efcse.eu

DONNEE PERSONNELLE, GOUVERNANCE ET MODELE ECONOMIQUE

Auteur : Laurent CAREDDA, Président EFCSE.
Extrait de Table ronde du 10 avril 2019 organisée par la Chaire Économie Numérique de la Fondation Dauphine, avec be-ys Group, sur le thème de la gouvernance des données personnelles

11 avril 2019

Mandataire juridique et modèle économique

Rappelons que la gouvernance de l'information est un élément d'accélération économique majeur dont le point de départ est la protection des données personnelles et des données économiquement sensibles.

Sur le principe d'un « accord » entre des parties dont les objectifs sont différents, un service digne de ce nom se doit de garantir à chaque partie prenante le bon contexte de collecte d'informations, l'usage qui sera fait de ces informations, dans quelles conditions elles seront échangées, où et comment elles seront stockées, combien de temps, qui pourra y avoir accès et comment. S'assurer de la bonne exécution de cet accord, de la valorisation de la sécurité juridique et de la sécurisation de toute transaction, se doit d'être géré par un acteur de confiance en position de neutralité par rapport aux parties associées à cet accord. Dans un tel schéma, l'identification sans faille de chaque acteur est essentielle, notons que l'identité numérique est un maillon fondamental de cet univers de confiance.

Dans ce contexte, le « mandataire numérique » est l'acteur de confiance par excellence, il est peut-être un des catalyseurs de la construction d'espaces économiques purement européens et de nouveaux modèles complètement différents de l'existant (ceux des GAFAM et autres BATX …). Derrière le mandataire, il y a la valeur juridique bien évidemment, mais aussi être au service de, agir pour le compte de, probablement dans des modèles économiques qui sont au service de cet engagement, cela devient un acte technique et rien d'autre.

C'est un axe qui semble intéressant, porteur et dans lequel nous allons voir émerger beaucoup d'initiatives, il y en a déjà quelques-unes, notamment avec tous ceux qui essaient de se positionner sur l'identité numérique. Cependant, les modèles économiques sous-jacents ne sont pas au service de l'engagement mais au service d'une dime commerciale, souvent d'une maitrise et sur le pilotage de la proposition de services, et donc de nature fondamentalement en antagonisme avec l'objectif poursuivi, si cela est vraiment au service de l'individu.

Il y a là un champ d'actions assez large où peu de travaux ont été faits au regard de ce qu'il est nécessaire d'entreprendre.

Ce sujet émerge plus du fait de la montée en puissance de la digitalisation des activités (humaines ? économiques ?) que du règlement de protection des données.

Gouvernance des données personnelles

Si l'on bascule sur le règlement (RGPD), c'est finalement le continuum de ce qu'a été la directive de 1995 (FR), la doctrine de la CNIL, il n'y a pas de grands changements, ça a été un peu mieux codifié, médiatisé et organisé, ça a été, et c'est

encore, appréhendé en Europe comme une contrainte. C'est la même chose en Amérique du nord, dans certains états, la Chine a pris des réglementations qui sont probablement plus drastiques que celles du RGPD, nous ne sommes pas dans un cas très particulier en Europe, mais cela a été vécu dans les entreprises et les organisations Européennes comme une obligation difficile.

Ceci souligne quelque chose de plus profond qui finalement touche l'organisation des systèmes d'information [SI] de l'entreprise qui ne sont pas bâtis autour de la gouvernance de la donnée, on assiste à cette mise en évidence, du fait des difficultés pour se mettre en conformité. Cela met en exergue la façon dont les systèmes d'information ont été conçus, notamment dans les grandes entreprises, où, dès les années 70 c'était le cœur métier qui était à l'origine de l'ossature informatique, puis par construction nous avons une grande difficulté à mettre la donnée au cœur du système et, à fortiori, l'individu.

