BCG
THE BOSTON CONSULTING GROUP

DLA PIPER

Le Big Data face au défi de la confiance

Carol Umhoefer, Jonathan Rofé, Stéphane Lemarchand - DLA Piper
Elias Baltassis, François Stragier, Nicolas Telle - The Boston Consulting Group
Juin 2014

Le Big Data est en mesure de constituer pour les entreprises un vaste champ de développement et de création de valeur. La croissance exponentielle des données dont disposent les entreprises crée des opportunités nouvelles et peut leur permettre de réinventer leur business model. Par la connaissance très fine des comportements et habitudes de consommation des clients, les entreprises sont en mesure de créer de nouvelles offres et de nouveaux produits, améliorer celles et ceux qui existent déjà, tisser des liens plus forts avec leurs clients, améliorer leurs résultats commerciaux.

Mais le Big Data traite une matière sensible : les données personnelles. La protection de ces données est assurée par un cadre juridique étoffé, complexe, en évolution constante et présentant des différences notables, notamment entre les États-Unis où l'approche réglementaire est sectorielle, et la France et l'Union européenne qui ont imposé leur propre cadre réglementaire. Exploiter ces données peut donc exposer l'entreprise à des risques, souvent sous-estimés ou méconnus. Les premiers sont d'ordre juridique, liés à la non-observation des règles en vigueur. Les autres risques concernent la réputation de l'entreprise auprès de ses clients si ces derniers ne sont pas convaincus qu'ils gardent un contrôle sur leurs données personnelles et que l'entreprise les utilise de façon loyale. Or, la confiance est la clé de la relation entre une entreprise et son client. Il est donc nécessaire de percevoir avec clarté les enjeux juridiques du Big Data afin que ce lien de confiance ne soit pas menacé.

Le Big Data, un gisement de valeur inépuisable…

Le Big Data est un univers qui recouvre trois composantes se complétant les unes les autres : les données collectées, aujourd'hui massives, liées notamment à la multiplication des objets connectés ; les nouvelles technologies qui permettent de les traiter, de les stocker, de les analyser de façon toujours plus précise et à des coûts de stockage et de traitement réduits ; des processus et techniques d'analyse de plus en plus performants permettant de passer de l'ère de l'observation à celle de la prévision et de l'anticipation.

Comprendre ce qui était incompréhensible, prévoir ce qui était imprévisible. Le potentiel du Big Data pour les entreprises est considérable. La masse de données disponibles croît de façon exponentielle. Ces données constituent un gisement de valeur inépuisable et précieux, pourvu que l'on se dote des bons outils pour les exploiter et les analyser. Grâce à la numérisation croissante des transactions économiques et des interactions sociales, les données produites embrassent un univers

beaucoup plus large que dans le passé. Elles sont aussi plus précises et plus personnelles. À côté des outils de transaction traditionnels (cartes de paiement ou de fidélité, achats en ligne, appels aux services clients, demandes d'informations…), apparaissent de nouvelles données issues des réseaux sociaux, de l'étude fine des navigations sur Internet, des objets connectés, qui apportent un éclairage nouveau sur les goûts, les habitudes de consommation et les centres d'intérêt des consommateurs. Ces nouvelles sources d'information rendent progressivement obsolètes les méthodes traditionnelles d'études des consommateurs, comme les panels ou les sondages.

La valeur du Big Data tient dans la richesse, la qualité et la granularité des données traitées. C'est de cette masse de données, des analyses dont elles font l'objet, des algorithmes qui permettent de dessiner des profils de consommation personnalisés, que l'on peut tirer une appréciation très fine, en temps réel, des évolutions des habitudes de consommation et des comportements. Dotée des meilleurs outils technologiques et d'analyse, l'entreprise est alors en mesure de prévoir, voire d'anticiper, les décisions d'achat et les comportements de ses clients.

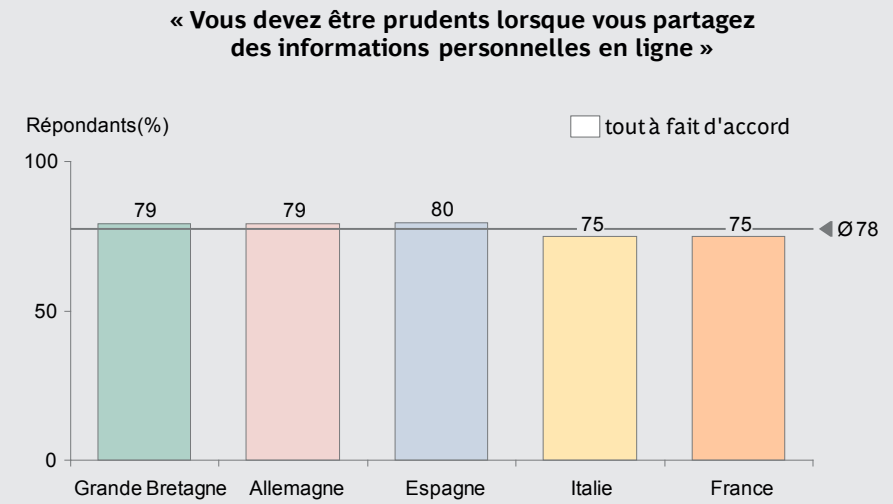
… Qui pourrait rester inexploré si les entreprises perdaient la confiance de leurs clients.

Une part importante du flot de données collectées et exploitées par les entreprises concerne leurs clients, donc des informations relatives à des personnes physiques que celles-ci livrent à chaque interaction commerciale ou informative avec l'entreprise, quels que soient les moyens utilisés (cartes de crédit, navigations Internet, informations relevées par les objets connectés…). Or, la sensibilité du public à la protection des données personnelles est grande. Elle s'est même accentuée récemment, après plusieurs événements qui ont marqué l'opinion, comme la surveillance exercée par la NSA sur les e-mails, communications téléphoniques, navigations Internet, réseaux privés, services de *cloud*, aux États-Unis mais aussi en Europe. Certains acteurs clés de l'Internet comme Google et Facebook se sont vus violemment critiqués après avoir modifié leurs règles de confidentialité.

La confiance est l'élément clé qui lie l'entreprise à ses clients. Elle est longue à s'établir mais peut être ruinée très rapidement. Les études du BCG ont démontré que, dans un domaine aussi sensible que le Big Data, la confiance sera l'élément déterminant pour permettre à l'entreprise d'avoir le plus large accès possible aux données de ses clients, à condition qu'ils soient convaincus que ces données seront utilisées de façon loyale et contrôlée. Certaines entreprises parviendront à créer ce lien de confiance, d'autres non. Or, les enjeux économiques de ce lien de confiance sont très importants. Les entreprises qui réussiront à le créer pourraient multiplier par cinq ou dix le volume d'informations auxquelles elles sont susceptibles d'avoir accès. Sans la confiance du consommateur, l'essentiel des milliards d'euros de valeur économique et sociale que le Big Data pourrait représenter dans les années à venir risquerait d'être perdu.

