Souveraineté numérique et logiciel libre

Quelques pistes de réflexion (WIP / rien d'officiel à ce stade).

Stéfane Fermigier

Founder & CEO, Abilian - Enterprise Social Software

abilian
CONNECTED, WE WORK!

Plan

1. Ce que dit la loi aujourd’hui
2. Rappel historique
3. Développements récents

Ce que dit la Loi aujourd’hui

“**Les administrations** mentionnées au premier alinéa de l'article L. 300-2 du code des relations entre le public et l'administration **veillent à préserver la maîtrise, la pérennité et l'indépendance** de leurs systèmes d’information.

Elles **encouragent** l'utilisation des **logiciels libres** et des **formats ouverts** lors du développement, de l'achat ou de l'utilisation, de tout ou partie, de ces systèmes d'information.”

Article 16 de la Loi République Numérique du 8 octobre 2016

abilian

TIO / Tio Libre (2008-2010)

abilian

Total Information Outsourcing (TIO)

Outsourcing of business informations systems is being revolutionized by the worldwide availability of broadband Internet and by the ubiquitous access to innovative Web services designed for the Enterprise. Buzzwords such as Web 3.0, Enterprise 2.0, SOA, SaaS, PaaS or Cloud simply mean that a company can now be entirely run through the Web using abrowser, a laptop or a mobile phone and a wireless access to the Internet. Total Information Outsourcing (TIO), from corporate servers to business applications, from online consulting to corporate information sharing, from e-learning to business process management, has become a relevant alternative to accelerate the implementation yet reduce the costs of corporate information systems. It also provides new opportunities for business optimisation which go far beyond the mere outsourcing of tangible and intangible IT facilities.

The first goal of the TIO workgroup is to study the consequences of TIO on Infrastructure Freedom. The second goal of the TIO workgroup is to provide definitions and guidelines - a.k.a. TIO Libre - to implement TIO without losing Freedom and Control of the Enterprise information system. Definition and guidelines are expected to be summarized in a research article. The third goal of the TIO workgroup is to increase the awareness of the market for TIO Libre solutions which provide a relevant alternative to proprietary TIO solutions.

FFII TIO Working Group

FFII started a working group on September 2008 to study TIO in the Information Infrastructure Freedom. This Wiki tries to provide a overview of TIO tools, services and practices. It will eventually lead to recommendations in the area of TIO to companies and governements looking for TIO services which are

Topics

- TioSecurity : what are the threats posed by TIO to corporate security or to national security
- TioTour: a tour of TIO practices such as SaaS (ex. Salesforce, co-ment, ERP5 Express), data aggregation services (ex. Lokad), hosting (ex. OVH, Amazon), social networks, etc.
- TioTaxonomy : a comprehensive set of abstractions which can be used to categorize the different kinds of TIO
- TioSwot : strength, weaknesses, opportunities and threats posed by TIO growth in companies and society
- TioNomics : the economy of TIO (competition, business models)
- TioPortability : keeping access to data structures and interoperability in a TIO context
- TioControl: keeping Information Systems under control in a TIO context
- TioHumanFactor: how can TIO provide the same guarantees in terms of loyalty as regular staff or civil servants
- Tio Libre Definitions: what does Information Freedom mean in the context of TIO
- TIO Guidelines: 3 easy steps to assess your TIO provider
- OpenSourceTio : what are the relations between open source and TIO
- TioSla : what should a TIO SLA (Service Level Agreement) contain to protect customers of TIO services
- SlaEffectiveness : how effective is an SLA
- SlaWorstPractice : examples of dangerous clauses in SLAs of certain TIO providers
- TioPrivacy : is privacy Law compatible with Freedom in the context of TIO
- TioDefinition : what is TIO ?

TIO Libre

TIO Libre est une association à but non lucratif française, composée d'experts et de fournisseurs de service d'externalisation de l'information.

L'objectif de cette dernière est de promouvoir la liberté des clients et la loyauté envers les clients des fournisseurs de service.

TIO est l'acronyme de Total Information Outsourcing.

Sommaire [masquer]

Définitions [modifier | modifier le code]

TIO Ouvert [modifier | modifier le code]

Un service est considéré ouvert si le contrat de service contient l'élément suivant[2] :

- **Liberté des données** : il est possible de migrer toutes les données de l'utilisateur, y compris les logs de connexion vers une infrastructure gérée par un opérateur tiers. Les données doivent être fournies dans un format qui doit être spécifié, correctement documenté et qui peut être utilisé avec des logiciels habituellement utilisés.

