

Septembre 2017

Les données, de la valeur métier à la conformité GDPR



En bref

S'il est admis dans tous les discours convenus que la Data est au coeur du business, encore faut-il savoir comment mettre en oeuvre ce beau principe. Les témoignages de GRTgaz, GRDF et In Extenso en montre ici des exemples. Enfin, la prochaine application du Règlement Général sur la Protection des Données (RGPD ou GDPR) va grandement modifier les conditions pratiques de cette utilisation de la Data.

Sommaire

Juridique

Bien comprendre et bien intégrer GDPR

Stratégie

Hervé Constant, DSI de GRTgaz : « Il faut donner envie aux métiers de nous utiliser »

Stratégie

Thien Than-Trong (GRDF) : « Nous produisons des données pour favoriser la maîtrise de l'énergie »

Projets

Martin Mathieu (In Extenso) : « la clé du succès d'un RSE, c'est qu'il soit utile »

Bien comprendre et bien intégrer GDPR



Maître Polyanna Bigle, avocate à la cour, a ouvert l'atelier GDPR du 21 juin 2017.

A l'occasion du Security Day, évènement mondial dédié à la cybersécurité organisé par le Groupe IDG le 21 juin 2017, CIO a choisi pour la France le thème du GDPR. Notre publication a ainsi organisé un atelier à l'Hôtel Napoléon à Paris où des experts ont échangé avec les participants DSI.

Le nouveau Règlement européen sur la protection des données personnelles (GDPR ou, en Français, RGPD) impacte fortement les entreprises, leurs DSI, les responsables sécurité, audit, juridique et plusieurs directions métiers, en particulier celles chargées de la relation client. Avant tout, GDPR est une question juridique. Lors de l'atelier organisé le 21 juin 2017 à l'occasion du Security Day du groupe IDG, le sujet a été présenté par Maître Polyanna Bigle, avocate à la cour, Directeur du département sécurité numérique au cabinet Alain Bensoussan.

Pourquoi sommes-nous tous impactés par GDPR (ou RGPD en anglais) ? Parce qu'il va non seulement toucher les organismes établis au sein de l'Union européenne (UE), mais également les entreprises qui travaillent avec des personnes ou avec des entreprises qui sont résidentes ou établies dans l'UE. Si on est dans un pays extérieur, on va tout de même être soumis au droit européen, ce qui montre l'impact du nouveau règlement, souligne d'emblée Maître Polyanna Bigle.

« Aujourd'hui, je veux aborder plus particulièrement dans ce RGPD, la problématique de la sécurité. RGPD ne parle pas que de sécurité, mais son titre est basé sur la sécurité des données, c'est tout un mécanisme de sécurité et de protection ». En introduction, sur ce règlement, qu'est ce qui change ? Ce règlement compte 99 articles, le précédent en comptait 34, et la loi Informatique et libertés 72. Les obligations des 99 articles opèrent un changement important de la législation.

La jurisprudence des autorités de contrôle

Par rapport à la hiérarchie des textes du droit français, ce Règlement va s'appliquer directement dans notre droit sans besoin de transcription dans le droit national, cela à partir du 25 mai 2018. Il faut savoir que le Règlement laisse des portes ouvertes au droit national et au droit des différents pays pour une adaptation. Ensuite, chacun sera soumis à la jurisprudence des autorités de contrôle comme la CNIL en France, et ces autorités de contrôle ont un pouvoir sensiblement accru par rapport à la loi de 1978. Des prémices existent depuis octobre 2016 avec la Loi pour une République numérique.

Les sanctions maintenant. Elles sont passées à trois millions d'euros depuis 2016 (avec cette Loi pour une République numérique), ce qui constitue une augmentation sensible des sanctions. Celles-ci font beaucoup plus peur (« c'est pour ça qu'on est là aujourd'hui » a relevé Polyanna Bigle). Mais il ne faut pas oublier tous les autres sujets : l'impact sur la DSI et les RSSI, les principes directeurs de sécurité, comment se structure la sécurité dans ce raisonnement, enfin la protection by design et la protection par défaut, un point sur la gestion des failles de sécurité qui va nécessiter des processus particuliers.

Pour la DSI et le RSSI, quand on n'a pas assuré une bonne protection des données, avec GDPR / RGPD, on risque jusqu'à 10 millions d'euros ou bien 2% du chiffre d'affaires mondial en amendes, même si les filiales étrangères n'y sont pour rien. On peut se dire « moi je ne risque que 10 millions », car sur d'autres principes de base comme la licéité, la loyauté des traitements des données, les grands principes qu'on doit mettre en oeuvre, on risque le double, 20 millions d'euros ou 4% du chiffre d'affaires. La sécurité est présente dans les deux cas. Et il va falloir démontrer qu'on a respecté les principes de la sécurité. On a donc une forte responsabilité en termes de sécurité, les sanctions sont conséquentes et modulées en fonction de plusieurs critères, on va prendre en compte les mesures de protection, ça va permettre de moduler les sanctions, et tous les efforts qu'on va faire vont moduler les sanctions éventuelles.