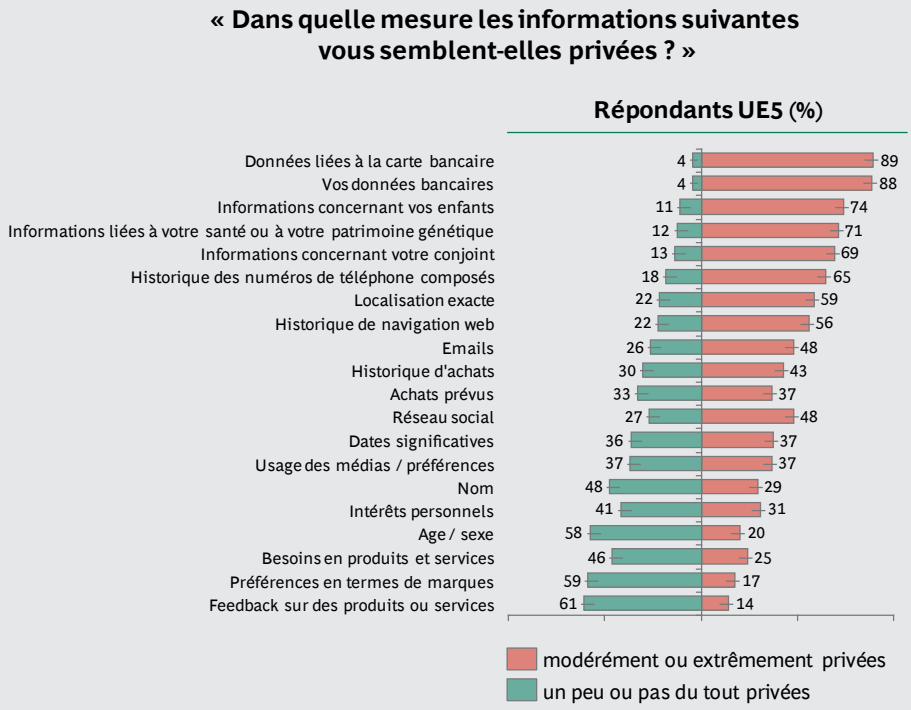
La sensibilité des consommateurs à la confidentialité des données varie selon les domaines. Une étude réalisée par le BCG[1] dans vingt pays, portant sur 10 000 consommateurs, montre que la sensibilité de ces derniers sur la confidentialité des données varie selon la nature de ces informations. Dans les pays de l'Union européenne étudiés, près de neuf personnes interrogées sur dix estiment que les données

Illustration 1 | Les consommateurs sont prudents lorsqu'il s'agit de partager des informations personnelles en ligne



Source: BCG Global Consumer Sentiment Survey 2013.
Question posée: « Merci d'indiquer dans quelle mesure vous êtes d'accord avec la déclaration suivante »

Illustration 2 | La sensibilité dépend du type de donnée

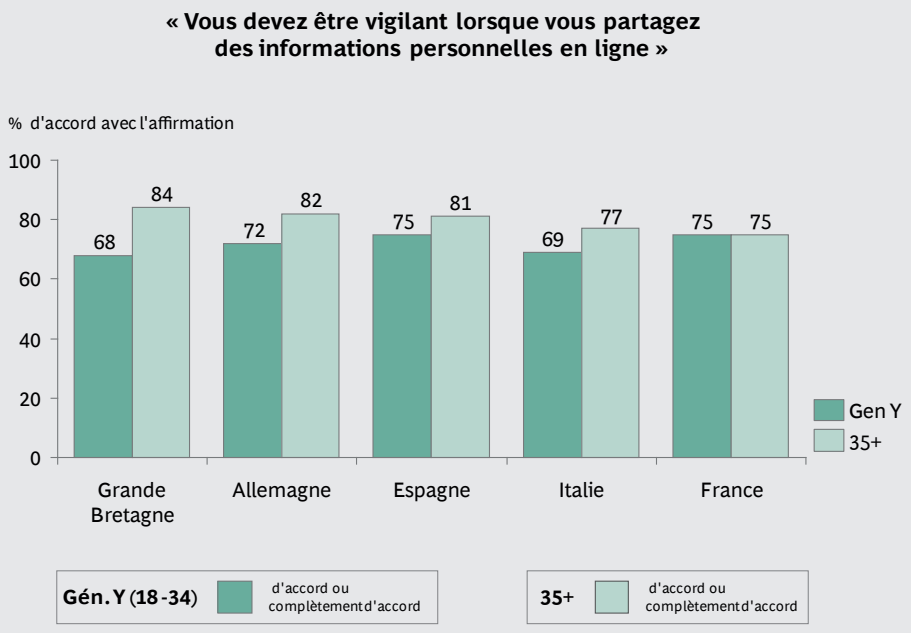


Source: BCG Global Consumer Sentiment Survey 2013.
Note: UE5 (Union Européenne 5) incluant l'Allemagne, la France, l'Italie, l'Espagne, et la Grande Bretagne.

financières et celles concernant les cartes de crédit sont privées. Sept personnes sur dix ajoutent à cette liste les données concernant les enfants, la santé, le conjoint, les communications téléphoniques. La sensibilité au côté privé des données est un peu moins forte concernant la géolocalisation, la navigation Internet, les e-mails, les historiques d'achat et les réseaux sociaux, mais est exprimée tout de même par un consommateur sur deux. Le nom de famille, les centres d'intérêt, l'âge et le genre, les préférences pour telle ou telle marque ne sont considérés comme privés que par une minorité de personnes interrogées.

Mais d'une manière générale, 75 % des personnes interrogées dans la plupart des pays estiment que le caractère privé des données personnelles est un sujet de première importance. Il est important de noter que cette opinion est partagée par l'ensemble des classes d'âge, même si l'on pouvait penser au départ que l'inquiétude face à l'utilisation des données personnelles concernerait surtout les *baby boomers*. En fait, les jeunes générations (génération Y) partagent l'inquiétude de leurs aînés.

ILLUSTRATION 3 | Contrairement à tout ce que vous avez pu lire, la génération Y partage les inquiétudes de ses aînés

