Constituer une base de données client / prospect en toute légalité

Chloé Torrès, avocat, directeur département Informatique et libertés du cabinet Alain Bensoussan
Emeline Bissoni, avocat au sein du département Informatique et libertés du cabinet Alain Bensoussan

Les fichiers clients/prospects sont essentiels à la vie des entreprises et font parfois partie intégrante de leur patrimoine. Certaines entreprises font même de ces données le cœur de leur business model en proposant des prestations de locations de fichiers, d'enrichissement de bases de données, de segmentations comportementales etc. Conjuguées au phénomène du « big data »[1] (croissance exponentielle des données produites) auquel l'entreprise n'échappe pas, les données seraient en train de devenir la nouvelle matière première de l'entreprise[2].

Au-delà de la maitrise des aspects techniques, pour valoriser les données qu'elle détient ou utilise, ou celles qu'elle récolte sur internet, l'entreprise devra tenir compte au droit des données à caractère personnel. Les données n'ont en effet de valeur que si l'entreprise les exploite dans le respect de la réglementation applicable et en toute transparence vis-à-vis des consommateurs. L'implémentation d'une politique de protection des données peut constituer un avantage concurrentiel et un réel gage de confiance vis-à-vis des clients actuels ou potentiels.

Le législateur a depuis longtemps adapté les règles juridiques existantes, afin d'encadrer la constitution de tels fichiers et limiter les risques d'atteintes aux libertés individuelles par crainte du phénomène « Big Brother ». Aujourd'hui, le législateur européen est en passe d'intégrer la notion de « privacy » dans le processus de conception d'un système exploitant des données. La Commission européenne prévoit de rendre obligatoire l'approche « Privacy by Design » (PbD) dans le projet de règlement européen visant à réformer la directive 95/46/CE relative à la protection des données à caractère personnel[3].

Cet article traitera de la nécessité croissante de prendre en compte le droit dans le développement des bases de données client.

1. DES DONNEES COLLECTEES EN TOUTE LEGALITE POUR UNE MEILLEURE VALORISATION

Les entreprises ont des obligations vis-à-vis des données personnelles (clients, fournisseurs, prospects, consommateurs) qu'elles détiennent. La constitution et l'exploitation d'une base de données clients/prospects est encadrée par les dispositions issues de la loi Informatique et libertés[4] et de la loi pour la confiance dans l'économie numérique[5].

---

[1] Jean-François Forgeron, « Vous avez dit Big Data ? », post du 3-5-2012, Blog tendances « Informatique et droit », http://www.alain-bensoussan.com/avocats/vous-avez-dit-big-data/2012/05/03

[2] Fabien Humbert, « Big data : la nouvelle matière première de l'entreprise, à côté du capital et du travail », Le Nouvel économiste n° 1600 Cahier n°, du 16 au 22 février 2012, p. 67 s. http://www.lenouveleconomiste.fr/lesdossiers/it-big-data-13734/

[3] Chloé Torres, « Privacy by design », post du 11-5-2012, Blo tendances "Informatique et libertés", http://www.alain-bensoussan.com/avocats/category/blog-tendances/informatique-libertes-blog-tendances

[4] Loi 78-17 du 6-1-1978 relative à l'informatique, aux fichiers et aux libertés.

[5] Loi 2004-575 du 21-6- 2004 pour la confiance dans l'économie numérique.

1.1 LA LOI INFORMATIQUE ET LIBERTES EN BREF

La loi Informatique et libertés impose plusieurs obligations dont nous nous contenterons de citer celles concernant les bases de données clients. La principale obligation est de déclarer les fichiers clients et/ou prospects auprès de la Commission nationale Informatique et libertés (Cnil) ou de les inscrire dans la liste des traitements tenue par le correspondant Informatique et libertés lorsqu'une telle fonction existe au sein de l'entreprise.

Le responsable du traitement a également l'obligation d'informer les personnes auprès desquelles les données sont collectées (clients, prospects, visiteurs, etc.) notamment de leur droit d'accéder aux données qui les concernent, de s'opposer à figurer dans le fichier, de demander à ce que leurs données soient mises à jour, etc.

Il doit également permettre aux personnes auprès desquelles les données ont été collectées, de s'opposer, sans frais, à ce que les données les concernant soient utilisées à des fins de prospection commerciale. Ainsi, il ne peut revendre ces données si les personnes auxquelles elles appartiennent n'ont pas été prévenues en amont.

