Compte rendu de la conférence du 10 février 2011

DONNÉES PERSONNELLES DANS L'ENTREPRISE : Protection ou Illusion ?

Master 2 Professionnel Droit du Multimédia et de l'Informatique
Université Paris 2 Panthéon-Assas
En partenariat avec l'Association Française des Juristes d'Entreprise

INTRODUCTION

Par Christophe RADÉ, Professeur à l'Université Montesquieu — Bordeaux IV

En guise d'introduction, il semble important de devoir fixer quelques pistes pour cadrer le sujet et de faire une présentation dynamique de la problématique, qui est celle de savoir si la protection des données personnelles est réelle ou bien une illusion. Il faut d'abord déterminer qui va être protégé et ce que l'on va protéger : on tente à travers la protection des données personnelles de protéger plusieurs choses, que ce soient les informations, les personnes, le secret des affaires ou l'entreprise en elle-même. Mais cette ambivalence des intérêts à protéger a pour conséquence une réelle diversité juridique.

On peut constater que cette protection n'est pas toute puissante et a parfois des difficultés pour assurer la fin qu'elle s'est fixée. En effet, l'entreprise est un lieu de danger pour les informations, car l'employeur a toujours besoin de connaitre certaines données personnelles pour gérer son entreprise, ne serait-ce que pour des questions de gestion de personnel. Certes, ce besoin a toujours existé mais dans la vision actuelle de la problématique, ce qui a changé, c'est que les données sont numérisées, stockées. Elles sont donc conservées de manière infinie et sont accessibles immédiatement. Paradoxalement, ces données qui sont nécessaires au fonctionnement de l'entreprise constituent une menace, non seulement pour les salariés, mais également pour l'entreprise elle-même : c'est le cas des données dont la révélation peut être une menace, notamment dans le cadre de la concurrence déloyale.

Du point de vue du droit du travail, le principe est celui de la protection, c'est un impératif premier, que l'on retrouve autant au niveau de la collecte de l'information qu'à celui de leur utilisation.

Pour la collecte tout d'abord, il y a des règles générales, ainsi que des règles spéciales concernant la protection des salariés édictées en 1992, qui reposent à la fois sur la connaissance de l'existence de ce dispositif de collecte par le salarié, sur un principe de pertinence des informations collectées, ainsi que sur un principe de nécessité et de proportionnalité.

Quant au stade de l'utilisation, le droit du travail s'efforce de mettre en place une frontière quasiment étanche entre la vie personnelle et la vie professionnelle des salariés : l'employeur ne peut fonder ses décisions sur la vie personnelle des salariés, et seules les données à caractère professionnel peuvent être exploitées.

Dans le cadre de la loi informatique et liberté, le régime mis en place par le législateur fait preuve d'une véritable sévérité, parfois dénoncée comme excessive, notamment quant aux sanctions. Les sanctions pour non-respect des dispositions relatives à la protection des données personnelles sont par exemple plus importantes qu'en cas de discrimination ou de harcèlement.

Il y a également des garanties d'application au plan civil. Sur le plan de la légalité de la preuve, il y a un principe de licéité : les données obtenues illégalement ne sont pas exploitables, on peut se référer par exemple à l'arrêt des « badgeuses » : la jurisprudence a refusé de tenir compte des informations récoltées par ce biais. On peut également citer ici le principe de la loyauté de la preuve, avec le principe selon lequel les données personnelles collectées ne peuvent être présentées en tant que preuve qui si elles sont collectées de manière loyale. Ce principe touche autant les données numériques que les données ordinaires.

Ce régime très protecteur laisse cependant place à l'utilisation des données collectées en entreprise. Le droit du travail est à la fois porteur d'idéaux mais extrêmement pragmatique, car il sait que les salariés peuvent user et abuser de cette protection instituée par la loi. Des garde-fous ont donc été prévus, comme, par exemple, la qualification des données sur le lieu de travail comme étant toutes présumées avoir un caractère professionnel. Certes cette présomption est simple et peut être renversée, mais elle fait tout de même reculer la protection des salariés.

On constate bien que même pour les données protégées, protection ne signifie pas immunité. Si on prend encore l'exemple des correspondances privées, l'employeur ne peut certes pas avoir un accès direct sans accord de son salarié, mais il peut avoir recours au juge pour y accéder par la voie de l'ordonnance sur requête.

