ALAIN BENSOUSSAN
Juristendances Informatique et Libertés
n° 39 – Mai – Juin 2011

DÉMARCHAGE TÉLÉPHONIQUE : ADOPTION D'UNE PROPOSITION PROTÉGEANT LES CONSOMMATEURS

Le principe de l' « opt-in » appliqué au démarchage téléphonique

▪ Déposée le 11 mars 2011 au Sénat, la proposition de loi visant à renforcer les droits des consommateurs en matière de démarchage téléphonique a été adoptée en première lecture par le Sénat le **28 avril 2011** (1).

▪ Estimant qu'il est inéquitable que le consommateur, en butte à des **pratiques commerciales agressives**, doive s'opposer, par une démarche active, à ce que des données le concernant soient utilisées à des fins de prospection commerciale, les sénateurs Jacques Mézard et Yvon Collin, rédacteurs de la proposition de loi, ont suggéré de réviser le cadre légal en vigueur en vue de **généraliser le principe de l' « opt-in ».**

▪ Ce texte devrait être soumis prochainement à l'examen de l'Assemblée nationale.

Un dispositif qui requiert l'implication active de l'ensemble des acteurs

▪ Le texte en projet propose l'insertion dans le **Code des postes et des communications électroniques** d'un **nouvel article L. 34-5-1** stipulant que, lors de la conclusion d'un contrat de fourniture de service téléphonique au public, l'opérateur de communications électroniques doit recueillir le **consentement exprès de l'abonné**, personne physique, pour l'utilisation par voie téléphonique, par un tiers au contrat, de ses données à caractère personnel à des fins de prospection directe.

▪ Il a pour particularité de ne pas modifier les dispositions de l'**article 38 de la loi Informatique et libertés**, contrairement à la première version du texte, qui en proposait une nouvelle rédaction.

▪ En outre, il préserve la faculté pour le consommateur de **manifester son refus à tout moment**, même après qu'il ait consenti au traitement de ses données.

▪ Il prévoit, par ailleurs, l'introduction, dans le Code des postes et des communications électroniques, d'un **nouvel article L. 39-3-2** adopté en vue de sanctionner le non-respect des dispositions de l'article L. 34-5-1 par le prononcé d'une **peine d'amende de 45 000 euros**.

▪ L'article 4 du texte en cours d'examen applique le principe de l' « opt-in » aux **abonnements téléphoniques en cours** en imposant à l'opérateur de recueillir l'accord de l'abonné à l'utilisation de ses données personnelles pour démarchage dans le délai d'un an à compter de la publication de la loi.

▪ La méconnaissance de cette obligation fait encourir à l'opérateur concerné une peine d'amende de 45 000 euros.

▪ À **défaut de réponse de l'abonné** dans le délai de deux mois à compter de la demande de l'opérateur, son **consentement** est **réputé acquis** afin de ne pas bloquer indéfiniment la pratique du démarchage par l'inaction de l'abonné. Le nouveau dispositif requière donc une démarche volontaire de l'abonné qui doit exprimer son refus d'être démarché.

▪ La **détermination des moyens** les plus appropriés au recueil du consentement est laissée à l'appréciation du pouvoir réglementaire.

L'enjeu

Réguler les appels téléphoniques intrusifs à des fins de prospection directe par l'application du principe de l' «opt-in».

Les perspectives

Ce nouveau droit dévolu aux abonnés devrait figurer sur le contrat d'abonnement téléphonique, au titre des informations obligatoires fixées par l'article L. 121-83 du Code de la consommation.

(1) Doc. Sénat n° 102 du 28-4-2011 ; Sénat, Dossier législatif

CELINE AVIGNON

LA MISE EN CONFORMITÉ INFORMATIQUE ET LIBERTÉS DES TRAITEMENTS DES COLLECTIVITÉS LOCALES

L'application de la loi Informatique et libertés par les collectivités

▪ Les collectivités territoriales sont amenées à **collecter et à traiter** nombre de **données à caractère personnel**, concernant les usagers des services publics, comme les administrés et les agents travaillant pour les collectivités.

▪ La diversité des compétences exercées par les communes d'une part, et d'autre part, le nombre important d'usagers concernés expliquent la multiplicité des traitements susceptibles d'être opérés. Un phénomène qui s'amplifie en raison notamment des **transferts de compétence** réalisés au profit des collectivités par l'Etat, en application de la **loi du 13 août 2004** (1).

▪ Les **principales catégories de traitements** de données personnelles peuvent être classifiées comme suit : l'état civil, les fichiers électoraux, l'administration des populations, l'urbanisme, la fiscalité, la sécurité municipale, les télé-services, la scolarité, le culturel, le tourisme.