Par ailleurs, le responsable du traitement doit encadrer les éventuels transferts de données clients/prospects vers des pays situés hors de l'Union européenne qui peuvent survenir par exemple, en cas d'hébergement de la base de données en mode cloud computing, de contrat de routage d'e-mail avec un prestataire, etc. Dans de nombreux cas, le client ne connaît pas la localisation des données. Or la simplicité des services à la demande et le faible coût des solutions « cloud » ne doivent pas masquer la complexité des systèmes informatiques et les questions relatives à la protection et à la sécurité des données personnelles.

La loi sur la protection des données exige en effet que le responsable du traitement de données prenne toutes les précautions utiles, en ce qui concerne la nature des données et les risques du traitement, pour préserver la sécurité des données et, en particulier, d'empêcher leur altération et les dommages, ou l'accès non autorisés de tiers

Les menaces qui pèsent sur les systèmes de bases de données à caractère personnel sont nombreuses : diffusion d'informations confidentielles, falsification, perte accidentelle de données personnelles, etc.

La sécurité doit être conçue pour tous les processus concernant ces données, qu'il s'agisse de leur création, leur utilisation, leur sauvegarde, leur sauvegarde ou leur destruction, et comprend leur confidentialité, leur intégrité, leur authenticité et leur disponibilité.

Les entreprises ont une obligation de « résultat » pénalement sanctionnée en ce qui concerne la sécurité des données. C'est une responsabilité de plus en plus lourde. Les données étant de plus en plus nombreuses, elles sont de plus en plus difficiles à sécuriser.

Le non-respect de ces obligations fait courir des risques financiers et d'images à l'entreprise. La plupart des manquements aux obligations susvisées sont susceptibles d'être sanctionnés de 5 ans d'emprisonnement et de 300 000 € d'amende. La Cnil peut prononcer, à l'issue d'une procédure de contrôle, des sanctions à l'encontre des entreprises n'ayant pas respecté les obligations issues de la réglementation Informatique et libertés.

La Cnil a augmenté fortement ses contrôles (plus de 300 contrôles en 2011) et est régulièrement saisie de plaintes de consommateurs dénonçant le non-respect de leurs droits à être supprimé de la base de données et à ne plus recevoir de prospection commerciale (près de 5000 plaintes ont été reçues en 2011). De tels contrôles ou plaintes constituent un risque majeur pour les entreprises puisqu'ils peuvent aboutir à un avertissement public,

fortement préjudiciable pour l'image de marque des entreprises ; cela pouvant aboutir à une perte de confiance de la part des consommateurs, des partenaires ou clients.

La CNIL a traduit en anglais son guide conçu pour aider les responsables de traitements de données à répondre à leurs obligations en matière de sécurité des données à caractère personnel[6].

1.2 LA LOI POUR LA CONFIANCE DANS L'ECONOMIE NUMERIQUE EN BREF

L'article 22 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique pose les conditions dans lesquelles les opérations de prospection commerciale peuvent être effectuées et les définit comme étant « Tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ».

Ce même article pose le principe de l'interdiction de toute prospection commerciale à destination d'une personne n'ayant pas donné son consentement préalable à celle-ci. « Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen ».

L'expression du consentement pas la personne concernée doit être libre, spécifique et informée. Elle pourra prendre la forme, en pratique, d'une case à cocher sur un formulaire de collecte de données.

En effet, l'article 22 de la loi pour la confiance dans l'économie numérique prévoit, en son deuxième alinéa, que « Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées afin de prospection directe ».

En outre, l'article 22 de la loi pour la confiance dans l'économie numérique prévoit que les personnes concernées doivent avoir la possibilité de s'opposer, sans frais - hormis ceux liés à la transmission du refus - et de manière simple, à l'utilisation de leurs coordonnées lorsque celles-ci sont recueillies et à chaque fois qu'un courrier électronique de prospection leur est adressé.

Chaque message de prospection commerciale doit, par ailleurs, indiquer des coordonnées valables auxquelles le destinataire de la prospection pourra utilement transmettre une demande tendant à obtenir que ces communications cessent, sans frais autres que ceux liés à la transmission de celle-ci. Le message doit également indiquer l'identité de la personne pour le compte de laquelle la communication est émise et mentionner un objet en rapport avec la prestation ou le service proposé(e).