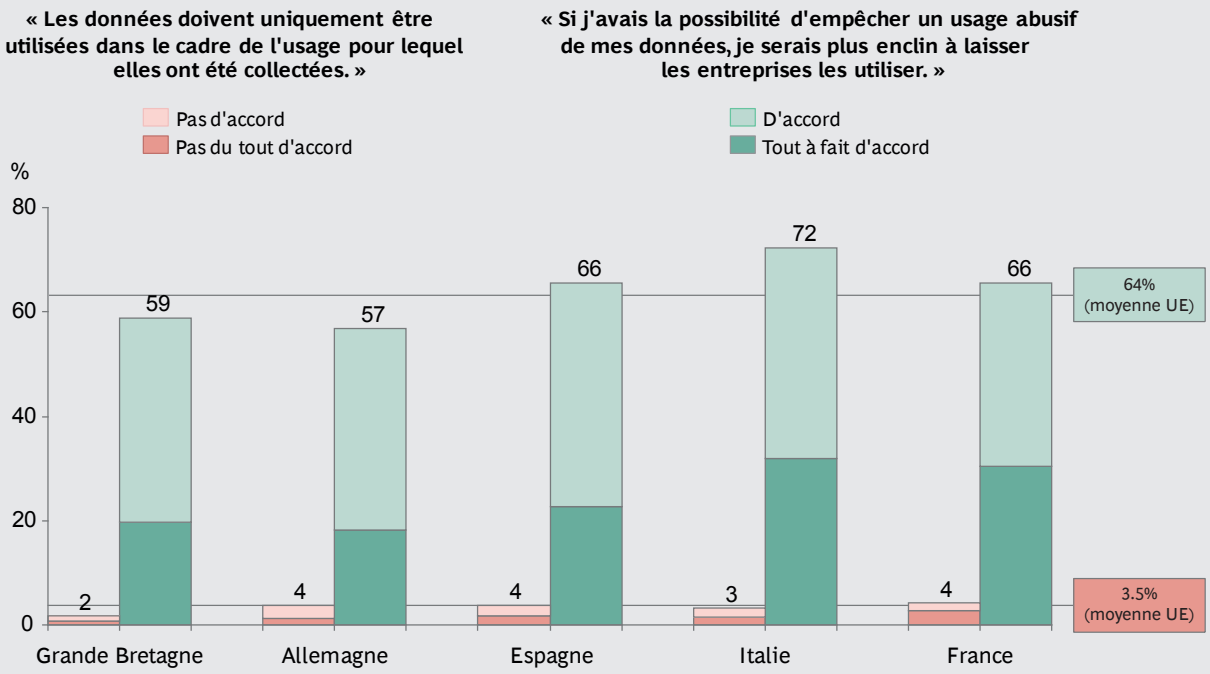


Source: BCG Global Consumer Sentiment Survey 2013.
Note: Génération Y: 18-34 ans

Cette étude du BCG montre également que, dans la plupart des pays étudiés, plus de la moitié des consommateurs accepteraient que les entreprises utilisent leurs données personnelles s'ils étaient convaincus que cette utilisation n'entraînerait aucune conséquence dommageable pour eux (66 % des consommateurs français partagent cette opinion, 57 % en Allemagne, 53 % aux États-Unis).

Dans un passé récent, certaines entreprises ont dû affronter les conséquences négatives pour leur image d'un défaut de protection des données. Citons par exemple le groupe de distribution Target aux États-Unis, victime d'un vol massif de données personnelles de ses clients (numéros de cartes de crédit).

ILLUSTRATION 4 | Accroître la confiance dans l'utilisation des données permet d'augmenter la quantité de données accessibles



Source: BCG Global Consumer Sentiment Survey 2013.

D'autres affrontent les conséquences d'une utilisation non souhaitée des données, comme le groupe espagnol Telefonica, vivement critiqué par les associations de consommateurs et les autorités publiques pour avoir mis au point, à destination des distributeurs, un ensemble de données concernant les déplacements de ses abonnés. Et ceci alors qu'en France, Orange, qui a pris soin d'échanger avec des représentants de la CNIL, commercialise une offre de même nature sans subir de critiques.[2]

Cela confirme que deux entreprises du même secteur, ayant accès aux mêmes données et aux mêmes technologies de traitement et d'analyse, obtiendront des résultats très différents en fonction du niveau de confiance qu'elles auront su créer avec leurs clients et le régulateur. Dans un contexte général où les consommateurs s'interrogent sur l'utilisation faite de leurs données personnelles, seules les entreprises qui sauront les convaincre qu'elles utilisent ces données de façon loyale et contrôlée pourront en élargir la variété et le volume.

Une utilisation raisonnée des données personnelles. Le Big Data est au point de rencontre de trois volontés contradictoires :

- celles des entreprises d'avoir accès au maximum de données personnelles de leurs clients afin d'améliorer leurs offres de produits et services et leurs résultats économiques ;
- celle de certains États et des instances de régulation qui entendent encadrer le plus

étroitement possible l'accès à ces données et leur utilisation ;

- celle des consommateurs qui souhaitent bénéficier d'un service individualisé et pertinent, tout en gardant le contrôle sur l'utilisation de leurs données.

Seules les entreprises qui sauront établir un lien de confiance avec leurs clients et le régulateur, par une utilisation raisonnée des données personnelles, seront en mesure de réconcilier ces trois volontés contradictoires.

Un cadre juridique complexe

Contrairement aux États-Unis où les règles diffèrent selon les États, où il n'existe aucune autorité dédiée à la protection des données personnelles, ni obligation de déclarer les traitements de données, la France s'est dotée d'un ensemble réglementaire et législatif relativement contraignant, notamment au titre de la loi Informatique et Libertés, qui transpose en droit français la directive 95/46/CE. Elle constitue le texte de référence en matière de protection des données à caractère personnel dans les pays de l'Union européenne. Un nouveau règlement européen est en cours d'élaboration, plus contraignant pour les acteurs du Big Data (lire l'encadré pages 19 et 20).

La loi Informatique et Libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004 transposant la directive de 1995, définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Elle renforce le droit des personnes sur leurs données et précise les pouvoirs de contrôle et de sanction de la Commission nationale de l'informatique et des libertés (CNIL).

Lorsque des manquements à la loi sont portés à sa connaissance, la CNIL peut adresser à l'entreprise fautive un avertissement (susceptible d'être rendu public). Après mise en demeure non suivie d'effets, elle peut imposer des sanctions pécuniaires (d'un montant maximal de 150 000 euros, doublé s'il y a récidive) et transmettre les plaintes de particuliers au procureur de la république pour demander la condamnation à des sanctions pénales.

Dans ces deux textes, les grands principes de protection des données personnelles, appliqués au Big Data, s'organisent autour de plusieurs thèmes clés.

La détermination du responsable du traitement. C'est la personne (le plus souvent une personne morale) sur laquelle pèsent les obligations de la loi. Le responsable du traitement est défini comme la personne qui, seule, ou conjointement avec une autre, détermine les finalités et les moyens du traitement des données. Même si le responsable du traitement en confie les moyens techniques à un tiers, il ne s'exonère pas des responsabilités au titre de la loi Informatique et Libertés transposant en France la directive européenne. Ce texte s'impose aux responsables du traitement établis sur le territoire français ou, s'ils sont établis en dehors de l'Union européenne, qui recourent à des moyens de traitement situés en France. Ainsi une société américaine n'ayant pas de présence physique en France, sera soumise à la loi Informatique et Libertés si elle dispose de serveurs sur le territoire français. De même, une société établie en France mais qui utilise, par exemple, des moyens de traitement situés en Inde, sera également soumise à la loi française.

CAS CONCRET

Une banque détenant une filiale d'assurance partageant le même réseau d'agences souhaite cibler sa base de clients bancaires pour promouvoir les produits de sa filiale assurance.

Recommandation

- Les clients de la banque doivent avoir expressément consenti à la réception de messages de prospection commerciale. S'il y a partage des données entre la banque et la filiale assurance les clients doivent y avoir expressément consenti.
- Le droit d'opposition des clients doit être respecté (par exemple, insérer un lien de désabonnement en cas de prospection par e-mail).

La finalité du traitement. C'est l'un des sujets les plus sensibles puisque l'intérêt du Big Data consiste notamment à pouvoir utiliser des données collectées pour une finalité précise (par exemple le suivi après-vente) pour une autre finalité (par exemple créer des profils dans le cadre d'une campagne de marketing). Or, selon la loi française, les finalités des traitements doivent être « déterminées, explicites et légitimes » et doivent avoir été préalablement portées à la connaissance de la personne dont les données sont collectées.

Il existe cependant une exception à cette règle. Lorsque les données n'ont pas été collectées directement auprès des personnes concernées, le responsable du traitement n'a pas à fournir cette information si elle se révèle impossible à donner ou exige, pour être délivrée, des efforts disproportionnés par rapport à l'intérêt de la démarche. Mais cette notion d'efforts disproportionnés est interprétée par la CNIL de façon restrictive. Elle a ainsi reproché à la société Pages Jaunes[3] de ne pas avoir informé, de manière précise et au stade de la collecte de données, l'ensemble des utilisateurs de six réseaux sociaux que leurs données publiques seraient indexées par le service d'annuaire Pages Blanches.