La double peine : attaque + inspection

Cela veut dire aussi, que on ne peut pas dire qu'on ne savait pas. On peut avoir mis en oeuvre des mesures pas suffisantes, mais et ça va moduler la sanction, on ne peut pas dire qu'on ne savait pas qu'on doit protéger les données. Ce qui signifie, si on fait l'objet d'une attaque extérieure qu'on va avoir une double peine : on subit une attaque (on ne peut plus travailler, par exemple) et en plus on va avoir le risque d'une sanction parce qu'on a pas suffisamment bien sécurisé ses données, on peut avoir la CNIL ou l'ANSSI chez soi. L'ANSSI va avoir non pas un pouvoir de sanction mais de plus en plus d'agents de terrain pour voir comment ça se passe et contrôler si les mesures de sécurité ont bien été mises en place. Sur le site de l'ANSSI, il y a une explication sur l'attaque contre TV 5 Monde et comment l'ANSSI l'a aidé à se retourner après l'attaque dont la chaîne a été victime.

La sécurité des données est au coeur des préoccupations. Il faut en effet savoir que le Règlement demande de mettre en place une sécurité « appropriée ». Appropriée, c'est-à-dire qu'il faut que les mesures soient constamment adaptées et évoluent en fonction de l'état de l'art et des menaces. On doit se remettre en cause tout le temps. La sécurité pourquoi faire ? Eviter qu'il y ait une utilisation de données illicites, c'est aussi une gestion des accès non autorisés. Cela peut impliquer le besoin de cloisonner les données : par exemple, tout le monde ne doit pas avoir accès aux données de la comptabilité. Enfin, il faut aussi évidemment se protéger contre la perte ou la destruction de données accidentelles. Il est intéressant de noter qu'assurer la protection des données, c'est avant tout préserver l'intégrité et la confidentialité des

données.

L'importance de l'intégrité des données

On doit donc s'assurer que les données à caractère personnel des individus n'ont pas été modifiées (et ne le seront pas) et qu'elles se sont pas divulguées à n'importe qui. Ce qui est nouveau avec le nouveau Règlement, c'est qu'en plus, il va falloir démontrer que l'on a respecté ces obligations. Il ne suffit pas de mettre en place des mesures, il faut démontrer leur efficacité. Il faut donc revoir sa PSSI, bien documenter toutes les mesures que l'on prend, tracer ses actions. De bonnes pratiques du DSI et du RSSI, l'entreprise va devoir basculer à un travail commun entre la DSI et les services juridiques. N'oubliez pas qu'en cas de contrôle CNIL, c'est chez vous, DSI et RSSI, qu'on va venir pour voir s'il y a bien eu toutes les mesures appropriées prises.

La mesure générale d'analyse de la sécurité se présente ainsi : bien réalisée, à jour, qui soit bien appliquée et qui doit inclure un chapitre sur la protection des données à caractère personnel. Ensuite, il y a comme composante de la protection des données la sécurité dès la conception, qui est une composante et la sécurité par défaut, et la sécurité stricto sensu qui fait l'objet d'un chapitre avec l'article 32. On retrouve la sécurité un peu partout dans le nouveau Règlement. « Je me suis amusé à compter, on a un peu plus de 55 fois le mot *sécurité* dans le règlement. C'est dire l'importance de ce terme » a pointé Polyanna Bigle.

La sécurité stricto sensu va s'appliquer et c'est très nouveau, au responsable de traitement, celui qui va traiter, utiliser des données à caractère personnel mais aussi les sous-traitants donc l'ensemble de ceux de ces prestataires qui ont vocation à toucher, transmettre et héberger les données à caractère personnel. Le sous-traitant lui-même est soumis à des exigences, il faut prévoir un cadre contractuel entre l'entreprise et ses sous-traitants.

Une obligation de moyens pour la sécurité des données

Concernant la structure de la sécurité des données, il est intéressant de noter le principe d'une obligation de moyens. Chacun doit mettre en place les mesures appropriées en fonction de l'intérêt général, de l'état de l'art. Si celui-ci prévoit un niveau élevé de sécurité, on peut se contenter de s'y conformer. Sinon, on se doit d'en faire plus. On a aussi le droit de moduler en fonction du coût. Polyanna Bigle a avancé : « je pense aux PME et TPE, qui sont aussi bien sûr soumises au règlement, ainsi qu'aux sous-traitants. »

On module aussi la sécurité en fonction du type de traitement, c'est-à-dire quel type de données. Il peut y avoir : des traitements RH, clients... Il faut regarder la nature du traitement, la portée et le contexte de celui-ci. On va faire la mesure des risques, leur probabilité, les atteintes possibles aux droits des personnes physiques. La règle est de faire en sorte de préserver les droits et les libertés des personnes privées. Pour les sous-traitants, le chiffrement des données, la résilience constante des systèmes, un PCA un PRA bien à jours et des mesures de sécurité sont nécessaires pour les données sensibles. Il faut aussi faire des mises à jour régulières.

Et enfin, on doit prouver sa sécurité. Le Règlement prévoit aussi qu'on peut mettre en place un code de conduite et se faire certifier. Un mécanisme plutôt côté prestataires : ceux-ci seront, une fois certifiés, supposés conformes au Règlement.

Un prérequis sera aussi l'analyse d'impact. Avant de mener une analyse d'impact, il faut d'abord savoir de quelles données on dispose et ensuite quels sont les impacts possibles d'incidents. Il ne s'agit pas d'avoir un niveau de sécurité très élevé pour tout car on peut l'adapter et choisir le bon niveau de sécurité suivant les sujets à traiter.