TIO Libre [modifier | modifier le code]

Une solution d'externalisation de l'information est considérée comme libre si le contrat de service contient les éléments suivants :

- **Liberté des données** : il est possible de migrer toutes les données de l'utilisateur, y compris les logs de connexion vers une infrastructure gérée par un opérateur tiers. Les données doivent être fournies dans un format qui doit être spécifié, correctement documenté et qui peut être utilisé avec des logiciels habituellement utilisés.
- **Liberté du logiciel** : tous les logiciels indispensables afin de permettre au client de quitter la plateforme et de pouvoir profiter du même service sur une infrastructure personnalisée doivent être sous licence libre.
- **Liberté de la concurrence** : il ne doit pas exister de verrous légaux empêchant des concurrents d'essayer de fournir le même service.

Un service respectant les principes du TIO Libre garantit aux clients qu'ils peuvent changer à tout moment de fournisseur de service, ou bien qu'ils peuvent à tout moment devenir leur propre fournisseur de service.

TIO Loyal [modifier | modifier le code]

Une solution d'externalisation de l'information est considéré comme loyale si le contrat de service contient les éléments suivants :

- **Droit d'accès** : le service doit pouvoir être utilisé par tous, d'où qu'ils soient, sans discrimination.
- **Droit de vie privée** : aucune donnée en relation avec l'usage du service par le client ne peut être fournie à un tiers, que ce soit sous la forme d'un verbatim, ou bien de façon anonyme, sans l'autorisation explicite de ce client donnée au cas par cas par ce dernier.
- **Droit de notification** : le client du service doit être notifié de tous incidents ou changements qui pourraient causer ou avoir causé une faille de sécurité dans le service ou qui changerait le service.
- **Droit de divulgation** : le fournisseur de service doit prendre toutes les mesures nécessaires afin de faire respecter les termes du service par ses employés ou fournisseurs et communiquera ces mesures aux clients sur simple demande.

Le TIO Loyal permet de fournir un cadre afin d'atteindre le même niveau de secret commercial et de la transparence qu'avec son propre personnel.

GTLL Systematic - 2013

abilian

SYSTEMATIC
PARIS REGION SYSTEMS & ICT CLUSTER
LOGICIEL LIBRE

Groupe Thématique Logiciel Libre
Contribution au plan industriel Cloud

20 décembre 2013

Ordre du jour

En 2013, en particulier, les révélations d'Edward Snowden ont remis sur le devant de la scène les questions de souveraineté des données, de protection de la vie privée, et le spectre d'une société orwellienne de surveillance généralisée.

Il va sans dire que les communautés du logiciel libre et open source sont à l'avant-garde de la vigilance sur ces questions, et sont force de proposition comme nous le voyons dans la suite de ce document. Nous reviendrons donc sur ces quatre critères essentiels :

- fiabilité ;

- souveraineté des données (cf. Snowden) ;

- sécurité ;

- portabilité et réversibilité.

Notons enfin le paradoxe suivant : le système américain de surveillance généralisé, PRISM, dénoncé par Snowden, utilise massivement le logiciel libre et aurait même pu en constituer une *success story,* si l'usage n'en avait pas été si détestable.

Point de départ (Open Cloud Manifesto)

- les prestations de cloud doivent être **pensées pour l'utilisateur**, et qu'il doit être le premier à en détenir le contrôle ;
- **l'ouverture des standards**, systèmes et logiciels est une garantie pour l'utilisateur ;
- la **transparence de la gouvernance** est une condition de la confiance et de la fiabilité ;
- **l'interopérabilité** conditionne l'efficacité du cloud en tant que ressource publique ;
- toutes les parties doivent être équitablement représentées dans les **processus de normalisation**, qui doivent être coordonnés et collaboratifs, aussi peu mûr soit le marché ;
- que **l'équilibre** entre l'intérêt du consommateur et l'intérêt mercantile doit être préservé et sinon en faveur du consommateur ;
- enfin que la **sécurité** est essentielle, et non point facultative.