La finalité du traitement et sa communication aux personnes, ainsi que le recueil du consentement des personnes dont les données personnelles font l'objet de ce traitement, constituent donc un enjeu juridique important. Le groupe de travail « Article 29 »[4], sans pouvoir de sanction, qui réunit les autorités de protection des données personnelles au sein de l'Union européenne, considère qu'indiquer une finalité trop imprécise (comme « amélioration des usages », « à des fins de marketing », de « sécurité informatique » ou de « recherches futures », sans autres indications) est contraire à l'exigence d'une finalité clairement déterminée. Certes, cet avis n'a pas, aujourd'hui, de valeur contraignante. Mais il est probable qu'il sera pris en compte dans la nouvelle proposition de règlement européen qui devrait imposer aux responsables de traitements l'obligation de fournir une information plus précise aux personnes concernées par ceux-ci, quant à leurs finalités, en indiquant, le cas échéant, les clauses et conditions générales du contrat justifiant le traitement ou encore les intérêts légitimes poursuivis par le responsable du traitement.

Le détournement des finalités d'un traitement est interdit. Ainsi, selon la lettre de la loi, les données personnelles ne peuvent faire l'objet d'un traitement que pour des finalités dont les personnes concernées ont eu connaissance. C'est au responsable du

traitement de fournir cette information au moment où les données sont collectées et de recueillir le consentement des personnes concernées, le cas échéant. Les entreprises doivent donc se limiter à ces finalités ou à des finalités compatibles avec celles annoncées au départ. En France, l'obligation de déclarer les traitements à la CNIL (une procédure sans véritable équivalent dans les autres pays de l'Union européenne) impose que les entreprises se limitent aux finalités déclarées. C'est donc au cas par cas qu'il faut distinguer les finalités indiquées au moment du traitement et celles qui en sont résolument différentes. Exemple : un traitement de données dont la finalité serait de déterminer le nombre d'utilisateurs connectés à leur téléphone portable, à un endroit et un moment donnés pour optimiser la gestion des réseaux, risquerait d'être considéré comme détourné de sa finalité initiale si les informations ainsi collectées étaient réutilisées pour adresser des messages publicitaires ciblés aux personnes concernées.

Tout changement de finalité du traitement devra être notifié aux personnes concernées, faire l'objet, le cas échéant, d'une nouvelle déclaration de traitement voire de la mise en place de nouvelles garanties en termes de confidentialité et de sécurité des données.

CAS CONCRET

Une compagnie d'assurance propose une assurance automobile à un tarif avantageux, à la condition qu'elle puisse collecter, à l'intérieur du véhicule, par un dispositif de mesures, des données de géolocalisation et de comportement du conducteur (accélérations, vitesse…) afin de s'assurer que la conduite s'effectue en « bon père de famille ».

Recommandation

- Selon la CNIL, il est nécessaire d'obtenir le consentement exprès et informé de l'assuré pour le traitement et en particulier la collecte des données de localisation.
- Il est interdit de collecter des données relatives aux infractions et donc, par exemple, aux éventuels dépassements des limitations de vitesse.

La collecte des données doit être licite et loyale. L'afflux de données disponibles sur Internet, dans un monde où elles semblent être à la disposition de tous, n'exonère en rien le responsable du traitement de données personnelles de les collecter de façon loyale et licite. L'obligation de loyauté de la collecte s'inscrit dans l'exigence de transparence, principe issu de la directive de 1995 et transposé en droit français.

Le simple fait que certaines de ces données soient disponibles sur Internet n'empêche en aucune manière la loi Informatique et Libertés de s'appliquer (le cas CNIL/Pages Jaunes, évoqué plus haut, dans lequel l'entreprise a été sanctionnée pour manquement à son obligation de loyauté). De même, la CNIL a considéré comme déloyale la collecte par les Google Cars d'adresses MAC (adresse physique unique d'une carte réseau d'ordinateur) pour les rapprocher des identifiants SSID d'utilisateurs de réseaux WiFi, à l'insu des personnes concernées. Elle a condamné l'entreprise américaine à une sanction pécuniaire de 100 000 euros, considérant qu'il s'agissait d'une « collecte déloyale »[5]. Dans une autre affaire portée devant la Cour d'Appel de Paris[6],

le site Internet Note2Be a été condamné pour avoir collecté, à leur insu, des informations sur des enseignants en vue d'alimenter un système de notation de professeurs en ligne. Enfin, la CNIL a condamné la société DirectAnnonces à des sanctions pécuniaires pour avoir compilé les annonces immobilières de particuliers (collectées sur plus d'une centaine de sites Internet) afin de proposer aux entreprises des alertes ciblées par secteurs d'activité. La CNIL a considéré que l'absence d'information délivrée par la société mise en cause ne permettait pas aux particuliers de disposer d'une indication claire quant à la finalité de la collecte ni d'exercer leur droit d'opposition à l'utilisation de leurs données dans un délai raisonnable.[7]

CAS CONCRET

Pour améliorer ses ciblages, une marque de grande distribution affecte sur la carte de fidélité d'un client les achats réglés par la carte bancaire habituellement associée à la carte de fidélité, même si le client n'a pas présenté cette dernière à la caisse. Le solde de points de la carte de fidélité s'en trouve néanmoins augmenté.

Recommandation

- L'utilisation du numéro de la carte de paiement doit avoir pour finalité l'une de celles listées dans la recommandation de la CNIL du 14 novembre 2013 relative au « traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance ». Cette recommandation n'inclut pas comme finalité autorisée l'utilisation du numéro de carte de paiement comme identifiant commercial.
- Dans l'hypothèse où la mise en œuvre de ce cas nécessite la mise en place d'une interconnexion entre le fichier contenant les données des cartes de paiement client et le fichier contenant les données afférentes aux cartes de fidélité alors, selon la CNIL, une demande d'autorisation devra être faite auprès de la CNIL.

Un consentement libre et éclairé. Il s'agit d'un autre point crucial du Big Data. Alors que l'objectif des entreprises est d'en savoir le plus possible sur leurs clients, la loi impose que tout traitement de données personnelles s'effectue avec le consentement de la personne concernée, sauf exception. Ce qui laisse néanmoins un certain flou sur l'expression et le mode de recueil de ce consentement. La loi Informatique et Libertés précise simplement qu'« un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée », laissant la possibilité d'un consentement implicite. La loi française n'a pas retenu la formulation prévue par la directive européenne du 24 octobre 1995 qui précise que la personne concernée doit avoir « indubitablement donné son consentement » (*« unambiguous consent »*).

Un consentement valable doit être libre et éclairé. Il incombe donc au responsable du traitement de placer la personne concernée en situation de comprendre en toute transparence les principaux éléments du traitement : nature des données collectées, finalités du traitement, destinataires des données, droits de la personne concernée (droit d'accès, de rectification et d'opposition au traitement), informations relatives aux éventuels transferts de données vers des pays extérieurs à l'Union européenne.

Les entreprises, en qualité de responsables du traitement, ne peuvent donc pas s'affranchir de leur obligation d'informer les personnes concernées des traitements projetés, même si ces personnes figurent déjà dans leurs fichiers.