Nous allons assister à une mutation, de même que vont émerger les rôles de mandataire numérique pour l'individu, parce que c'est complexe, voire pour beaucoup d'entreprises, parce que les coûts d'intégrations sont rédhibitoires pour une mise à niveau qui soit compétitive et qui crée de la valeur. Nous sommes dans un schéma assez puissant de modification de l'écosystème.

En parallèle, nous voyons que l'urbanisation des SI est centrée sur le métier, ce qui explique pourquoi beaucoup de grandes entreprises éprouvent des difficultés lorsqu'elles souhaitent étendre leur champ d'activité ou se positionner face à de nouveaux acteurs, entrés sur la scène mondiale de façon disruptive et très rapide. Ce sont souvent des acteurs qui ont construit des SI dont la donnée et sa gouvernance sont au centre du système. Malheureusement nous voyons rarement ce type d'approche, représentant pourtant un élément extrêmement fort de la gouvernance des schémas d'urbanisation dans les entreprises, les institutions publiques et toutes organisations.

Lorsqu'il s'agit de données personnelles, une question se pose, doivent-elles continuer à se trouver au sein de l'entreprise ? Ou bien l'entreprise, qui se prévaut en général de mettre son client au centre de son organisation, ne doit-elle pas aller jusqu'à chercher la donnée là où le client lui précise qu'elle peut être gérée pour son compte ?

Nous allons probablement assister à des modèles extrêmement dynamiques sur des schémas disruptifs pour les entreprises qui adopteront des approches de ce type. C'est probablement une des frontières des 10 années qui viennent. Nous voyons que dans l'évolution d'Amazon, Google, Facebook et autres, il y a tentative de cette prise de position, avec des modèles économiques qui sont à un niveau qui nécessite une captation de la chaine de valeur qui n'est pas forcément compatible avec les engagements qui correspondent à la société européenne aujourd'hui.

En allant un peu plus loin, le RGPD n'est pas vraiment un sujet de préoccupation, la problématique est plutôt d'organiser la gouvernance de la donnée, tout en étant en conformité avec le RGPD bien évidemment, c'est sur cette gouvernance qu'il y a un espace de création de valeur extrêmement fort.

Quand nous regardons la façon dont a été appréhendé le RGPD, par les entreprises et les organisations, des budgets considérables ont été consommés essentiellement pour répondre à une des problématiques qui est relativement la plus simple, à savoir, la constitution de registres permettant de montrer que l'on inventorie, que l'on pilote et que l'on trace l'évolution des modèles de données, des systèmes, des droits à l'habilitation et de la gouvernance. En parallèle, a généralement été fait un inventaire des données structurées et non structurées, de façon à pouvoir indexer l'ensemble des informations en cas de demande de l'individu, cela va rarement beaucoup plus loin.

Le cœur du RGPD ce sont les traitements au fil de l'eau, toute donnée entrante dans une organisation doit être tracée, pseudonymisée, minimisée, il y a très peu d'entreprises et d'organisations qui ont mis cela en place.

La bonne gouvernance des données passe par là et nous, groupe be-ys, sommes assez à l'aise sur ces sujets car nous avions commencé en 2002 à traiter des données nominatives de santé personnelles, alors que la doctrine dominante était plutôt : « c'est interdit, il faudrait une loi pour le faire. ».

C'était « amusant » car 6 mois plus tard les expérimentations dites Balbusiaux[1] ont démarré, se posait alors la question suivante, « peut-on anonymiser ou est-ce du consentement express qui nous permet de traiter les données pour pouvoir apporter du service ? » La tendance générale était de dire, en dehors de l'expérimentation Balbusiaux, on ne peut rien faire. Nous avions adopté une position, dans la mesure où en droit Français l'Etat n'est pas censé avoir des dérogations juridiques, en conséquence de quoi, s'il faisait une expérimentation telle que Balbusiaux, c'est que cela était possible.