▪ A l'instar des autres organismes privés ou publics, les collectivités sont soumises à la loi Informatique et libertés pour les traitements de données à caractère personnel qu'elles mettent en œuvre, des **contrôles** étant susceptibles d'être faits **par la Cnil**.

▪ En cas de méconnaissance des dispositions de la loi, des **poursuites pénales** sont susceptibles d'être engagées à l'encontre du **responsable de traitement** à savoir, le représentant légal de la collectivité : maire, président d'un établissement public de coopération intercommunale (EPCI) EPC, président du Conseil général ou régional.

▪ La **loi du 10 juillet 2000**, dite « loi Fauchon » (2), a toutefois aménagé le régime de **responsabilité pour faute non intentionnelle**, en vue de limiter les mises en cause pénales d'élus locaux jugées excessives. Désormais, un élu n'encourt plus de condamnation pénale s'il rapporte la **preuve des diligences accomplies**.

Contrôle de légalité des traitements mis en œuvre par les élus locaux

▪ Le **3 février 2011**, la Cnil a procédé à la **mise en demeure** d'une collectivité territoriale qui s'était constituée un **tableau d'évaluation des agents**, comportant notamment leurs congés de maladie (3).

▪ La Commission a relevé qu'aucun des autres traitements mis en œuvre par cette collectivité (vidéosurveillance, badgeuse) n'avait fait l'objet de **formalités préalables** et ne disposait d'une **politique de conservation des données**. Elle a mis en demeure la collectivité, de procéder sous 2 mois à l'ensemble des formalités, de faire cesser les collectes excessives de données et d'informer les personnes visées de leurs droits (3).

▪ Dans cette même logique, rappelons la récente condamnation d'un maire à une peine d'amende de **1 500 euros** pour **détournement de la finalité** d'un fichier et **collecte illicite** de données par constitution d'un « **fichier de population** » avec les données issues du **recensement Insee** (4).

▪ Enfin, notons les condamnations de l'**Ealing Council** et de l'**Hounslow Council**, prononcées par l'ICO (5) à la suite du **vol d'ordinateurs portables** non cryptés d'employés à leur domicile personnel. Les données sensibles de quelques 1 700 administrés de ces institutions ont été volées.

▪ L'ICO relève un **risque significatif pour la vie privée des administrés** (seul un mot de passe protégeait l'accès à ces ordinateurs alors même que les employés n'officiaient qu'en télétravail). En conséquence, l'ICO a imposé une **sanction pécuniaire** s'élevant à **£80 000** à l'Ealing Council et **£70 000** à l'encontre de l'Hounslow Council.

L'actualité

Le développement des télé-services, préconisé par le plan France Numérique 2012, impose aux collectivités de se conformer au référentiel général de sécurité (RGS), élaboré par l'ANSSI, relatif à la sécurité des échanges entre administrations, ou entre administrations et usagers.

(1) Loi 2004-809 du 13-8-2004
(2) Loi 2000-647 du 10-7-2000
(3) Cnil, Communiqué du 28-3-2011
(4) TGI Cambrai du 13-7-2010; Cnil, Communiqué du 31-1-2011

Les conseils

Les élus locaux doivent recenser l'ensemble de leurs traitements de données personnels afin d'instaurer des procédures opérationnelles de vérification de la conformité visant à garantir une traçabilité des actions. Ces actions pourraient être exercées par un Correspondant Informatique et Libertés.

(5) Décis. ICO du 4-2-2011, homologue Cnil sur l'Ealing Council et Décis. ICO du 4-2-2011, homologue Cnil sur l'Hounslow Council.

STEPHANIE LE BRIS

Le responsable de traitement est-il tenu de garantir la sécurité des données ?

▪ **Oui**, la sécurité des données, objet de collecte et de traitement, incombe au responsable de traitement..

▪ Il est soumis à cette obligation qu'il s'agisse de la création, de l'utilisation, de la sauvegarde, de l'archivage ou de la destruction des données concernées, tant au regard de la **confidentialité**, que de l'**intégrité**, de l'**authenticité** et de la **disponibilité des données**.

▪ Le responsable du traitement des données n'est pas soumis à une obligation de résultat, il devra néanmoins être en mesure de prouver qu'il a mis en œuvre toutes les **mesures techniques et d'organisation** pouvant raisonnablement être attendues pour s'assurer du respect de la protection des données (2).

▪ Les **mesures** prises doivent être **conformes à l'état de la technique** et **adaptées au risque** présenté par les données, qu'il soit de nature **informatique** (intrusion, cheval de Troie, etc.) **ou matériel** (incendie, vol physique de données, etc.).