Ce point est un sujet de contentieux potentiel entre les entreprises et leurs clients. Une étude menée par la CNIL et dix-neuf de ses homologues à travers le monde en 2013 a montré que l'information donnée aux internautes est insuffisante : 20 % des sites mondiaux les plus importants, et 50 % des applications de téléphones mobiles n'apportent aucune information sur les traitements effectués, privant ainsi les utilisateurs de la possibilité de donner leur consentement libre et éclairé à l'utilisation de leurs données.[8] Constat équivalent dressé par le groupe de travail « Article 29 » pour qui la plupart des applications mobiles pour smartphones et tablettes n'informent pas suffisamment les personnes concernées des traitements réalisés grâce à leurs données.

En décembre 2013, la CNIL a infligé à Google une sanction pécuniaire de 150 000 euros, pour l'utilisation combinée de données personnelles issues de l'ensemble de ses services, insuffisamment décrite dans sa politique de confidentialité. Pour la CNIL, Google n'informait pas dans les détails ses utilisateurs sur les conditions et les finalités de traitement de leurs données personnelles (informations incomplètes ou trop approximatives), ne leur donnant ainsi aucune possibilité d'exprimer leur consentement libre et éclairé. Depuis lors, Google a modifié ses règles de confidentialité[9].

Par ailleurs, la Cour de Justice de l'Union européenne a considéré dans une décision très remarquée du 13 mai 2014[10] que Google était responsable du traitement des données personnelles apparaissant sur ses pages, et qu'à ce titre, le moteur de recherche était contraint de supprimer les données personnelles présentes dans les résultats de recherches d'un internaute qui en a fait la demande. Depuis le 29 mai 2014, Google propose aux internautes d'effectuer une demande de suppression des données les concernant que la société jugerait « hors de propos, obsolètes ou inappropriées », par le biais d'un formulaire, non pas probablement à cause du montant de la sanction, mais en raison du risque réel de perte de confiance de ses utilisateurs.

CAS CONCRET

Un opérateur de télécommunications crée une régie publicitaire afin de vendre à des tiers, à des fins de marketing, des données de contact de ses clients (nom, adresse de contact…) associées à des données comportementales agrégées (localisation, niveau de consommation de services de télécoms…) permettant un ciblage publicitaire plus fin que la simple catégorie socioprofessionnelle.

Recommandation

Seules les données de localisation peuvent être traitées, avec le consentement exprès, éclairé et informé de la personne concernée, sous réserve que le traitement de ces données ne révèle pas de données sensibles[1].

1. Si des données de trafic sont collectées par l'opérateur télécom, elles doivent être anonymisées sans possibilité de ré-identification selon les recommandations de la CNIL et du G29 (la simple agrégation est insuffisante).

CAS CONCRET

Un opérateur de téléphonie mobile souhaite promouvoir une nouvelle offre pour les communications internationales. Il lance une campagne marketing auprès de tous ses clients ayant passé plusieurs appels depuis l'international chaque mois, sur une durée de trois mois.

Recommandation

- L'abonné doit être informé dans son contrat d'abonnement ou dans la politique de confidentialité de l'opérateur qu'il sera amené à recevoir de la prospection commerciale émanant de l'opérateur de téléphonie.
- Cependant, la collecte de données de localisation par l'opérateur de téléphonie mobile (afin de déterminer les clients susceptibles d'être intéressés par cette nouvelle offre) nécessite le consentement exprès de l'abonné dûment informé.
- En tout état de cause, l'abonné doit pouvoir exercer son droit d'opposition afin de ne plus recevoir de prospection commerciale.

CAS CONCRET

Un site de vente en ligne engage un partenariat avec une compagnie d'assurance dont les termes sont les suivants : le site avertit en temps réel l'assureur lorsqu'un client acquiert un bien susceptible d'être assuré (produits high-tech notamment). Le site communique ainsi à la compagnie d'assurance les données de contact de ces acheteurs.

Recommandation

- Il convient de s'assurer que les données partagées avec l'assureur sont pertinentes, adéquates et non-excessives.
- Obtenir le consentement exprès et éclairé des acheteurs.
- Mettre les personnes concernées en mesure d'exercer leur droit d'opposition.

La conservation des données doit être limitée. Un point important du cadre juridique du traitement des données personnelles concerne la durée de leur conservation. La loi Informatique et Libertés dispose que le responsable du traitement ne peut conserver les données personnelles que pour la durée nécessaire aux finalités de la collecte et du traitement. Cette durée est donc forcément limitée. Des dispositions législatives et réglementaires imposent des durées de conservation minimum et maximum pour certaines catégories de données et de traitements et les autorités de protection des données peuvent émettre des recommandations pour certains traitements. Ainsi, pour les données collectées à des fins de marketing, la CNIL recommande que les données relatives aux personnes prospectées ne soient pas conservées plus de trois ans à compter de leur collecte ou du dernier contact émanant du prospect.

CAS CONCRET

Un opérateur de téléphonie mobile souhaite analyser les bases de ses anciens clients et cibler ceux de ses clients résiliés qui seraient intéressés par une nouvelle offre (exemple : clients résiliés dont l'analyse indique une cause probable « trop de dépassements de forfait » qui pourraient être intéressés par une nouvelle offre illimitée).

Recommandation

- L'opérateur de téléphonie mobile peut éventuellement bénéficier de l'exception dite « des produits et services analogues » au titre de laquelle le consentement exprès préalable des abonnés n'est pas requis avant l'envoi de messages de prospection commerciale

- Le cas échéant l'opérateur devra vérifier que ces clients ont résilié leur contrat avec l'opérateur depuis moins de trois ans.

L'interconnexion des fichiers est strictement encadrée. L'une des bases du Big Data est de pouvoir croiser entre elles des données issues de différents fichiers afin d'obtenir une information plus précise et de meilleure qualité. Mais là encore, le législateur a souhaité encadrer strictement cette pratique. La loi Informatique et Libertés limite le recours aux interconnexions de fichiers relevant d'autres personnes et dont les finalités principales sont différentes.[11] Elle considère qu'il y a interconnexion lorsqu'au moins deux fichiers ou traitements de données personnelles ayant des finalités différentes sont mis en relation de manière automatisée. Ces interconnexions nécessitent une autorisation préalable de la CNIL.

L'anonymisation des données personnelles, une solution pour échapper au cadre de la loi ? Les données personnelles, au sens de la loi Informatique et Libertés, sont définies comme toute information relative à une personne physique identifiée ou directement ou indirectement identifiable grâce à un numéro d'identification, ou à un ou plusieurs éléments qui lui sont propres. Dès lors que le traitement ne porte pas sur des données personnelles, mais sur des données anonymisées, la loi n'a pas vocation à intervenir.

De nombreuses applications de Big Data concernent précisément des données personnelles anonymisées, ce qui permet de sortir du cadre imposé par la loi Informatique et Libertés. Encore faut-il qu'existe une définition commune des données anonymisées au sein de l'Union européenne, ce qui n'est pas le cas aujourd'hui :

- Au sens de la directive européenne, il convient de considérer « *l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* » pour déterminer si la donnée est anonymisée.

- Pour le groupe de travail « Article 29 », si, compte tenu de ses moyens, la possibilité hypothétique de distinguer une personne n'existe plus ou est négligeable, cette personne ne saurait être considérée comme identifiable[13].

- En France, la loi Informatique et Libertés n'impose pas un examen des moyens « raisonnablement susceptibles » d'identifier une personne mais oblige à examiner si une personne « peut être identifiée, directement ou indirectement », optant ainsi pour une acception plus large de la notion de données personnelles. Dès lors, selon la CNIL, seule une anonymisation « irréversible » permet de sortir du périmètre de la loi Informatique et Libertés.