L'entreprise devra donc mettre en œuvre un process permettant d'obtenir le consentement préalable du client et/ou prospect faisant l'objet de la prospection commerciale. Si l'entreprise fait appel à un prestataire extérieur pour effectuer des opérations de prospection (soit par la location de fichiers, soit des opérations d'e-mailing), les contrats devront prévoir une garantie opt-in.

---

[6] Guide Sécurité des données personnelles 2010, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/index.html

De plus en pratique, le courrier électronique de prospection commerciale envoyé par l'entreprise devra indiquer au client :

- sa possibilité de s'opposer, sans frais, hormis ceux liés à la transmission du refus, à l'utilisation de leurs coordonnées ;
- des coordonnées valables auxquelles le destinataire de la prospection pourra utilement transmettre une demande tendant à obtenir que ces communications cessent ;
- l'identité de la personne pour le compte de laquelle la communication est émise ;
- un objet en rapport avec la prestation ou le service proposé(e).

La loi pour la confiance dans l'économie numérique prévoit une dérogation au principe du consentement préalable lorsque la personne a déjà été contactée à l'occasion d'une vente ou d'une prestation de service « analogue » par l'organisme souhaitant la démarcher.

Ainsi, si l'un des partenaires de l'entreprise souhaite adresser des messages commerciaux pour assurer la promotion de produits et services « analogues », cette prospection commerciale pourra être effectuée sans que le consentement préalable de la personne ne soit nécessaire.

Le non-respect du principe du consentement préalable est sanctionné par une amende de 750 € pour chaque message irrégulièrement expédié.

Face à ces nombreuses obligations légales et aux risques inhérents, il est nécessaire à l'entreprise d'implémenter une politique de mise en conformité Informatique et libertés adaptée à son secteur d'activité afin de rassurer les consommateurs ainsi que ses partenaires commerciaux.

2. L'APPROCHE « PRIVACY BY DESIGN » (PbD) POUR UNE MEILLEURE PREVENTION DES RISQUES

Toute nouvelle technologie recèle des dangers. Le potentiel intrusif de certaines d'entre elles exige que la vie privée et la protection des données à caractère personnel soient prises en compte et protégées dès la conception en pratiquant l'approche « Privacy by Design » (PbD) prônée par la Commission européenne. L'adoption de cette approche par l'entreprise peut être complétée par la désignation d'un Correspondant Informatique et libertés.

2.1 LA PRIVACY BY DESIGN

La protection des données doit être au cœur des process internes. Le concept de Privacy by Design consiste à concevoir des produits et des services en prenant en compte dès leur conception les aspects liés à la protection de la vie privée et des données à caractère personnel. Il implique également le respect de ces valeurs tout au long du cycle de vie de la technologie concernée.

Ce concept est une tendance très marquée, principalement dans les groupes internationaux, et est amené à se développer de plus en plus dans les entreprises de BtoC. La pratique du PbD constitue en effet, un nouvel outil de différenciation face à la concurrence et un gage supplémentaire de qualité et de confiance pour les clients et consommateurs.

Cette tendance est appelée à se généraliser, dans la mesure où elle correspond à l'esprit du projet de règlement européen visant à réformer la directive n° 95/46/CE relative à la protection des données à caractère personnel.

La Commission européenne prévoit ainsi de rendre obligatoire l'approche « protection des données personnelles dès la conception » et propose l'adoption du Privacy by Design pour tous les produits, services et systèmes exploitant ce type de données.

Du côté des consultants qui se sont prononcés sur la PbD, « il importe peu qu'une technologie soit invasive à la base, puisqu'elle peut être accompagnée et corrigée par des dispositifs améliorant ou dégradant le traitement des données personnelles en fonction des finalités du dispositif »[7]. C'est ce que certains appelle la « mutabilité des technologies »[8].

Pour le député Patrick Bloche qui s'est prononcé en février 2012 sur la proposition de résolution européenne, il faut encourager la PbD afin de doter l'Europe « d'une véritable politique industrielle du numérique et lui permettre ainsi de bénéficier d'un indéniable avantage comparatif dans la compétition mondiale »[9].

L'implémentation d'une politique de Privacy by Design permet ainsi, aux entreprises de s'assurer de la conformité des traitements qui seront mis en œuvre à la réglementation Informatique et libertés et constitue ainsi un outil de management du risque juridique.