Protection by design ou par défaut

Un sujet à ne pas négliger est celui de la protection by design et de la protection par défaut. La protection by design, c'est la protection physique dès que l'on met en place un fichier de données, dès l'origine, et tout au long de l'utilisation de ces données. La protection par défaut, c'est le devoir d'assurer de manière systématique avec une obligation de garantie (y compris avec mes sous-traitants) ces données ne sont accessibles qu'avec les personnes qui disposent des accès et des habilitations. En pratique, on doit donc mettre en place des mesures organisationnelles.

Dernier point, quand on fait l'objet d'une difficulté, ce sera une obligation pour tous de déclarer une faille de sécurité auprès de l'Autorité de contrôle qu'est la CNIL. Les prestataires de services de confiance et des OIV ont un délai très court, 72 heures après la découverte de la faille, pour travailler avec les intervenants. « Je vous invite à prévoir en amont la mise en place d'une cellule de crise pour savoir avec qui vont travailler le RSSI et le DSI : la DG, la communication pour savoir s'il faut communiquer ou pas, et en fonction des problèmes rencontrés leur dire si elles font l'objet d'une faille de sécurité » a recommandé Polyanna Bigle.

Cinq conseils ont été donnés en conclusion : faire une analyse de risque et d'impact, réviser ses politiques de sécurité en conséquence, prévoir une politique de gestion des failles de sécurité, auditer ses sous-traitants en fonction de leurs projets de mise en conformité RGPD, adopter un code Informatique et Libertés. Il ne faut pas oublier enfin, que ce sont les droits des personnes qu'on doit protéger, pas le SI. C'est bien parce que des personnes vous ont donné des données qu'on doit les protéger.

Didier Barathon
Journaliste

Hervé Constant, DSI de GRTgaz : « Il faut donner envie aux métiers de nous utiliser »



(c) Alexia Perchant

Pour Hervé Constant, DSI de GRTgaz, les usages sont la clé de tout.

Devenu DSI de GRTgaz en 2011, Hervé Constant a terminé la séparation informatique avec Engie. Il a lancé un grand projet pour les utilisateurs, et en prépare d'autres sur le cloud et l'innovation.

***CIO* : Vous êtes un DSI atypique, vous ne venez pas de l'informatique, pour commencer quelques mots sur votre parcours ?**

Hervé Constant : J'ai effectué l'ensemble de ma carrière dans le secteur du gaz mais je ne suis DSI de GRTgaz que depuis 2011. Je suis passé par différents métiers. Au début, le terrain, celui de la distribution, en manageant des équipes de maintenance et d'exploitation du réseau. J'ai adoré la partie RH dans cette première fonction. Une deuxième vie m'a mené à une fonction achats très particulière pendant six à sept ans, j'ai travaillé à l'international pour négocier des approvisionnements en gaz puis en gérer les RH. Troisième étape, l'IT, un domaine à l'époque inconnu pour moi, assez complexe et « jargonnant » de premier abord. Mais le digital et l'IT sont une composante assez impressionnante de la transformation des entreprises.

***CIO* : C'est vous qui avez demandé, ou on vous a proposé ce poste de DSI ?**

Hervé Constant : En fait, on m'a proposé un poste de management. J'ai un profil de manager, c'est comme ça que je suis arrivé à la DSI. Ce qui m'a toujours intéressé dans mon parcours, c'est le changement, et j'aime voir les résultats de mes actions sur les choses « dures », celles qui sont quantifiables, ou « molles », celles qui tiennent à la matière humaine.



CIO : Quel type de DSI êtes-vous, en dehors de votre parcours, de quoi êtes-vous porteur ?

Hervé Constant : Nous devons réfléchir aux technologies, mais pas que... Le côté social, au sens large, de mon poste est essentiel, pour savoir comment transformer, « désiloter », « déverticaliser » l'entreprise par l'IT. Je crois qu'un SI ne peut pas se construire en solitaire, qu'on ne peut faire un SI de qualité qu'en étant dans l'interaction et l'empathie avec les métiers. Et en gardant comme impératif : les usages. Nous nous mettons à la place de l'utilisateur en permanence, en embarquant le management. De plus, le monde de l'informatique est un écosystème ouvert sur le monde et en perpétuel mouvement. L'IT peut donc apporter cet état d'esprit à l'entreprise. Il faut que nos métiers profitent de nous, qu'on partage avec eux.



CIO : Quand on pense à GRTgaz, on pense d'abord à la séparation informatique avec votre maison mère, est-elle effective ?

Hervé Constant : Oui, définitivement. Une première séparation informatique eu lieu en 2008 avec EDF, une deuxième avec GDF Suez, devenu Engie, en 2011. Cette deuxième phase est totalement achevée, elle a pris trois ans pour se terminer fin 2014. L'autre grand changement qui a marqué la DSI de GRTgaz a été le passage à Office 365 qui a permis d'externaliser les services de messagerie de l'entreprise. Les utilisateurs en sont très satisfaits, la DSI aussi.

CIO : Deuxième grand sujet, votre projet de nouvelle organisation MoveIT. Quelles sont les caractéristiques ?