L'objectif d'anonymisation irréversible est difficile à atteindre car, par l'effet de recoupements massifs que permet le Big Data, des données anonymisées suffisamment précises permettent d'identifier la personne concernée.

L'anonymisation irréversible des données dépendra donc notamment de la taille de l'agrégat de données à anonymiser. À titre d'exemple, au Royaume-Uni, il est possible d'identifier une personne simplement à partir de son code postal (certains codes postaux correspondent en effet à un unique habitant), tandis que cette identification nécessite, à Paris, un agrégat plus important (un code postal peut correspondre à plus de 200 000 personnes).

Le Groupe de travail « Article 29 »[13] a récemment proposé trois critères cumulatifs permettant de déterminer si une solution d'anonymisation offre des garanties suffisantes :

- L'individualisation, qui se définit comme la faculté d'isoler un individu ;
- La corrélation, qui consiste à relier entre elles les données relatives à un individu ;
- La faculté d'obtenir des informations sur un individu par inférence.

S'il manque un critère d'anonymisation, la solution nécessitera en outre une analyse détaillée des risques de ré-identification.

CAS CONCRET

Un opérateur de télécommunications engage un partenariat avec un fournisseur de GPS pour lui fournir des informations de déplacement de ses abonnés et permettre ainsi au fournisseur de GPS d'améliorer ses prévisions de trafic.

Recommandation

- Les données de trafic collectées par l'opérateur télécom doivent être anonymisées sans possibilité de ré-identification selon les recommandations de la CNIL et du G29 (la simple agrégation est insuffisante).
- Seules les données de localisation peuvent être traitées, avec le consentement exprès, éclairé et informé de la personne concernée, sous réserve que le traitement de ces données ne révèle pas de données sensibles.
- Ces recommandations sont valables sous réserve que l'opérateur ne traite et partage que des données pertinentes pour l'amélioration des systèmes GPS.

Les détenteurs de données sont responsables de leur sécurité. La sécurité des données devient un enjeu majeur pour l'ensemble des acteurs, États comme entreprises. À la lumière d'affaires récentes (comme les cas de hacking de données de plus en plus nombreux dont ont été notamment victimes Orange[14] et Ebay[15], les attaques de Robert Gates contre la France[16], l'accusant d'organiser le pillage des données d'entreprises américaines…) on mesure l'importance que revêtira à l'avenir le fait de préserver au maximum la sécurité des données.

En France, la loi Godfrain du 5 janvier 1988 a introduit dans le code pénal les atteintes directes ou indirectes dans un système de traitement automatisé des données (STAD). La loi sanctionne toute personne qui chercherait à s'introduire, par le biais d'un fichier espion par exemple, dans un STAD, d'entraver ou de fausser son fonctionnement, d'introduire, de falsifier ou de supprimer des données de manière frauduleuse (notamment par le biais de la technique du phishing, qui consiste à usurper l'identité numérique d'un site Web et à inviter les internautes à se connecter sur un autre site lui ressemblant afin de capter des informations confidentielles).

La loi Informatique et Libertés fait obligation aux responsables de traitements de prendre toutes les précautions nécessaires pour assurer la sécurité des données personnelles qu'ils traitent. Les données personnelles ne doivent pas être déformées, endommagées ou faire l'objet d'un accès non autorisé par des tiers. Le sous-traitant qui traite des données personnelles doit présenter des garanties suffisantes pour assurer la mise en œuvre des procédures de sécurité et de confidentialité, et le contrat liant le sous-traitant au responsable du traitement doit préciser les obligations incombant au sous-traitant en matière de protection, de sécurité et de confidentialité des données personnelles.

Des obligations particulières s'imposent aux opérateurs de télécommunications et aux banques. Les données traitées par les opérateurs de télécommunications et les banques font l'objet, de par leur caractère très personnel, de réglementations spécifiques.

Ainsi, les opérateurs de télécommunications, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances, y compris le secret du contenu des e-mails. Les données de trafic (les données traitées en vue de l'acheminement d'une communication sur le réseau ou pour établir la facturation) ne peuvent être conservées par les opérateurs que pour établir les factures, commercialiser leurs propres services et fournir des services à valeur ajoutée avec le consentement de l'abonné. Les données de localisation des clients ne peuvent être utilisées, pendant la communication, qu'à des fins d'acheminement des appels. Une fois la communication terminée, l'utilisation de toute donnée de localisation nécessitera d'obtenir le consentement de l'abonné, après qu'il aura été informé de la nature des données concernées, de la durée de leur traitement, de ses finalités et du fait que ces données puissent être transmises à des tiers.

En particulier, bien que certaines sociétés fournissant des services de messagerie électronique analysent le contenu des e-mails afin de proposer des annonces publicitaires ciblées, la validité de ce processus n'a pas encore été confirmée par la CNIL, même si ce traitement est effectué de manière automatique, sans intervention humaine.

Quant aux banques, elles sont soumises au secret bancaire qui interdit toute divulgation de données confidentielles à des tiers (solde des comptes, montant des prêts accordés), sous réserve du consentement des clients.[18]

CE QUI EST LOYAL ET CE QUI NE L'EST PAS… 1/2

L'ensemble des obligations s'imposant aux acteurs du Big Data en matière de protection des données personnelles dresse donc un paysage juridique assez complexe où la frontière entre ce qui est « loyal » et « déloyal » n'est pas toujours tracée avec précision. Certes, le Big Data permet de recueillir des données personnelles comme les adresses e-mail et postales, les numéros de téléphone et de fax, afin de permettre aux entreprises de faire connaître leurs produits et services. Toutefois, s'agissant notamment de la prospection commerciale directe par voie électronique, est interdit tout acte de prospection non sollicité, sans avoir recueilli le consentement exprès de la personne dont on collecte l'adresse e-mail. La CNIL recommande que ce consentement soit recueilli par le biais d'une case à cocher (opt in) et rappelle qu'une case pré-cochée (opt out) est contraire à l'esprit de la loi. Mais il est tout de même possible de prospecter des personnes physiques sans leur consentement si quatre conditions sont réunies :

1. les coordonnées du destinataire ont été recueillies directement auprès de lui (et non récupérées auprès d'un tiers)

2. l'entreprise qui prospecte a déjà fourni un bien ou un service, ce qui témoigne d'une relation entre lui et son client

3. la prospection concerne des services ou produits analogues à la prestation initiale

4. la prospection est réalisée par la même personne physique ou morale. Lorsque plusieurs entreprises co-exploitent un même site Internet, elles ne peuvent donc pas s'échanger leurs bases de clients.

On conviendra que l'ensemble de ces conditions est difficile à remplir, ce qui implique que les acteurs du Big Data qui utilisent des données personnelles pour leur prospection commerciale doivent, le plus souvent, apporter la preuve du consentement préalable des personnes prospectées. Elles doivent également permettre à ces personnes d'exprimer leur droit d'opposition au moment de la collecte des données, et à chaque envoi d'e-mail et/ou de SMS.

La CNIL s'oppose à l'usage de logiciels de collecte automatique d'adresses électroniques à l'insu de leurs propriétaires, à des fins de prospection commerciale. La position de la CNIL a d'ailleurs été suivie par la Cour de Cassation, dans un arrêt de 2006, qui a rappelé que le fait de recueillir à leur insu des adresses électroniques personnelles de personnes physiques sur Internet était « déloyal ».