La mise en œuvre d'une politique de Privacy by Design nécessite, dans un premier temps, l'élaboration d'une méthodologie permettant de l'intégrer concrètement dans les projets technologiques. Elle implique dans un deuxième temps, d'analyser le traitement envisagé. Cela permettra enfin, de déterminer très précisément dans le cahier des charges, au regard de la réglementation applicable, les caractéristiques de la base de données client/ prospects afin que celles-ci soient en adéquation avec les modalités du traitement. Ainsi, l'entreprise aura une réelle visibilité sur les catégories de données, l'origine des données et leur durée de conservation.

Cela permet ainsi de pratiquer une réelle transparence à l'égard des consommateurs souhaitant obtenir des informations sur le traitement de leurs données. La mise en œuvre de cette approche peut être complétée par la désignation d'un Cil.

2.2 LA DESIGNATION D'UN CIL

Depuis sa création en 2004, près de 8000 entreprises ont fait le choix de désigner un correspondant Informatique et libertés chargé d'assurer le respect des obligations prévues par la loi Informatique et libertés au sein de l'entreprise.

Cette désignation est facultative en France, toutefois le projet de règlement européen relatif à la protection des données personnelles, publié par la Commission européenne le 25 janvier 2012, prévoit de rendre obligatoire la désignation d'un Cil lorsque le traitement est mis en œuvre par une entité qui emploie au moins 250 personnes et qu'il exige un suivi régulier et systématique des personnes concernées et présente ainsi des risques particuliers au regard des droits et libertés.

La désignation d'un Cil présente de nombreux avantages. En premier lieu, cela améliore la sécurité juridique. Les risques liés à la non-application de la loi Informatique et libertés sont majeurs depuis la réforme de 2004[10] qui a augmenté le montant des condamnations et développé les pouvoirs de contrôle et de sanction de la Cnil. La désignation d'un Cil permet à l'organisme de limiter les risques juridiques en :

---

[7] « Une place au droit dans la Privacy by design ? », GBH-Consultant, Chronique juridique du 1er mars 2012 : http://www.gbh-consultant.fr/?p=44

[8] Anne Cavoukian Ph.D., « Get Smart About Privacy: Smart Privacy and Privacy by Design », 20 octobre 2009, http://www.ipc.on.ca/images/Resources/2009-10-20-IAPPKnowledgeNet.pdf

[9] Rapport AN n° 4326 du 7-2-2012, http://www.assemblee-nationale.fr/13/pdf/rapports/r4326.pdf

[10] Loi 2004-801 du 6-8-2004 modifiant la loi 78-17 du 6-1-1978.

- favorisant l'atteinte et le maintien en condition opérationnelle de la complétude légale par la centralisation des problématiques Informatique et libertés autour d'une seule et même personne ;
- s'assurant que l'informatique de l'entreprise se développe sans danger pour les droits des clients et des salariés sur les données les concernant ;
- permettant à celle-ci de bénéficier d'une veille juridique en matière Informatique et libertés ;
- facilitant une meilleure application des modifications issues de la loi n°2004-801 du 6 août 2004.

En second lieu, cela renforce l'image de l'entreprise vis-à-vis des consommateurs et des partenaires commerciaux. La désignation d'un Cil montre la volonté de l'entreprise de respecter la loi Informatique et libertés et les recommandations de la Cnil. C'est un facteur d'amélioration de la compétitivité des entreprises en augmentant le degré de confiance que peuvent avoir à leur égard les salariés et les clients.

En dernier lieu, cela participe à la mise en œuvre d'une approche qualité. Les qualifications inhérentes à la fonction de Cil ainsi que la tenue d'une liste des traitements mis en œuvre dans l'entreprise, sont de nature à s'inscrire dans une approche qualité de la gestion de l'information au sein de l'entreprise et plus particulièrement des traitements de données à caractère personnel.

La désignation d'un Cil permet en outre de maintenir une adéquation permanente entre les exigences de la loi et les recommandations de la Cnil avec les réalités quotidiennes de l'entreprise s'agissant en particulier de l'évolution permanente des technologies impliquant des traitements de données à caractère personnel.

***

Avec les échanges de données dans l'ère de la mondialisation et le phénomène du "Big data", les nouveaux défis en matière de protection des données personnelles et de la vie privée sont nombreux pour l'entreprise.