Hervé Constant : Nous avons désormais une organisation bimodale. D'un côté, les quatre domaines classiques d'une DSI (le front office de la relation Métiers et utilisateur, les projets, la partie exploitation / production et l'architecture d'entreprise), de l'autre les

activités digitales. L'idée est que le digital accompagne la transformation et que les usages sont la clé de tout. Quand je suis arrivé dans l'IT, j'ai dit aux équipes « on ne construit pas un produit, on répond aux usages ». Notre seul juge de paix c'est : est-ce utile ?

Aujourd'hui, la révolution qui se profile chez nos salariés, c'est celle des services et des usages. Elle touche nos 4 500 utilisateurs, dont plus de la moitié en mobilité.

Comment se traduit cette révolution ? On implique de plus en plus les utilisateurs dans la construction des outils et dans le choix des matériels qu'ils utilisent. Ils ont le choix de leur matériel dans un catalogue, alors qu'auparavant tous les utilisateurs d'un même profil recevaient le même matériel. Comme ils sont davantage impliqués, les utilisateurs sont plus attentifs à leur matériel, celui-ci est adapté à leurs usages quotidiens, ils sont plus responsables, il y a moins de réparations. Et il a fallu changer aussi notre façon d'acheter : finie la massification des achats directement auprès des constructeurs, mais des achats plus agiles via un distributeur. C'est 20 à 25% d'économies au final sur le TCO du poste. Nous utilisons le modèle économique du Cigref pour piloter et benchmarker nos coûts.



CIO : Cloud public, privé, hybride, où en êtes-vous sur ce sujet ?

Hervé Constant : Nous avons une forte réflexion sur notre transformation vers le cloud public. Les questions ne manquent pas : on y met quoi, on y va comment, est-ce qu'on déplace une partie de notre SI, une partie d'applications critiques ou pas ? Nous avons adopté une démarche particulière. Pendant six mois, d'octobre à mars, nous sommes sortis de l'entreprise pour rencontrer les acteurs du marché, les experts, les offreurs de solutions ou encore nos pairs. De quoi se forger une opinion globale.

Début mars, nous sommes entrés en séminaire avec des représentants des différents métiers de la DSI. Nous allons faire nos choix stratégiques d'ici à l'été avec un certain nombre de critères déjà définis pour les fournisseurs potentiels comme principalement la réversibilité et la sécurité. Mais nous ne sommes pas entrés sur ce sujet uniquement via le prisme de la réduction des coûts: le sujet c'est avant tout d'obtenir la meilleure qualité globale - disponibilité, time to market... Nous ne sommes pas non plus partis de zéro, nous avons plusieurs services en SaaS, Office 365 dont j'ai déjà parlé, d'autres pour les achats, les RH, la finance, et même, c'est propre à notre métier, les données météo !

CIO : Comment abordez-vous l'innovation ?

Hervé Constant : Nous travaillons sur plusieurs idées. Par exemple, une pour nos chefs de secteur, les exploitants du réseau. Au cours d'une journée, ils doivent gérer de nombreuses tâches dans différentes applications. Notre promesse de valeur a consisté à mettre en oeuvre avec eux un portail consolidant ces tâches. Les drones sont

Thien Than-Trong (GRDF) : « Nous produisons des données pour favoriser la maîtrise de l'énergie »



De gauche à droite : Thien Than-Trong (DSI) et Isabelle Drochon (Responsable du Programme Données) présentent les évolutions en cours du SI de GRDF.

Au sein de GRDF (Gaz Réseau Distribution France), Thien Than-Trong (DSI), appuyé par Isabelle Drochon (Responsable du Programme Données) pour la partie données externes, est à la tête d'un SI qui va être bouleversé par une forte digitalisation de l'activité et l'arrivée des compteurs communicants Gazpar. Les données produites par Gazpar, comme d'autres, sont avant tout destinées à devenir une matière première qui n'aura de valeur qu'après un traitement par d'autres acteurs.

CIO : Officiellement créé le 31 décembre 2007, dans le cadre de l'ouverture à la concurrence des marchés de l'énergie, GRDF est finalement une entreprise jeune. Comment est constitué son SI ?

Thien Than-Trong : Notre création est récente c'est vrai mais nous avons encore de nombreux liens, historiques et fonctionnels, en particulier avec Enedis (ex-ERDF) en charge de la distribution de l'électricité. Il faut comprendre, pour commencer, que GRDF a la gestion des réseaux de distribution de gaz qui appartiennent aux collectivités ou à des syndicats intercommunaux. En tant que principal opérateur du réseau de distribution de gaz naturel en France, nous sommes présents dans 9 541 communes et 77 % de la population habite une collectivité desservie en gaz par GRDF. Par ailleurs, existent également 22 ELD [Entreprises Locales de Distribution] qui exploitent certains réseaux locaux tels que ceux de Grenoble, Strasbourg ou Bordeaux.

Le réseau que nous exploitons, le plus long d'Europe, mesure 198 886 km et permet de
Les données, de la valeur métier à la conformité GDPR

faire transiter et de distribuer le gaz naturel jusqu'au consommateur final, et ce, pour le compte des fournisseurs dont le rôle est de commercialiser cette énergie. Depuis quelques années, avec la multiplication du nombre de sites de production de biométhane (le biométhane est un gaz 100% renouvelable produit localement à partir de déchets et du recyclage de décharges, sources agricoles, etc.) ce réseau évolue et notre rôle de distributeur également.