Pour les autres données, il n'y a pas une telle protection. Pour les fichiers contenus sur le disque dur de l'ordinateur, même s'ils sont identifiés comme personnels, le salarié ne peut pas s'opposer à ce que l'employeur y ait accès, le seul droit qu'il a est celui d'être présent ou représenté lors de leur ouverture.

Des éléments de la vie personnelle ainsi obtenus peuvent justifier des sanctions sur le plan disciplinaire, comme un licenciement pour faute grave (il faut qu'il y ait un lien entre la vie personnelle du salarié et sa vie professionnelle). Même hors du plan disciplinaire, il y a une jurisprudence sanctionnant le trouble anormal apporté à l'entreprise par le salarié, alors même que le comportement litigieux aurait lieu dans sa vie personnelle.

En guise de conclusion, on peut affirmer que cette protection a une finalité : protéger l'exercice par le salarié de ses droits et libertés, sans que cette protection ne lui permette de faire n'importe quoi.

On peut donc constater qu'il y a une protection efficace, qui protège à la fois le salarié et l'entreprise, tout en apportant la nuance qu'évidemment « le droit ne peut pas tout » contre l'imagination de certains acteurs.

UTILISATION DES RÉSEAUX SOCIAUX PAR L'ENTREPRISE

Par François COUPEZ, Avocat Associé, Cabinet CAPRIOLI & Associés, Chargé d'enseignement à l'Université Panthéon-Assas Paris 2

Alors que l'utilisation des réseaux sociaux par les entreprises se généralise, les règles concernant la protection des données à caractère personnel sont parfois mises à rude épreuve, que l'entreprise soit confrontée aux réseaux sociaux les plus classiques ou qu'elle intègre les réseaux sociaux en son cœur (réseaux sociaux internes). En effet, ceux-ci ne deviennent depuis quelques années à peine rien de moins qu'une nouvelle composante de l'organisation du travail au sein de certaines entreprises. Or, dans tous les cas, l'employeur doit protéger des données à caractère personnel dont il assure le traitement (données de ses salariés, données de ses clients, etc.), que ce soit en vertu de la loi Informatique, Fichiers et Libertés du 6 janvier 1978 ou des règles issues du Code du travail.

Qu'est-ce qu'un réseau social ? Le regroupement par communauté d'intérêts d'une ou plusieurs catégories d'utilisateurs (certains réseaux sociaux peuvent avoir une approche très restreinte ou viser un spectre au contraire beaucoup plus large). Ces réseaux sont faits pour interagir, pour communiquer, pour échanger, ou parfois simplement se montrer. Il y a souvent une véritable exaltation de l'ego dans la manière dont les réseaux sociaux fonctionnent, qui vont inciter l'utilisateur à publier le maximum d'informations à caractère personnel le concernant. De façon paradoxale, compte tenu de l'importance de la protection des données à caractère personnel, l'utilisateur va souvent être amené à partager toujours plus d'informations sur le réseau social qu'il utilise (sans forcément le maîtriser) jusqu'à devenir l'éditeur de sa vie privée.

L'entreprise, quant à elle, est confrontée à un autre paradoxe, fondé sur l'attraction et la répulsion : elle va vouloir utiliser les réseaux sociaux pour valoriser et vanter ses produits, promouvoir son image ou encore recruter, mais elle va, dans le même temps, lutter contre la dissémination d'informations (souvent à caractère personnel) qu'elle détient et qui peuvent être mises en ligne, consciemment ou inconsciemment, par ses salariés.

Au plan juridique, notons que le groupe de travail dit de « l'article 29 » sur la protection des données définit les « services de réseautage social » dans son avis 05/2009 adopté le 12 juin 2009 comme des « plateformes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs ». Cette attention portée par le groupe de l'article 29 montre que l'analyse juridique de ces réseaux est souvent menée sous l'angle de la protection des données à caractère personnel. Or, si les problématiques sont communes, il n'en reste pas moins que les réseaux sociaux internes d'entreprise peuvent receler quelques spécificités.

