



Atelier 3

Entreprises, quand la culture de la donnée devient un avantage concurrentiel

La question de la propriété des données personnelles est au cœur de cette édition du Forum d'Avignon. Il a été souligné précédemment que le contrôle de la donnée personnelle était un enjeu stratégique tant pour l'individu, dont elle constitue un élément de l'identité numérique, que pour l'entreprise qui ne peut plus raisonnablement envisager de se développer sans la capter pour l'exploiter et la valoriser.

La question du contrôle des données est cruciale pour l'individu car la quantité de données qui sont désormais collectées, traitées et stockées sur chaque personne permet d'aller très loin dans sa connaissance et contribue à un profilage très précis avec la possibilité – en fonction des catégories de données traitées – de produire des modèles probabilistes pour en apprendre davantage sur ses croyances religieuses, ses opinions politiques, son mode de vie, son orientation sexuelle, ses goûts et habitudes et bien d'autres aspects de sa vie personnelle et intime.

La question de la confiance devient encore plus fondamentale pour l'entreprise lorsqu'il est question de bâtir une relation durable avec les clients, afin de répondre à des doutes ou des craintes qui pourraient freiner le développement de ce qui semble être appelé à devenir un levier majeur de création de valeur, tant pour les citoyens que les entreprises.

#1 Le droit ne se prononce pas explicitement sur la question de la propriété des données personnelles mais dessine les fondamentaux d'une éthique des données.

Le droit ne traite pas directement de la question de la propriété des données personnelles. Le droit d'auteur, qui a une dimension patrimoniale, ne confère pas un droit de propriété sur tout type d'information ou de donnée personnelle car il ne protège que la structure et l'organisation de la base et non pas l'information qu'elle contient (sauf si celle-ci est protégée indépendamment de son inclusion dans la base, par exemple des titres d'œuvres protégées par le droit d'auteur ou lorsque l'information fait partie d'une base de donnée protégée par le droit sui generis).

A cet égard, le Conseil d'Etat vient de publier le 9 septembre 2014 une étude intitulée « Le Numérique et les droits fondamentaux » qui réfute la pertinence du droit de propriété (proposition n° 1) pour encadrer l'utilisation des données personnelles et consacre, en s'appuyant sur le droit allemand, l'idée d'un droit personnel sur ses propres données. Ainsi, selon le Conseil d'Etat, *« la reconnaissance du droit de propriété ne permettrait pas en effet de rééquilibrer la relation entre les individus et les acteurs économiques et compliquerait l'exercice de la régulation par les pouvoirs publics. Le droit à « l'autodétermination informationnelle », concept dégagé par la Cour constitutionnelle allemande en 1983, est à la différence du droit de propriété un droit attaché à la personne, tendant à « garantir en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ».*

¹ Par exemple, Dir. Parl. Et Cons. CE n° 95/46, 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et la libre circulation de ces données, JOCE 23 nov., n° L 281, p. 31

² Harvard Law Review Vol IV, December 15, 1890, N°5, P 193

#2 Comment l'éthique des données permet à l'entreprise de disposer d'un avantage concurrentiel ?

Dans un contexte où les questions de confidentialité et de vie privée suscitent un intérêt grandissant pour l'ensemble des citoyens, de plus en plus d'entreprises intègrent cette dimension dans leurs actions de communication envers leurs clients, tentant ainsi de démontrer l'importance qu'elles attachent à la protection de la vie privée. Au-delà de l'aspect juridique, la conformité à la réglementation en matière de protection des données personnelles devient un moyen efficace pour les entreprises de communiquer sur leur engagement éthique et sociétal. Le respect des bonnes pratiques en matière de protection des données à caractère personnel constitue indéniablement un avantage concurrentiel pour les entreprises, quel que soit leur secteur d'activité, mais également un moyen de se prémunir du risque de perte de réputation.

Partant du postulat reconnu que la rétention d'un client requiert un investissement bien moindre que son acquisition, les entreprises déploient des stratégies pour maintenir et entretenir la fidélité de leurs clients. Celle-ci repose essentiellement sur la confiance, laquelle ne peut être

C'est d'ailleurs la philosophie du droit de la protection des données à caractère personnel¹ qui donne à l'individu des leviers juridiques pour contrôler l'utilisation qui est faite de ses données en imposant des obligations positives et sanctionnées de transparence, d'information, de sécurité et de confidentialité, ou encore d'effacement à celui qui détient ces données au bénéfice de celui à qui elles se rapportent.

Le 15 décembre 1890 déjà, deux universitaires américains Samuel Warren et Louis Brandeis avaient publié dans la *« Harvard Law Review »*² un article intitulé *« the right of privacy »*, c'est-à-dire le droit au respect de la vie privée en le mettant en perspective avec un concept de Common Law intitulé *« the Law of implied trust »*, aux termes duquel celui à qui une information confidentielle est confiée est tenu de protéger les intérêts de celui qui lui a confié cette information, c'est-à-dire de traiter l'information dans l'intérêt de ce dernier et non dans son propre intérêt.