La sécurité demeure le socle de l'activité de GRDF. En plus des actions « classiques » de raccordement ou de relève des indices, nos salariés sont notamment en charge du service Urgence Sécurité Gaz (mobilisable 24/24h et 7/7jours) et doivent également gérer ce que nous appelons les dommages aux ouvrages (typiquement : un coup de pelleuse dans une conduite) qui sont en baisse constante depuis 2010 et pour lequel nous avons un objectif qui est de descendre sous la barre des 2 600 dommages aux ouvrages d'ici à 2018 (2 980 en 2016).

De fait, notre SI témoigne de cette double dimension : jeune et avec une histoire ancienne. D'un côté, il y a donc un SI de gestion visant à faire fonctionner l'entreprise, avec ses missions, ses clients, ses partenaires. De l'autre, il y a un SI nettement plus ancien, construit pour les activités « de terrain », et qui est encore pour une bonne part partagé avec Enedis (ex-ERDF) au travers des services communs d'intervention sur le terrain, avec beaucoup de développements spécifiques. Ce dernier SI, baptisé « Disco » [DIStributeur COmmercialisateur], est géré directement par nos services communs, à l'inverse du SI propre, placé sous ma responsabilité. Ainsi, nous transmettons les données de consommation des utilisateurs aux fournisseurs de gaz afin qu'ils puissent facturer leurs clients. Cette facturation comprend une partie « acheminement » fixée de manière réglementaire qui correspond à nos missions de service public. Et bien entendu, il y a de nombreux flux entrées/sorties entre les deux parties de notre SI.

CIO : Quelle est l'architecture de ce SI propre ?

Thien Than-Trong : En coeur, nous avons SAP sur plate-forme Linux avec des bases Oracle. A cela s'ajoutent des développements pour des portails d'interactions avec nos clients et partenaires. Nous avons également recréé dans ce SI spécifique des outils pour gérer l'urgence gaz. Bien entendu, nous nous autorisons des technologies de type Hadoop/Spark pour améliorer le traitement des Big Datas, notamment issues de l'IoT. Nous n'avons pas de datacenters propres mais un hébergement privé. Nous ne recourons pas au cloud public. Au sein de notre hébergement, nous disposons de serveurs classiques pour les bases centrales et de cloud privé lorsque la scalabilité est nécessaire, par exemple pour les frontaux. Nous achetons de la ressource « as a service » sur des baies réservées mais le matériel ne nous appartient pas.



(c) Alexia Perchant

CIO : Que signifie la digitalisation pour vous ?

Thien Than-Trong : Avec l'arrivée des compteurs communicants gaz, l'activité de relève - prise en charge dans le cadre du service commun - va nécessairement diminuer. Ce changement technologique va donc entraîner une évolution de l'organisation des activités d'intervention sur le terrain. Ainsi nous dotons les agents de terrain de tablettes qui sont équipées de logiciels exploitant les données de Disco et d'autres outils métier spécifiques et de la GMAO issue du « jeune GRDF ». Il s'agit notamment d'optimiser les tournées en temps réel. Nous mettons en valeur nos « deux SI » via le Digital.

Isabelle Drochon : En fait, la télé-relève existe déjà depuis cinq ans (déploiement entre 2010 et 2012) pour les clients dits « gros consommateurs » : essentiellement des industriels et des activités tertiaires multi-sites. Ceux-ci représentent 50 % de la quantité de gaz naturel distribué mais seulement 100 000 clients. Pour l'autre moitié des volumes distribués, la digitalisation de la collecte des 11 millions de clients de GRDF passe par le compteur communicant Gazpar. La quantité de données traitée par notre SI va donc être multipliée par 180 puisque nous passerons d'un relevé actuellement semestriel à un relevé quotidien.

Après une phase de test dans 4 zones pilotes démarrés début 2016, le déploiement généralisé du compteur Gazpar commence le 1er Mai 2017 avec une fin prévue en 2022. A ce jour, plus de 150 000 compteurs communicants ont déjà été posés et notre objectif est de 600 000 compteurs installés d'ici la fin de l'année. Une fois le système mis en place, les fournisseurs de gaz recevront une transmission des données de facturation mensuellement.

CIO : Comment vont être exploitées les données de Gazpar ?

Isabelle Drochon : Le client particulier pourra avoir accès aux données brutes de son compteur dans un espace personnalisé et sécurisé sur GRDF.fr. Il y trouvera des chiffres exprimés en kWh et pourra également choisir quel tiers sera autorisé à accéder à ses données. De fait, ces données ne seront pas partagées avec n'importe qui car l'enjeu de confidentialité est évident : personne ne souhaite faire savoir quand il part en vacances et cesse de consommer de l'énergie par exemple.

Pour le suivi des consommations quotidiennes, étant donné que le compteur émet deux fois par jour, la finesse des données émises n'autorise pas, par exemple, à savoir à quelle heure les particuliers se lèvent ou se couchent. Toutefois, pour les clients qui le souhaitent, nous proposons, dans le cadre d'une tarification complémentaire spécifique, un service de remontée de données horaires. Une remontée en temps réel est aussi techniquement possible mais cela suppose d'acquérir un module externe et de le maintenir, ce qui ne rend cette offre attractive que pour les gros consommateurs.