Une pratique est considérée comme déloyale lorsqu'elle est contraire aux exigences de la diligence professionnelle et qu'elle peut altérer, de façon substantielle, le comportement du consommateur, raisonnablement informé et avisé, à l'égard d'un bien ou d'un service[1]. Cette définition est assez large, et elle n'empêche pas que, dans certains cas, les données personnelles

CE QUI EST LOYAL ET CE QUI NE L'EST PAS… 2/2

collectées et traitées en masse, soient effectivement utilisées à des fins de concurrence déloyale.

La discrimination par les prix pose un problème particulier. Proposer à certaines catégories de clients des tarifs personnalisés, sans les informer des mécanismes conduisant à ces prix différenciés, pourrait fort bien constituer une pratique commerciale trompeuse. Cela concerne notamment les pratiques d'IP tracking (utilisées par certains sites de voyage), qui font évoluer le prix des prestations à la hausse en fonction de la localisation de l'adresse IP (qui peut donner une indication du pouvoir d'achat du client). Selon la CNIL, le recours à de telles méthodes « est susceptible de porter préjudice à certains clients qui se verraient appliquer des tarifs moins avantageux en fonction de leur profil de navigation ». Elle considère que l'IP tracking ressort des pratiques commerciales déloyales, même si l'Assemblée Nationale a refusé de légiférer sur la question lors de l'examen du projet de loi sur la consommation. Mais la question devrait être abordée lors de la discussion du projet de loi sur le numérique, qui devrait être porté cette année devant le Parlement.

1. Code de la consommation, art. L. 120-1.

Au-delà des données personnelles, les bases de données en elles-mêmes sont protégées par le droit. À côté des obligations qui leur incombent en matière de traitement des données, exposées plus haut, les créateurs et producteurs de bases de données sont protégés à la fois au titre du droit d'auteur mais également par le droit *sui generis.* Ils bénéficient de la protection du contenu de leurs bases lorsque leur constitution, leur vérification, leur présentation attestent « d'un investissement financier, matériel et humain substantiel » selon l'article L. 341-1 du code de la propriété industrielle français, une notion reprise dans le droit européen en des termes presque similaires : « investissement substantiel du point de vue qualitatif et/ou quantitatif »[18]. Cela implique, entre autres, de démontrer l'acquisition ou la location de serveurs pour le traitement et le stockage des données, l'investissement dans des capacités réseau importantes ainsi que l'embauche d'équipes compétentes pour le développement et la maintenance des bases.

Le producteur d'une base de données peut donc agir contre tout tiers procédant à une extraction substantielle de son contenu ou la réutilisant sous une forme ou sous une autre. Le caractère « substantiel » de la violation du droit de propriété s'apprécie au cas par cas mais tient compte d'une série de critères comme l'existence ou non d'une situation de concurrence, la nature des données extraites, la référence au contenu de la base, la disponibilité des données extraites en dehors de la base… La notion de réutilisation est assez large puisqu'elle recouvre tout acte non autorisé ayant pour but de diffuser au public tout ou partie du contenu de la base. Cela implique donc que les acteurs du Big Data obtiennent une autorisation préalable avant l'utilisation et l'exploitation de toute base de données tierce.

L'Open Data, c'est-à-dire les informations mises à la disposition de tous par l'État, les collectivités territoriales et les entités de droit public poursuivant une mission de

services publics, constitue un cas particulier. Ces informations sont gérées par la mission Etalab[19], créée en 2011 et sont en général utilisables sous licence ouverte Etalab. Cette licence pose néanmoins une restriction préalable : l'obligation de mentionner la source des données et la date de leur dernière mise à jour. La licence permet notamment de reproduire, copier, publier et transmettre les données publiques et de les exploiter à titre commercial, par exemple en les combinant avec d'autres données ou en les incluant dans sa propre application. L'entité publique qui met à disposition ses données doit le faire gratuitement mais elle ne garantit pas leur absence de défauts ou d'irrégularités. Elle garantit néanmoins que les données ne sont pas protégées par des droits de propriété intellectuelle appartenant à des tiers

CE QUE POURRAIT ÊTRE LA NOUVELLE RÉGLEMENTATION EUROPÉENNE 1/2

Une nouvelle réglementation européenne sur la protection des personnes physiques quant au traitement de données à caractère personnel, est actuellement en cours d'élaboration. Elle s'articulerait autour de plusieurs principes, dont certains font toujours l'objet de négociations au moment de la publication de cet article :

- La définition des données personnelles s'élargit, et cite de manière explicite les identifiants chiffrés, les données de géolocalisation et les identifiants Internet.
- Lorsque le consentement des personnes concernées est nécessaire au traitement des données, ce consentement doit être explicite dans tous les cas. La notion de consentement sans équivoque disparaît.
- Le droit à l'oubli (qui reste néanmoins à définir) est consacré par un texte législatif
- La réglementation européenne s'applique aux entreprises établies en dehors de l'Union si elles suivent ou vendent des produits et des services sur son territoire ou aux consommateurs européens
- Les entreprises réalisant des traitements portant sur plus de 5 000 personnes sur une période continue de 12 mois et les entreprises publiques doivent nommer un responsable de la protection des données.
- En cas de violation de la sécurité des données, le responsable du traitement doit en informer les autorités compétentes, dans un délai de soixante-douze heures, si possible.
- Identification des traitements présentant des risques particuliers en raison de leur finalité ou de leur portée : les traitements à grande échelle visant à évaluer ou prédire les caractéristiques d'une personne et les traitements portant sur les préférences, le comportement, la situation économique, la fiabilité de la personne, sur la base desquels des décisions sont prises.
- En cas de violation de cette réglementation, il est prévu des amendes d'un ordre de grandeur comparable à celui des amendes prononcées en matière de droit de la concurrence.

CE QUE POURRAIT ÊTRE LA NOUVELLE RÉGLEMENTATION EUROPÉENNE 2/2

Cette nouvelle réglementation pourrait avoir des incidences certaines sur les entreprises utilisant le Big Data. La nécessité du consentement explicite pourrait avoir pour effet de submerger les personnes dont les données font l'objet de traitement, de demandes de consentement et d'avertissements en continu. Cette réglementation pourrait aussi conduire à une réduction des données disponibles, ce qui diminue les possibilités de traitement de masses de données. Les obligations supplémentaires incombant aux entreprises pourraient augmenter le poids et le coût administratif du traitement de données. Cet ensemble de règles nouvelles pourrait constituer une menace pour de nombreuses stratégies de monétisation des données, diminuer l'innovation et réduire les opportunités futures.

Pour préserver la confiance, un partage de valeur gagnant-gagnant avec les consommateurs

Évoluer sans encombre dans cet environnement réglementaire et législatif n'est pas chose simple pour les acteurs du Big Data. C'est une condition nécessaire pour maintenir la confiance avec les consommateurs. Mais est-ce suffisant ? En réalité, il faut aussi trouver un juste échange de valeur entre le client qui confie ses données personnelles à l'entreprise et cette dernière qui va les traiter et les exploiter.

Ce partage de la valeur peut-être clairement explicite (la fourniture de données personnelles donne lieu à rétribution (comme le proposent les sites *www.datacoup.com* ou *www.handshake.com.uk*), partiellement explicite (attribution de cartes de fidélité ou de bons de réduction) ou modérément explicite (à l'exemple de Facebook) qui n'explique pas clairement que la contrepartie à l'utilisation gratuite de ses services par les internautes est l'exploitation de leurs données personnelles).