Cette notion d' *« implied trust »*, inspirée de la fiducie de droit romain, est plus pertinente que jamais puisqu'elle fait du détenteur de données d'autrui son gardien et protecteur sans pour autant l'empêcher d'en tirer profit puisque le mécanisme du trust a précisément pour objet de permettre au propriétaire d'un bien de le confier à un tiers au bénéfice d'un autre.

Ces règles, quel que soit le système de droit de référence, renferment toutes la notion de confiance, la donnée est communiquée pour autant qu'elle soit traitée en respectant les intérêts de celui dont elle dévoile la personnalité, concept reflété dans les obligations de recueil du consentement ou d'information mais aussi dans le concept de *« trust »*. Il s'agit bien de poser des règles éthiques pour gagner et pérenniser la confiance de celui dont les données personnelles ont vocation à être utilisées par un tiers.

construite et entretenue qu'en tenant compte des deux valeurs fondamentales que sont la **connaissance** et la **reconnaissance**. La **connaissance** enregistre *« l'historique du client »*, c'est-à-dire ses interactions avec les différents services de l'entreprise, auxquelles s'ajoutent des informations relatives aux produits. La **reconnaissance** est la réponse personnalisée que l'entreprise peut apporter en fonction du client : il s'agit donc de s'appuyer sur la connaissance du client pour lui apporter une réponse ciblée, voire de devancer ses attentes.

L'évolution constante des technologies qui a rythmé les dix dernières années, à laquelle s'ajoute le décalage qui existe encore trop souvent entre les engagements, volontaires ou imposés, en matière de protection des données et les pratiques de traitement des données, ont pour effet de renforcer les attentes des consommateurs en matière de confiance et de transparence. Les entreprises qui l'auront compris renforceront leur crédibilité. C'est d'ailleurs une tendance marquée chez nos clients qui nous mandatent régulièrement en Europe comme dans le reste du monde, pour les assister sur la définition et le déploiement des meilleures pratiques en matière de conformité réglementaire relative à la protection des données personnelles (réalisation d'audit labellisé, mise en place de Binding Corporate Rules, coaching des data privacy officer, privacy by design ...).

#3 Pas d'éthique des données in concreto sans culture de la donnée

L'éthique des données doit s'appuyer sur des comportements, d'où l'importance de développer une culture de la donnée.

La culture de la donnée peut répondre à plusieurs objectifs, parfois cohérents et parfois antagonistes. L'entreprise recherchera sans doute à augmenter sa part de marché,

c'est-à-dire à augmenter la conversion de l'internaute en cyberacheteur, voire en lecteur ou encore en ambassadeur d'une marque, mais aussi à améliorer la sécurité des données pour rassurer les clients qui lui confient leurs données. Le régulateur de la protection des données percevra de son côté la culture des données comme un dispositif en vue de favoriser la conformité aux textes afin d'assurer la protection des libertés individuelles dont il est le gardien.

#4 De la culture de la donnée à la gouvernance des données, quels outils et quelles évolutions en Europe ?

Les objectifs des parties prenantes de la culture des données sont sans doute différents mais sont indissociables de l'idée de gouvernance. La gouvernance des données sur le plan éthique va s'appuyer sur des outils techniques et juridiques permettant aux individus, citoyens et consommateurs, de ne pas perdre le contrôle de leurs données.

Sur le plan juridique, en prônant des règles plus strictes de protection des données, la Commission européenne a pris l'initiative avec un projet règlement en cours de discussion, qui devrait être applicable en 2017, et qui vise à contribuer à accroître la confiance des consommateurs dans les services en ligne, et plus largement des citoyens lorsqu'ils utilisent les nouvelles technologies tout en continuant à bénéficier des avantages du marché intérieur.

L'enjeu actuel pour les entreprises est dès lors de structurer leur gestion de la data autour de la réglementation, de la sécurisation et de la certification, comme autant de facteurs de confiance et donc de création de valeur, de performance et de différenciation. En effet, le futur règlement européen va venir ajouter aux principes fondateurs de la Directive 95/46 deux nouvelles exigences fondamentales qui méritent d'être soulignées car elles vont profondément transformer les pratiques des entreprises, à savoir le principe de minimisation des données et surtout le nouveau principe d'« **accountability** », c'est à dire l'obligation faite à l'entreprise de justifier des mécanismes internes mis en œuvre afin de garantir la conformité de ses traitements à la réglementation « informatique et libertés ». Il ne suffira plus pour l'entreprise

de respecter la loi, elle devra également documenter et étayer le dispositif opérationnel déployé pour garantir le pilotage récurrent de cette conformité.