Le responsable du traitement peut-il être sanctionné en cas de défaillance ?

▪ **Oui**, des **sanctions administratives ou financières** sont susceptibles d'être prononcées à l'encontre du responsable du traitement par la Cnil, réunie en formation contentieuse, lorsqu'elle constate des manquements graves à la loi Informatique et libertés dans le cadre d'opérations de contrôle diligentées sur place.

▪ Les sanctions, prises sur le fondement de l'**article 45 de la loi Informatique et libertés**, se déclinent comme suit : l'avertissement, la mise en demeure, les sanctions pécuniaires et l'injonction de cesser la mise en œuvre du traitement.

▪ Le responsable du traitement encourt également des **sanctions pénales** prévues aux **articles 226-16 à 226-24 du Code pénal** (3), la Cnil ayant la faculté de dénoncer au procureur de la République les infractions à la loi dont elle a connaissance.

▪ Ainsi, le non-respect des dispositions de l'article 34 susvisé, y compris par négligence, est puni de **cinq ans d'emprisonnement** et de **300 000 euros d'amende**, en application de l'article 226-17 du Code pénal.

Quelles sont les bonnes pratiques à mettre en oeuvre ?

▪ En vue de garantir, à long terme, la sécurité des données à caractère personnel collectées à des fins de traitement, il est proposé :

- de rédiger un **référentiel des bonnes pratiques** à destination de l'ensemble des personnels en charge de la collecte et du traitement des données ;

- de désigner un **correspondant Informatique et libertés (Cil)** ayant pour mission de définir et mettre en œuvre des procédures de vérification de la conformité des pratiques aux exigences de la loi Informatique et libertés, cette désignation ayant pour finalité de garantir la traçabilité des actions engagées, des alertes et des corrections apportées, dans le cas où une pratique non-conforme ou une pratique à risque aurait été décelée ;

- d'effectuer périodiquement des **actions de sensibilisation** du personnel en vue de garantir le respect effectif des dispositions de la loi Informatique et libertés.

L'essentiel

(1) En vertu de l'article 34 de la loi Informatique et libertés, il « est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès », Loi 78-17 du 6-1-1978 modifiée

(2) Directive 95/46/CE du 24-10-1995, art. 17

(3) Code pénal, art. 226-16 à 226-24

Adoption par la Cnil du programme annuel des contrôles 2011

▪ La Commission a adopté, le 24 mars 2011, le programme annuel des contrôles pour l'année 2011. Ces **contrôles, estimés à 400** par la Commission, seront axés principalement sur les dispositifs de vidéoprotection, la sécurité des données de santé à caractère personnel, la prospection par voie électronique, le profilage des personnes, ainsi que les flux transfrontaliers de données (1).

Journée consacrée aux Cils au Palais du Luxembourg

▪ Le 8 avril 2011, était organisée à Paris, sous l'égide de la Cnil, une journée dédiée aux correspondants Informatiques et libertés (Cil). Cinq ans après la parution du décret instituant le Cil, cette journée a permis, selon la Cnil, « de **dresser un premier bilan** de ce nouveau métier et de ses perspectives d'évolution, notamment au regard de la révision de la directive de 1995, qui pourrait conduire à rendre obligatoire la désignation des Cil ». Elle a aussi été l'occasion pour des Cil français et étrangers de témoigner de leurs expériences et de leurs réflexions (2).

Mise en ligne du nouveau formulaire de réclamation auprès du CEPD

▪ Toute personne qui estime que ses droits n'ont pas été respectés par une institution ou un organe de l'Union européenne, lors de la mise en œuvre d'un traitement de données la concernant, peut déposer une réclamation auprès du CEPD. Le nouveau formulaire de dépôt de réclamation (3) est **disponible sous format électronique**. Il est conseillé d'y adjoindre l'ensemble des éléments susceptibles d'étayer la demande.

Avis du CEPD sur les données des dossiers passagers (données PNR)

▪ Le Contrôleur européen de la protection des données (CEPD) a émis, le 25 mars 2011, un avis (4) sur la proposition de directive de l'Union européenne du 2 février 2011 visant à imposer aux **compagnies aériennes** de transmettre aux États membres de l'Union des données recueillies auprès des passagers (Passenger Name Record – PNR) de vols internationaux en provenance et à destination de l'Union en vue de lutter contre les actes criminels graves et les actes de terrorisme.

Formalités allégées pour les PC portables à lecteur d'empreintes digitales

▪ Depuis mars 2011, les ordinateurs **portables professionnels** intégrant des lecteurs d'empreintes digitales font partie des dispositifs bénéficiant d'une déclaration simplifiée (c'est-à-dire d'un simple engagement de conformité) (5).
▪ Pour en bénéficier, les traitements mis en oeuvre doivent avoir pour unique but de contrôler l'accès à des ordinateurs portables professionnels. Il ne doit pas être utilisé à des fins de contrôle du temps de travail, finalité nécessitant une autorisation de la Cnil.