Nous avions poussé un peu plus loin le système et nous avions été parmi les premiers à systématiser la signature en temps réel, du propriétaire des données, de l'individu, pour toutes transactions de données nominatives de santé, cela nous a donné un schéma industriel. Quand nous nous sommes posé la question de le faire, comme nous étions sur la « tangente » d'un point de vue de la tendance générale [nous contestions à la CNIL le contrôle d'opportunité mais nous étions tout à fait d'accord avec le contrôle de conformité], nous nous sommes dit que si nous étions contrôlés, il faudrait que nous soyons exemplaires.

Tout ceci pour souligner le fait que, concernant le RGPD, lorsque vous traitez une donnée personnelle sensible, vous êtes dans un droit protecteur, qui consiste à ce que devant un juge, en cas de démarche judiciaire, vous devez apporter un dossier de preuve formelle et recevable par le juge, que la partie adverse ne puisse pas écarter. C'est vrai sur le droit de l'assurance, sur beaucoup de droits bancaires, sur le droit des placements avec la directive européenne sur les placements financiers, c'est vrai aussi sur tous les droits de protection et à ce niveau, devant un juge, il y a énormément de débats …

Il s'agit donc bien d'être en conformité avec le règlement eIDAS[2] qui codifie tous les objets technologiques que l'on utilise dans la digitalisation. La 1ère chose étant « d'équiper l'identité » car si je ne suis pas capable de rattacher mon identité à des faits, je ne suis pas concerné.

Dans un droit de protection, si un individu peut se défendre en disant « prouvez que c'est moi », dans le monde digital, la plupart des acteurs ne peuvent pas se défendre car la signature mise en œuvre n'est pas une signature qualifiée.

Une signature qualifiée nécessite un enrôlement à l'identité, dans une relation en face à face, avec contrôle des pièces d'identité puis remise d'un objet qualifié, dont la garde (l'usage) est acceptée par l'individu, avec signature d'un contrat manuscrit permettant de relier cet objet, la chaine est alors valable pour opérer, y compris pour le renouvellement de l'objet qualifié.

[1] Expérimentation Babusiaux : autorisée en février 2005, cette expérimentation a débuté en octobre 2007 et a été prolongée à deux reprises, jusqu'en décembre 2012. Sur le principe elle permettait d'accéder, de manière anonymisée, aux données de santé présentes sur les feuilles de soins électroniques", en particulier les codes des médicaments et la liste des prestations et produits.

[2] Le règlement eIDAS concerne principalement les organismes du secteur public et les prestataires de services de confiance établis sur le territoire de l'Union européenne. Il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE. L'ANSSI est l'un des organismes nationaux chargés de la mise en œuvre de ce règlement (source : ssi.gouv.fr)

Il n'y a pas d'objet qualifié aujourd'hui en Europe, hormis une carte à puce ou un « dongle », c'est la même technologie, le téléphone ne sera jamais qualifié, nous sommes donc dans une problématique d'ergonomie d'usage.

Avec le RGPD nous sommes exactement dans le même type de problématique : « je peux traiter des données personnelles, je peux mettre une case à cocher, je peux avoir un contrat et, si ce sont des données personnelles sensibles, outre le contrat, à chaque transaction il faut que j'aie une signature électronique, un consentement express, qui devant le juge est la preuve que j'ai exercé mon consentement. »

Les enjeux du futur sont probablement la mise en place de plateformes internet permettant de partager de l'enrôlement, de l'identité numérique et toutes les technologies sous-jacentes. Dans ce contexte avoir une signature qualifiée pour les transactions permet alors de faire beaucoup de choses, notamment de proposer en permanence des avenants de contrats pour gérer progressivement, dans la durée, les évolutions de traitement qui vont pouvoir être apportées à toutes ces données.

Deux éléments importants pour ce futur : d'une part, les données clients traités en conformité [traçabilité, pseudonymisation et minimisation], et d'autre part, de disposer de toutes les possibilités de valorisation qui correspondent aux clauses [relation contractuelle] qui ont été acceptées par le client.

Selon la nature du contrat, s'il n'est pas nécessaire de passer par l'étape de minimisation, il est donc possible de faire un rapprochement d'information.