Avec le projet de règlement, le droit de la protection des données « s'opérationnalise ». Les entreprises, soucieuses de fidéliser la confiance de leurs clients tout en retirant les bénéfices de la révolution digitale, doivent dès maintenant être en capacité de démontrer qu'elles ont mis en place les outils et procédures leur permettant de protéger sur le plan juridique et organisationnel les données que leur confient leurs salariés, leurs clients, leurs fournisseurs, etc. Elles limiteront ainsi de manière significative leur **exposition aux sanctions** qui vont être considérablement renforcées (la dernière version du projet de règlement prévoit un plafond de 5% du chiffre d'affaires mondial).

L'investissement dans la gouvernance des données et la conformité au cadre réglementaire deviennent incontournables, mais cet investissement devrait donner un avantage certain aux acteurs qui s'en préoccupent. Il devrait contribuer à favoriser un climat de confiance qui permettra aux entreprises de se prémunir du risque de perte de réputation, dans un contexte où les consommateurs avertis sont largement sensibilisés aux manquements en matière de protection de leur vie privée sur les réseaux sociaux.

« Si l'on veut construire une innovation durable, qui ne soit pas rejetée par l'utilisateur, les entreprises doivent apporter des garanties en termes de protection des données personnelles. Ce n'est pas un coût, c'est un investissement. »³

C'est cet usage conforme au droit et à l'éthique qui permettra aux exploitants des données personnelles de se développer, de promouvoir et de pérenniser leur savoir-faire.

³ Isabelle Falque Pierrotin, « Data la nouvelle ruée vers l'or », Enjeux Les Echos, mars 2013.

#5 La culture de la donnée, c'est aussi le savoir-partager pour éviter l'émergence de monopoles naturels

Les demandes d'analyses permettent aux acteurs du Big data de rentabiliser leurs investissements mais entraînent également une croissance des données disponibles qui renforce la qualité des analyses et par la même la puissance de ces mêmes acteurs. Ceci crée une forte barrière à l'entrée et renforce l'identification du ou des acteurs dominants.

Deux phénomènes viennent généralement rééquilibrer le marché dans ce type de situation :

- ▶ L'acteur dominant étant clairement identifié, une réglementation se met en place pour l'obliger à partager son actif essentiel et favoriser la **concurrence**.
- ▶ Le risque de perte de **confiance** peut se traduire par une réaction des usagers favorisant des concurrents plus agiles, parfois en rupture technologique.

La culture éthique de la donnée devient alors un avantage car essentiel pour ces nouveaux acteurs les protégeant jusqu'à ce qu'ils atteignent à leur tour cette **masse critique** ...

Ernst & Young Société d'Avocats

EY Société d'Avocats est un des cabinets leaders de la fiscalité et du droit. De par notre appartenance à un réseau de dimension mondiale, nous mettons notre expertise au service d'une performance durable et responsable. Nous faisons grandir les talents afin qu'ensemble, ils accompagnent les organisations vers une croissance pérenne. C'est ainsi que nous jouons un rôle actif dans la construction d'un monde plus juste et plus équilibré pour nos clients, nos équipes et la société dans son ensemble.

Ernst & Young Société d'Avocats
Inscrit au Barreau des Hauts de Seine
Membre d'Ernst & Young Global Limited

EY désigne l'organisation mondiale et peut faire référence à l'un ou plusieurs des membres d'Ernst & Young Global Limited, dont chacun est une entité juridique distincte. Ernst & Young Global Limited, société britannique à responsabilité limitée par garantie, ne fournit pas de prestations aux clients. Retrouvez plus d'informations sur notre organisation sur www.ey.com.

© 2014 Ernst & Young Advisory.
Tous droits réservés.
Photos : © Gettyimages

Studio EY France - 1409SG114
SCORE France N° 14-045

Document imprimé conformément à l'engagement d'EY de réduire son empreinte sur l'environnement.

Cette publication a valeur d'information générale et ne saurait se substituer à un conseil professionnel en matière comptable, fiscale ou autre. Pour toute question spécifique, vous devez vous adresser à vos conseillers.

ey-avocats.com

Contacts

Fabrice Naftalski

Associé, Ernst & Young Société d'Avocats
Responsable EMEA des activités Droit des Technologies de l'Information et de la Propriété Intellectuelle
Tél. : + 33 (0)1 55 61 10 05
E-mail : fabrice.naftalski@ey-avocats.com

Bruno Perrin

Associé, Ernst & Young et Associés
Responsable du secteur Technologies, Médias et Télécoms en France
Tél. : + 33 (0)1 46 93 65 43
E-mail : bruno.perrin@fr.ey.com

Louisa Melbouci

Responsable Marketing Technologies, Médias et Télécoms
Tél. : + 33 (0)1 46 93 76 47
E-mail : louisa.melbouci@fr.ey.com