de santé par exemple, pourquoi diantre laisser fabriquer un process d'agrément qui ne barre pas la route aux entreprises assujetties à des lois extraterritoriales ? La dernière décision en date où le gouvernement français a pris la décision d'héberger les informations de santé de millions de Français (Cf. projet Health Data Hub) sur les serveurs de Microsoft, au détriment d'OVH, une société française, s'apparente à un bras d'honneur à tous les travaux en cours pour tenter de sauver ce qui peut encore l'être en matière de souveraineté.

GAIA-X une solution souveraine ?

Cette décision malheureuse pour la souveraineté concernant le Health Data Hub tombe au pire moment. Celui où l'Allemagne et la France annoncent la création de GAIA-X, censé offrir une alternative aux solutions de Google, Amazon et Microsoft. On peut résumer que GAIA-X est une sorte de catalogue de services numériques portés par des fournisseurs qui se seront préalablement engagés sur des standards supposés renforcer la confiance de leurs clients en matière de sécurité des données, mais aussi de transparence des contrats et enfin d'interopérabilités des technologies d'un hébergeur à l'autre. Mais on apprend que GAIA-X ne sera pas fermé aux GAFAM qui pourront proposer leurs services à condition de respecter le cahier des charges. Je ne suis pas spécialiste juridique, mais cette hypothétique

adhésion à GAIA-X ne les rendra pas hermétiques aux lois extraterritoriales de leur pays d'origine, dans ce cas pourquoi mettre GAIA-X au crédit des offres souveraines ?

En conclusion, personne ne peut le nier, les résultats ne sont pas à la hauteur des attentes. Le sujet pourrait sembler éculé, car les projets de souveraineté numérique sont évoqués depuis plusieurs décennies, et pourtant la situation de dépendance ne fait qu'empirer. Et si nous nous y prenions mal ?

J'insisterais cependant sur quelques mesures :

- Légiférer sur la protection des données sensibles des entreprises qui ne sont pas soumises au RGPD et qui devraient n'être éligibles qu'à des clouds de confiance.
- S'intéresser aux données hautement valorisables qui devraient aussi être candidates au cloud de confiance.
- Soutenir la filière pas seulement par des investissements massifs, mais par des commandes à commencer par l'État qui n'a pas donné l'exemple ces derniers mois.
- Changer le mode de pensée qui implique que l'herbe est plus verte de l'autre côté de l'Atlantique. Les solutions françaises et européennes sont là et ne demandent qu'à se développer.
- Trouver les moyens sans protectionnisme exacerbé pour donner une préférence française/européenne comme le font les américains chez eux pour leurs propres fournisseurs, un « Patriot » (au sens premier du mot) Act européen en quelque sorte .
- Mettre les solutions européennes et non-européennes sur un pied d'égalité fiscale.