Le programme compteurs communicants de GRDF représente un investissement d'un milliard d'euros. Par la meilleure connaissance de la consommation qu'il rendra possible, nous estimons qu'il permettra une économie moyenne d'énergie de 1,5% sur l'ensemble du territoire. Il va de soi que nous voulons que les données générées soient donc les plus utilisées possible. Cette utilisation pourra se faire via des plates-formes à destination des grands bailleurs, des collectivités, des start-up, etc. Nous envisageons qu'à terme, les données du gaz y soient associées à d'autres données, par exemple pour estimer le coût énergétique global d'un logement ou un cumul de charges locatives. Sur ce sujet, nous travaillons aussi en coordination avec les ELD qui sont intéressées par ces solutions qui tendent toutes à favoriser les actions de maîtrise de l'énergie.

Thien Than-Trong : Nous avons lancé un grand programme d'API management qui aboutira en 2018. Les données de Gazpar vont être injectées dans notre SI et, via les API, être mises à disposition sur notre portail propre mais aussi pour nos partenaires et pour les fournisseurs de gaz. Nous menons actuellement un vaste chantier de normalisation des processus autour du traitement de ces données.

Nous produisons des données destinées essentiellement à être valorisées par d'autres. En tant que service public, il en va de notre responsabilité de délivrer cette brique à ceux qui pourront en tirer une valeur d'usage.

Isabelle Drochon : Notre rôle n'est pas de construire un business autour de ces données mais de les rendre accessibles dans le respect de la réglementation en vigueur.



***CIO* : Techniquement, comment les données sont-elles remontées alors que vous ne pouvez pas les transmettre en utilisant votre propre réseau comme vos confrères de l'électricité ?**

Isabelle Drochon : La technologie Gazpar utilise une fréquence ouverte proche de la bande FM - le 169 MHz - qui sert aux compteurs d'eau, de gaz, etc. Le compteur comporte une pile capable de durer vingt ans car il ne se « réveille » que quelques fractions de secondes par jour. Les données de chaque compteur sont ensuite transmises vers des concentrateurs installés sur des points hauts. Chaque concentrateur couvre un rayon de deux kilomètres environ.

Si nous détectons une anomalie (comme une absence de remontée de données par exemple), des contrôles sont faits à distance, et si nécessaire, un agent de terrain est envoyé pour changer le compteur.

Thien Than-Trong : A partir des concentrateurs, nous remontons ensuite les données en GSM. Ce choix technique est approprié car il y a peu de données et une remontée lente suffit. Nous avons d'ailleurs constitué une alliance ouverte, nommée Wize Alliance, avec Suez (pour les compteurs d'eau) et Sagemcom pour promouvoir cette technologie - notamment pour l'IoT- et à ce jour plus de 35 sociétés en Europe nous ont déjà rejoints.

***CIO* : Plus concrètement, quelle valeur vos partenaires vont-ils pouvoir tirer des données de Gazpar ?**

Isabelle Drochon : Cela dépend des acteurs. Les premiers intéressés sont les

collectivités locales pour travailler sur la planification énergétique des territoires, prévoir l'évolution des réseaux tout en sécurisant la fourniture d'énergie selon les anticipations de besoins à des échéances de 20, 30 voire 50 ans. Nous pouvons de fait basculer d'une analyse nationale ou régionale à une analyse locale.

Pour les grands bailleurs, il s'agit de travailler à l'efficacité énergétique de leurs bâtiments, pour piloter une politique de rénovation et d'isolation. Des grands cabinets de gestion pourraient, à terme, proposer des plates-formes de services où les consommations énergétiques trouveraient leur place, comme les carnets numériques d'entretien des immeubles par exemple.

Et puis, il y a de nouveaux acteurs offrant des services autour de la donnée. Par exemple, on peut réaliser du pilotage domotique dans une logique de smart-home avec du machine learning pour caler le chauffage aux besoins réels. Certains comparateurs de prix entre fournisseurs pourraient ainsi se caler sur les consommations réelles. Certains acteurs travaillent aussi sur des coffres-forts numériques rassemblant des données d'origines variées comme les données bancaires, celles de l'énergie, etc. Nous sommes convaincus qu'un secteur d'activité innovant fondé sur les actions de maîtrise de l'énergie peut émerger demain grâce aux données, et ce, au profit de tous.

CIO : Adoptez-vous une démarche d'open-data ?

Isabelle Drochon : Tout à fait ! La remise des données sera gratuite mais, les données étant sensibles, l'accès ne sera pas libre.

Début 2018, les entreprises intéressées pourront souscrire au service GRDF-ADICT (Accès aux Données Individuelles des Clients par des Tiers). Un contrat précis, avec les droits et obligations de chaque partie, sera alors conclu. Pour un recueil des données détaillées, il faudra un consentement explicite des personnes concernées.