Dernier sujet via l'angle RGPD, nous avons tout ce qui concerne le traitement des données lorsqu'elles sont pseudonymisées pour tous les services à la personne, au propriétaire ou aux parties prenantes comme des droits sur ces données. Nous [groupe be-ys] sommes allés assez loin sur ce sujet, notamment avec une approche blockchain qui permet d'encapsuler les droits de traitement de parties prenantes pour des traitements particuliers. Aujourd'hui, technologiquement cela fonctionne mais économiquement, c'est inaccessible car le coût du traitement est rédhibitoire, cependant, cela donne des pistes de réflexion …

Pour ce qui est de l'anonymisation, le fait de disposer de données anonymes permet de sortir, de fait, du scope RGPD, le champ des possibles est alors illimité.

Pour compléter cet exposé, tout ce qui concerne les droits de l'individu, notamment le droit à l'oubli et la portabilité, est piste à réflexion pour l'urbanisation des systèmes d'informations. Par exemple, dans certains cas nous [groupe be-ys] avons pris la décision en termes de portabilité, de mettre dans un coffre (électronique) de l'individu, toutes les données de toutes les transactions de services qu'il a pu avoir au fil de l'eau, de façon qu'au moment où il décide d'arrêter [le service] il puisse partir avec ses données et en disposer à sa convenance.

La transformation numérique en cours va bien au-delà de préoccupations purement technologiques, elle prend racine sur un socle d'usages existants actuellement en mutation vers de nouvelles formes qui commencent tout juste à s'exprimer, où la donnée est le dénominateur commun du futur digital.

Problématique du consentement : focus sur le monde bancaire

Le secteur bancaire est un des premiers secteurs qui se soit « dématérialisé » en termes d'échanges de flux. Finalement la sécurité y a été conçue à partir des mouvements financiers et la culture technologique, y compris dans les 1ers moments pour répondre au RGPD, est fille de l'approche technologique bancaire.

Explication : lorsque vous êtes sur des transactions bancaires, vous avez un risque sur les flux, si vous avez une usurpation d'identité, ou une fraude, en général ce sont des choses très bien suivies, dans les 48h les gens se manifestent. En fin d'année, à la clôture des comptes, la banque peut provisionner le risque, c'est un risque mathématique facile d'appréhension et la logique des systèmes bancaires aujourd'hui répond à cette problématique, pratiquement toutes les approches de sécurisation répondent à cela.

Lorsqu'on est sur la gouvernance des données, sur RGPD, sur la maitrise des données personnelles, ce n'est plus un problème de flux mais un problème de stock, où un litige massif peut potentiellement s'opérer sur le stock. Les enjeux de sécurité ne sont pas les mêmes parce que les enjeux financiers en cas de sinistre ne sont pas identiques.

C'est la même chose que sur la Directive sur la Distribution d'Assurances, où, s'il y a un krach, les épargnants vont sans doute se manifester en évoquant le défaut de conseil. En cas de défaut de conseil, l'organisme de placement est redevable du capital, donc prouver l'exigence de conseil attaché à la DDA n'est pas simple car c'est un conseil renforcé qui nécessite d'avoir bien compris toute la composition familiale, les flux de revenus, de patrimoine, l'aversion au risque, etc…

Pour résumer, nous pouvons dire qu'il y a des années de formation pour comprendre de quoi il s'agit, que la personne qui épargne ait compris l'ensemble du système et que le conseiller lui propose une synthèse intelligible.

Comment prouver que tout cela a été fait ?

Dans ce cas, nous ne sommes plus sur les systèmes classiques d'un flux de paiement mais bien sur un stock avec des enjeux qui n'ont plus rien à voir.

Aujourd'hui, compte tenu de la culture bancaire, du fait de l'organisme de contrôle, de l'intérieur de l'organisation ou entre pairs, des maitrises technologiques et de la rapidité avec laquelle les contingences évoluent, ceci ne semble pas être compatible avec la culture des SI bancaires et peu de banques sont capables de répondre à cette problématique pour le moment …