Les garanties de confidentialité et de sécurité des données, la transparence sur les traitements dont elles font l'objet, le contrôle par les consommateurs de leur utilisation, font clairement partie de ce partage de la valeur.

Les rapides développements technologiques et la prise en considération croissante des problématiques de vie privée par les consommateurs façonneront la perception du Big Data jusqu'à son arrivée à maturité. Les acteurs du Big Data devront suivre de près les nouveaux comportements et les nouvelles pratiques, sans en ralentir la nécessaire évolution, pour pouvoir pleinement profiter de leurs outils informatiques.

Quelques règles d'or pour gérer les risques d'un projet Big Data

1. Privilégier les données anonymes lorsque cela est possible
2. Obtenir le consentement éclairé du consommateur lors de la collecte des données
3. S'assurer que le profilage des consommateurs ne crée pas de discrimination
4. Déclarer des finalités de traitement ni trop précises ni trop vagues
5. S'assurer que les données sont exactes et sécurisées
6. Donner aux utilisateurs le contrôle sur l'utilisation de leurs données
7. Mettre en évidence un échange de valeur attractif
8. Ne pas procéder à l'extraction de bases de données tiers sans leur autorisation

NOTES

1. The Trust Advantage: How to Win with Big Data, BCG, November 2013
2. Offre « Flux Vision » d'Orange : http://www.orange-business.com/fr/presse/flux-vision-la-premiere-offre-big-data-d-orange-business-services-a-destination-des
3. Délibération de la formation restreinte de la CNIL, n° 2011-203 du 21 septembre 2011 portant avertissement à l'encontre de la société Pages Jaunes
4. Le groupe de travail « Article 29 » sur la protection des données a été institué par la directive 95/46/CE. Il revêt un caractère consultatif et agit en toute indépendance. Il se compose d'un représentant des autorités de contrôle compétentes désigné par chaque état membre, d'un représentant de l'autorité mise en place par les institutions et organes de l'Union Européenne et d'un représentant de la Commission. Ses missions consistent à fournir des avis d'experts à la Commission sur la question de la protection des données et à promouvoir l'application de la directive européenne dans les pays membres.
5. Délibération n° 2011-035 de la formation restreinte de la CNIL prononçant une sanction pécuniaire à l'encontre de la société GOOGLE Inc.
6. CA Paris, 14e chambre, section A, 25 juin 2008, RG 08/04727.
7. Délibération n° 2009-148 du 26 février 2009 de la formation restreinte de la CNIL prononçant une sanction pécuniaire à l'encontre de la société DIRECTANNONCES.
8. V. http://www.cnil.fr/linstitution/actualite/article/article/operation-internet-sweep-day-une-premiere-mondiale-visant-a-apprecier-le-niveau-dinformat/
9. Modification effective au 31 mars 2014, http://www.google.fr/intl/fr/policies/privacy/
10. CJUE, 13 mai 2014, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González, C-131/12.
11. Article 25 de la Loi Informatique et Libertés.
12. Avis du groupe de travail « Article 29 » n° 4/2007 sur le concept de données à caractère personnel.
13. Avis du groupe de travail « Article 29 » n° 5/2014 sur les Techniques d'Anonymisation.
14. Vol de données personnelles le 18 avril 2014, notifié par Orange le 6 mai, affectant potentiellement 1.,3 millions de clients et prospects
15. Compromission d'une base de 145 millions d'utilisateurs en mai 2014
16. http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/ [EN]
17. Code monétaire et financier, art. L. 511-33.
18. Article 7 de la directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.
19. Décret n° 2011-194 du 21 février 2011 portant création d'une mission « Etalab » chargée de la création d'un portail unique interministériel des données. Le site officiel de la mission Etalab est disponible à l'adresse suivante : *www.etalab.gouv.fr.*

Les auteurs

DLA Piper
Stéphane Lemarchand, Avocat à la cour, Associé DLA Piper Paris
stephane.lemarchand@dlapiper.com

Jonathan Rofé, Avocat à la cour, Counsel DLA Piper Paris
jonathan.rofe@dlapiper.com

Carol Umhoefer, Avocat à la cour, Associée DLA Piper Paris
carol.umhoefer@dlapiper.com

The Boston Consulting Group
Elias Baltassis, Directeur Big Data & Analytics, BCG Paris
baltassis.elias@bcg.com

François Stragier, Principal BCG Paris
stragier.francois@bcg.com

Nicolas Telle, Project Leader, BCG Paris
telle.nicolas@bcg.com

Remerciements à : Jeanne Dauzier, Avocat à la cour, DLA Piper Paris, Patrick Cookson, Avocat à la cour, DLA Piper Paris

Cette publication contient, à titre d'illustration, des cas issus de cas concrets rencontrés dans l'industrie, mais simplifiés à des fins pédagogiques. Seuls des cas pouvant faire l'objet de commentaires en quelques lignes sont présentés. Ils ne sont pas représentatifs de la complexité des situations qui peuvent être rencontrées par une entreprise souhaitant mener une approche Big Data.

Les recommandations apportées dans la présente publication ne sauraient en tout état de cause constituer une analyse juridique exhaustive ou une validation des conditions dans lesquelles les cas peuvent être implémentés. Ces recommandations ne sont valables que sous réserve d'une analyse au cas par cas.

DLA Piper

Avec 4 200 avocats dans plus de 30 pays à travers l'Amérique du Nord et latine, l'Asie Pacifique, l'Europe et le Moyen-Orient, DLA Piper s'impose comme un partenaire de premier plan pour accompagner les entreprises partout dans le monde. À Paris, DLA Piper réunit 115 avocats dont 33 associés et conseille les entreprises, banques et fonds d'investissements français et internationaux pour l'ensemble de leurs besoins juridiques en matière de droit des affaires.

Avec 18 avocats dont 7 associés à Paris, notre équipe IT s'inscrit au sein du groupe IP&T qui compte plus de 400 avocats à travers le monde. Cette équipe, classée année après année parmi les meilleures au monde par les guides de référence internationaux, est dirigée par Stéphane Lemarchand au niveau international et Carol Umhoefer à Paris. Notre équipe est l'une des seules en France capables d'intervenir, en conseil comme en contentieux, sur tous les sujets IT/Outsourcing, innovation, protection des données personnelles, brevets, télécommunications et réglementation, ainsi qu'en marques, contrats commerciaux, distribution et marketing dans de nombreux secteurs d'activité tels que l'informatique, l'internet, les communications électroniques/télécoms, et les médias, à la fois sur des projets domestiques et multi-juridictionnels.

The Boston Consulting Group (BCG)

Le BCG est un cabinet international de conseil en management et le leader mondial du conseil en stratégie d'entreprise. Nous travaillons avec des clients de tous les secteurs partout dans le monde pour identifier ensemble les meilleures opportunités, les aider à affronter leurs défis et faire évoluer leurs activités. À travers une approche personnalisée, nous leur apportons notre vision de la dynamique des entreprises et des marchés ainsi que notre expertise à chaque niveau de leur organisation. Nous leur garantissons ainsi un avantage concurrentiel durable, des organisations plus performantes et des résultats pérennes. Fondé en 1963, le BCG est une entreprise privée présente dans 45 pays avec 81 bureaux. Plus d'informations sur *http://www.bcg.fr/* et *www.bcgperspectives.com*, le portail éditorial du BCG donnant accès aux réflexions et concepts les plus innovants de nos experts en matière de stratégie et de management.


BCG
The Boston Consulting Group


DLA PIPER