Deux cas de figure sont prévus. Dans le premier, c'est le tiers qui recueille le consentement des personnes et GRDF le valide positivement par défaut pour lui ouvrir les droits d'accès, avec des contrôles opérés par GRDF et un strict respect des règles définies par la CNIL. Dans le second, le consentement est géré par GRDF, recueilli lorsque le client se connecte à son compte, sur le modèle de l'utilisation des données Facebook par des applications tierces. Si le deuxième circuit est 100% digital, il n'est pas nécessairement le plus pertinent dans tous les cas. Le premier circuit serait plutôt destiné aux gros acteurs, gérants de nombreux compteurs, le deuxième est, selon nous, davantage adapté aux start-up. Nous travaillons à ce sujet avec les associations de consommateurs pour vérifier que le process est clair et sécurisant. Nous avons ainsi prévu une fonction « listing des consentements accordés » sur le portail de GRDF avec une capacité de révocation en ligne.

Thien Than-Trong : Comme nous démarrons une phase expérimentale avec quatorze partenaires, la gestion des API et des ouvertures de droits est encore très manuelle. Pour l'instant, les fournisseurs de gaz utilisent une connexion « canal historique » avec notre SI mais ils pourront ensuite basculer en mode « GRDF-ADICT » s'ils le souhaitent.



CIO : Nous avons parlé des données individuelles. Allez-vous distribuer également des données agrégées et, ainsi, davantage ouvertes ?

Isabelle Drochon : La Loi prévoit en effet que des données agrégées par quartier puissent être mises à disposition librement. Nous avons, à cette fin, ouvert un portail utilisant la solution d'OpenDataSoft en décembre 2016. Les données de production de biométhane ou d'acheminement du gaz y sont régulièrement téléchargées. Nous sommes encore dans une phase d'apprentissage car beaucoup de questions demeurent sur le seuil minimal d'agrégation garantissant l'anonymat. Nous sommes prudents sur l'ouverture des données afin de ne pas diffuser de données potentiellement sensibles.

CIO : Mis à part Gazpar, avez-vous d'autres dispositifs IoT, par exemple pour surveiller le réseau ?

Thien Than-Trong : En effet, mais ce sont plutôt des données internes. Nous travaillons sur un dé-silotage et sur la qualité des données. Nous menons un très gros travail sur l'exploitation de telles données avec une logique de démonstrateurs. Chaque test nous permet d'apprendre et de vérifier la pertinence de la démarche. Si l'intérêt est manifeste, nous industrialisons. Nous faisons un gros travail, pour répandre la culture de la donnée dans l'entreprise.

L'IoT transforme l'approche de la maintenance de nos installations. Actuellement, nous avons des obligations très réglementées en matière de maintenance. Mais nous avons une vraie opportunité d'optimisation pour entretenir l'infrastructure de distribution en réalisant de la maintenance préventive.

CIO : Si on excepte le point précis des plus gros volumes de données, en quoi les chantiers en cours impactent-ils réellement le coeur du système d'information ?

Isabelle Drochon : Aujourd'hui, on nous demande des informations dont nous ne disposions pas auparavant. Par exemple, on nous demande la consommation par secteur d'activité. Or, pour nous, que le consommateur soit un hôpital ou une usine, cela nous est indifférent en matière de distribution au sens strict. La donnée n'existait donc pas dans nos systèmes. Il a fallu trouver un moyen de l'insérer.

Le réseau de distribution dont nous avons la gestion évolue aussi. Par exemple, il nous faut intégrer le décompte des injections de biométhane. Enfin, nous nous préparons à la mutation de nos métiers et à leur digitalisation.

Martin Mathieu (In Extenso) : « la clé du succès d'un RSE, c'est qu'il soit utile »



© B.L. / CIO France

Martin Mathieu, directeur associé chez In Extenso (réseau Deloitte), a fait de l'intranet collaboratif une colonne vertébrale de la communication interne.

Le réseau d'experts comptables In Extenso (groupe Deloitte) a déployé successivement plusieurs outils d'intranet et de réseaux sociaux d'entreprise pour en faire la colonne vertébrale de la communication interne. L'unification des outils va aboutir avec Elium, le nouveau nom de Knowledge Plaza.

« Le client fait son métier, nous faisons le reste » est le credo du réseau d'experts-comptables In Extenso créé en 1991 à l'initiative de Deloitte et d'experts-comptables indépendants. La structure du groupe est très fédérale : chaque cabinet local est détenu à 49 % par un ou plusieurs experts-comptables et à 51 % par la holding de tête qui, de son côté, est détenue d'une part par Deloitte, d'autre part par les experts-comptables du réseau. La holding de tête détient également des parts de filiales telles que In Extenso Avocats. Les 230 associés sont appuyés en tout par 4700 collaborateurs et seulement 80 sont présents au siège, dont la moitié à la DSI. Car, si In Extenso est plus un réseau de PME qu'une seule organisation, son système d'information est unique et sa gestion harmonisée. Le groupement avait donc besoin d'outils de communication interne efficaces.

« Nous avons un même intranet, de même outils de communication, une même gestion interne, une même paye... » confirme Martin Mathieu, directeur associé chez In Extenso notamment en charge de l'IT, du marketing et de l'animation du réseau. Il complète : « l'intranet nous assure un accès à toute la documentation interne afin que nous ayons les mêmes procédures, avec les mêmes outils et les mêmes méthodes dans tout le réseau. »

Une nécessité d'harmonisation

Par exemple, si un réseau de franchise est client d'In Extenso et qu'un associé fait une proposition commerciale à un franchisé, il doit tenir compte des autres propositions faites aux autres franchisés du même réseau, le cas échéant avec des conditions commerciales négociées entre les deux réseaux (franchiseur et In Extenso). Si le franchiseur ne peut pas s'intéresser à la gestion quotidienne de ses franchisés, il peut exiger des tableaux de gestion formatés. L'associé In Extenso doit disposer de ces demandes pour effectuer son travail. Enfin, il peut être pertinent pour les franchisés de disposer d'un extranet leur permettant de disposer de chiffres remontés automatiquement des systèmes financiers (avec anonymisation) pour se benchmarker par rapport aux autres. « Autant le franchiseur et chaque franchisé que l'associé In Extenso tirent profit de cette approche » souligne Martin Mathieu.