Sources

(1) Cnil, rubrique Actualité, article du 26-4-2011.

(2) Cnil, rubrique Actualité, article du 7-4-2011 ; Décret 2005-1309 du 20-10-2005

(3) Contrôleur européen de la protection des données CEPD, Formulaire type de dépôt de réclamation

(4) CEPD, Avis du 25-3-2011

(5) Cnil, Délib. 2011-074 du 10-3-2011

Directeur de la publication : Alain Bensoussan
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres, Céline Avignon, Stéphanie Le Bris et Isabelle Pottier, avocats
Diffusée uniquement par voie électronique
ISSN 1634-071X
Abonnement à : paris@alain-bensoussan.com

par Isabelle Pottier

Le CIL, véritable pivot de la conformité informatique et libertés au sein de l'entreprise

Hélène Legras, Correspondant informatique et libertés des sociétés du groupe AREVA auprès de la CNIL (*) membre de l'AFJE (**) et administrateur de l'AFCDP (***)

1. Pouvez-vous brièvement nous dire en quoi consiste la fonction de CIL d'un grand groupe comme AREVA ?

Tout d'abord, il convient de préciser que je suis le CIL « mutualisé » de tout le Groupe AREVA constitué de 337 sociétés françaises et étrangères. Le CIL mutualisé d'un grand groupe International doit se constituer un réseau interne de Relais Informatique et Libertés, dont fait partie le Correspondant à la Protection des Données, (*datenschutzbeauftragter*) des filiales allemandes. Effectivement le CIL est obligatoire en Allemagne dans les entreprises de plus de 9 salariés pour le traitement automatisé de données. Il doit pouvoir appliquer les spécificités de sa loi locale aux traitements mis en œuvre par la maison mère française.

L'animation du réseau est importante car ce sont les relais qui informent le CIL de toutes les collectes et traitements de données personnelles, ainsi que sur les éventuels flux transfrontaliers. La tenue du registre est indispensable car il est le reflet des traitements mis en œuvre et doit par conséquent répondre aux exigences légales et réglementaires de la CNIL, laquelle peut demander à le consulter. C'est le CIL qui demande à la CNIL les autorisations nécessaires pour certains traitements. Mais il rayonne aussi à travers son activité relationnelle et pédagogique sous forme de conseils, de recommandations, de formations internes, voire externes, d'interviews, de rédaction d'articles.

2. Selon vous quelles sont les évolutions d'une telle fonction tant au plan national qu'international ?

La proposition de loi des sénateurs Détraigne et Escoffier récemment votée en 1ère lecture par le Sénat voudrait rendre le CIL obligatoire en France. La réforme en cours de la directive communautaire de 1995 semble avoir le même objectif. Cette fonction, inconnue avant le 6 août 2004, a pris un formidable essor. Les CIL nouvellement nommés s'impliquent dans cette fonction essentielle et indispensable. Le CIL est un véritable expert, pivot de la conformité informatique et libertés de son entreprise. Le CIL interne est salarié de son entreprise dont il connaît les rouages et l'organisation. Il faudrait que cette fonction existe dans tous les pays ayant une législation sur la protection des données personnelles et que les missions et statuts des CIL internationaux soient au moins harmonisés à défaut d'être identiques.

3. Qu'avez-vous à dire aux entreprises qui ont encore des réticences à la désignation d'un CIL ?

Il ne faut pas hésiter à nommer un CIL. L'entreprise affirme ainsi une démarche qualité qui lui permet de mieux maîtriser et gérer ses nombreux traitements de données personnelles. Quant au CIL nommé, il va pouvoir s'investir dans un challenge passionnant. Le CIL a des contacts privilégiés avec la CNIL dont il est l'interlocuteur unique. Il peut aussi échanger, participer à des groupes de travail avec les CIL d'autres entreprises. Ces échanges lui permettent de mener à bien ses missions et d'assurer une veille juridique. C'est aussi l'occasion pour lui d'être un acteur de l'adaptation nécessaire de la législation sur les données personnelles aux nouvelles technologies qui évoluent sans cesse.

(*) http://www.areva.com/ ; (**) Association Française des Juristes d'Entreprise http://www.afje.org/ ; (***) Elle anime aux côtés de Maître Chloé Torres, le groupe de travail « CIL Groupes internationaux » de l'Association Française des Correspondants à la protection des Données à caractère Personnel, http://www.afcdp.net/