Contexte et objectifs (2013)

Ces principes devront être étudiés, certainement complétés, sous l'angle des questions posées par les différents acteurs, en particulier les utilisateurs, notamment à la lumières des révélations et des débats qui ont eu lieu depuis la rédaction de l'Open Cloud Manifesto :

- refus de la **confiscation des données personnelles et professionnelles** par les opérateurs du Cloud ;
- refus de **l'espionnage et de l'intelligence économique** au profit de puissances ou d'acteurs étrangers ;
- refus de la **société de surveillance généralisée**, de quelque origine qu'elle soit. À noter qu'un bon encadrement des captations administratives de données par l'État serait un avantage compétitif considérable pour les acteurs français du cloud ;
- encouragement à **utiliser les technologies les plus ouvertes et interopérables**, notamment le développement de standards autour du cloud computing (à tous les niveaux : IaaS / PaaS / SaaS).
- encourager la **R&D sur les technologies ouvertes** de cloud distribué, sur l'interopérabilité des clouds, sur la résilience, la sécurité, etc.

Livrables (2013)

Ce travail pourrait aboutir :

- **à une version amendée, complétée, adaptée** à la mentalité et au droit français et européen de l'**Open Cloud Manifesto.** Les opérateurs de cloud devront être fortement incités sinon contraints à s'engager sur ce manifeste.
- à un **label de confiance**, associé à de la certification, qui prenne en compte ces différents principes et les formalise sous une forme vérifiable concrètement. Des normes françaises ou internationales pourront être invoquées, ou développées, dans le cadre du développement de cette certification ;
- à définir une **charte d'interopérabilité** (ou charte de l'open cloud) et d'inscrire des clauses d'interopérabilité dans les commandes et actions de soutien public ;

Dans tous les cas, une communication importante doit remettre au cœur du débat, et en particulier dans l'esprit des acheteurs, les principes que nous évoquons et qui seraient affirmés dans ce manifeste.

OSBA - 3 novembre 2019

abilian

Position récente de l’OSBA sur la souveraineté dans le Cloud (1/2)

1. Dans le cadre de sa stratégie d'informatique dans les nuages, l'État doit mettre l'accent sur les **questions stratégiques** (comme la souveraineté numérique) **plutôt que sur les questions pragmatiques** lors du choix des solutions et des fournisseurs.
2. Les responsables doivent être informés des implications juridiques de la **protection des données** et des **implications stratégiques** d'une décision pour les services dans les nuages.
3. **Les décisions sur les stratégies de cloud computing doivent inclure le savoir-faire sur la technologie open source et les standards ouverts.** Ce savoir-faire devrait être développé en interne ou intégré par l'intermédiaire d'experts de la région.
4. L'État devrait préférer des solutions totalement transparentes et mises en œuvre avec des **interfaces ouvertes**.
5. L'État devrait préférer les fournisseurs et les centres de données qui sont basés sur des approches totalement **transparentes et ouvertes**.

abilian

Position de l’OSBA sur la souveraineté dans le Cloud (2/2)

6. Pour les données critiques et sensibles, l'État devrait s'appuyer exclusivement sur des plates-formes de cloud computing **construites à l'aide de technologies et de standards ouverts et qui permettent de changer facilement de fournisseur**.
7. L'État doit **promouvoir** directement et indirectement le développement de technologies et d'offres appropriées.
8. L'État doit veiller à ce que ses propres données ne soient stockées que dans un environnement répondant aux normes européennes les plus élevées en matière de **protection des données**.
9. En tant que modèle, l'État lui-même doit appliquer des critères stricts lors de la mise en place de solutions de cloud computing tout en conservant son **indépendance vis-à-vis des fournisseurs** individuels.

abilian

CIGREF - 25 novembre 2019

abilian

CIGREF

#SWIPO – Le Cigref et ses adhérents ne peuvent pas reconnaître, à ce stade, la légitimité des documents (codes de conduite, descriptif de la future entité légale de gouvernance de ces codes) qui devraient être remis, le 26 novembre 2019, à Helsinki, aux ministres de la présidence finlandaise du Conseil de l'Union européenne.

Le Cigref fait le constat de l'échec du processus d'autorégulation du marché du cloud en Europe. Cet échec est essentiellement la conséquence d'une **asymétrie systémique de compétences, de moyens et d'objectifs** entre ceux de certains grands fournisseurs mondiaux de services cloud d'une part, qui défendent le cœur de leur activité commerciale et **leur capacité d'enfermement de leurs clients**, et d'autre part ceux des utilisateurs dont le lobbying dans ce domaine n'est pas le métier. Aucune des propositions formulées par les membres du Cigref pour améliorer le code de conduite SaaS et la gouvernance ultérieure des codes de conduite par l'entité légale n'a été prise en compte, au mépris des règles de gouvernance du SWIPO Working Group.

abilian