Cette indispensable circulation d'information a nécessité très tôt la création d'un intranet, baptisé Nexty, au début des années 2000. Le premier outil choisi a été Advantys, depuis racheté par Hoozin. Ce produit est orienté workflow. Il ne permettait pas la création d'un portail client dont la nécessité était pourtant déjà perçue. Martin Mathieu explique : « nous avons voulu commencer par l'interne pour habituer les collaborateurs. »

D'abord du Top-Down

Au départ, l'intranet avait un fonctionnement plutôt Top-Down pour diffuser de l'information interne, des liens vers des bases de connaissances et gérer des processus internes (par exemple : une demande de formation). L'outil était, à l'époque, très innovant. Et structurant. « C'était un facteur de séduction pour les cabinets voulant adhérer au réseau In Extenso » relève Martin Mathieu. Mais l'intranet n'était pas collaboratif à cette époque. Il était donc difficile d'y trouver une vraie valeur ajoutée même si sa force était la facilité d'alimenter en document. Au final, l'intranet a donc bien été utilisé.

En 2010, le réseau décide de mettre en oeuvre Microsoft Sharepoint pour son collaboratif interne, simplement parce qu'il en disposait déjà pour son site web. Mais cette technologie permet juste le partage documentaire, pas le collaboratif temps réel. Hoozin, qui a repris Advantice, est donc utilisé à cette fin. Mais In Extenso souhaitait un outil polyvalent. Martin Mathieu constate : « il faut que les collaborateurs aient besoin de l'outil pour que ça marche et qu'ils l'utilisent. »

Une approche progressive

Fin 2014, par une veille sur les produits disponibles, Knowledge Plaza (devenu depuis Elium) est repéré pour son mode SaaS. La signature du contrat sera finalement réalisée en 2016. « Outre un tarif correct, une bonne fiabilité, l'outil est souple, simple d'installation avec la possibilité de travailler en commun et de gérer un mode mur (comme Facebook) sans oublier un moteur de recherche efficace » se souvient Martin Mathieu. Le coût global du projet à ce jour est qualifié de très raisonnable, de l'ordre de 120 000 euros en cumulant les abonnements par utilisateur, le coût interne et les 25 jours de consultants. Il ajoute : « un élément qui a beaucoup joué est que la démonstration a été effectuée par une documentaliste avec des cours sur la gestion de documents. »

Dans un premier temps, seul Sharepoint est fermé. Plusieurs espaces sont ouverts dans Knowledge Plaza (aujourd'hui : Elium). Par exemple, l'équipe qui met en oeuvre le portail client travaille dans l'un avec les équipes régionales de déploiement. Une communauté des spécialistes du domaine social, habituée à Advantys, y déplace les discussions de ses 950 adhérents. « Nous avons fermé d'un côté et ouvert de l'autre

pour tester une telle bascule » indique Martin Mathieu. L'adoption est bonne, simplement parce que l'outil répond aux besoins. Les communautés peuvent être plus ou moins fermées : secrètes (réservées aux membres), publiques (pour tous les collaborateurs) ou entre deux (lecture publique mais écriture sur autorisation).

Disparition de l'e-mail

Les communautés se multiplient progressivement et, en leurs seins, les e-mails disparaissent. Le suivi d'actualité type Facebook avec notifications facilite cette évolution. Même en cours de réunions à distance, il est possible de corriger collaborativement des documents. Si l'outil pourrait être installé en interne, In Extenso a préféré le SaaS car la phase d'expérimentation n'est pas terminée et qu'ainsi l'accès ubiquitaire est garanti. La SSO est gérée par la DSI en dehors de l'outil.

Les usages propres d'In extenso ont poussé à des évolutions de Elium (ex-Knowledge Plaza) vers un meilleur support des fonctions d'intranet. Une nouvelle version va ainsi permettre d'y gérer des formulaires. Quelques outils procéduraux font l'objet de développements spécifiques. Mais Elium va devenir la page d'accueil et l'outil unique de l'intranet du réseau.

Bertrand Lemaire
Rédacteur en chef de CIO

Pour toute demande concernant CIO.focus :

contact-cio@it-news-info.com

Une publication de IT NEWS INFO : 40 bd Henri Sellier 92150 Suresnes

Rédacteur en chef : Bertrand Lemaire, blemaire@it-news-info.com

Tél. : 01 41 97 62 10

Principaux associés : Adthink Media et International Data Group Inc.

Président : Bertrand Gros

Directeur de publication : Bertrand Gros

Directeur général : Jean Royné

Président du groupe Adthink Media : Sylvain Morel

CIO est édité par IT NEWS INFO, SAS au capital de 3000000 €

Siret : 500034574 00029 RCS Nanterre