I. Les réseaux sociaux comme sources d'information de l'entreprise

A. Pour permettre un recrutement

Pour l'entreprise, l'utilisation d'un réseau social regroupant une partie importante de ses clients ou prospects apparaît souvent pertinente d'un point de vue marketing (rappelons malgré tout que la plupart des réseaux sociaux encadrent très fortement voire interdisent purement et

simplement la publicité en leur sein dans leurs conditions générales d'utilisation). Mais le réseau social peut aussi représenter pour l'entreprise un vivier de talents à attirer ou à débaucher, en lui permettant spécifiquement de viser des profils bien précis.

Mais parallèlement, ces réseaux sont aussi des outils marketing à disposition du candidat, qui va chercher lui aussi à valoriser son image et parfois en mettant sa vie en scène en mettant en avant les aspects positifs de sa candidature et en gommant les aspects négatifs (« Personal Branding »). Face à ces pratiques, l'employeur qui cherche bien souvent à vérifier le profil et les références du candidat qu'elle souhaite recruter est conscient que les informations présentes sur LinkedIn ou Viadeo ne sont que la partie émergée de l'iceberg. Or, des métamoteurs de recherche permettent maintenant de rassembler toutes les informations disponibles en ligne sur une personne, réduisant au quasi néant le droit à l'oubli numérique que beaucoup appellent de leurs vœux (voir notamment la position de la CNIL ou la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique déposée au Sénat le 6 novembre 2009) : être le plus gros « fêtard » de sa promotion peut assurer une image positive auprès de ses amis étudiants, lorsque l'on est à la Faculté. Mais les photos des beuveries débridées présentées au futur recruteur, quelques années après, risquent d'avoir un tout autre effet…

Est-ce que la vérification de ces références par l'employeur est licite ? Quelles en sont les limites ?

La jurisprudence a eu l'occasion de rappeler que la vérification des compétences qui sont mentionnées sur le CV est à la charge de l'employeur. Or, celui-ci s'adaptant aux moyens modernes, vérifie de moins en moins en prenant contact directement avec ex-employeurs ou formateurs du cabinet et privilégie de plus en plus les ressources en ligne. D'où la tentation de prendre connaissance des pages figurant sur les SRS plus privés, du type Facebook, où l'on considère que les informations sur le candidat seraient plus représentatives de la personnalité réelle du candidat.

Pourtant, les principes de la loi de 1978 concernant notamment la transparence doivent être suivis, tout comme l'art. L. 1221-9 du Code du travail requérant l'information préalable du candidat sur les méthodes de collecte utilisées par l'employeur. Surtout, que peut faire l'employeur d'une information « compromettante » à ses yeux dont il aurait eu connaissance ? Car il doit également respecter les articles L. 1132-1 du Code du travail ou encore 225-2 du Code pénal réprimant la discrimination notamment à l'embauche. D'autant que le candidat peut par exemple savoir qui a consulté son profil et ainsi être plus facilement tenté d'agir en justice en démontrant que sa candidature a sans doute fait l'objet d'une discrimination. Ces consultations pouvant être l'œuvre de tout collaborateur de l'entreprise (et pas forcément le service officiellement chargé du recrutement). Une véritable formation de l'ensemble des collaborateurs devrait donc être effectuée par l'employeur pour éviter ce type de comportements, d'autant que le profil en question peut être celui d'un homonyme peu recommandable, voire que ce profil a été mis en ligne pour nuire à l'intéressé).

Les professionnels du secteur en tout cas s'engagent : 40 cabinets de recrutement ont signé le 12 novembre 2009 la charte d'autorégulation « Réseaux sociaux, internet, vie privée et recrutement » indiquant que les réseaux sociaux à orientation privée (Facebook, etc.) n'étaient notamment consultables dans le cadre d'un recrutement que si le candidat y invitait l'employeur. Quant au droit à l'oubli, certains réseaux sociaux ont signé la Charte du « droit à l'oubli dans les sites collaboratifs et les moteurs de recherche » le 13 octobre 2010 sous l'égide de Nathalie Kosciusko-Morizet.

B. Pour permettre une sanction ?

Face aux réseaux sociaux, tous n'ont pas les mêmes réflexes et l'on constate malheureusement que les hypothèses de salariés se moquant ouvertement des clients ou critiquant vertement leur employeur se multiplient (1 salarié sur 5 pour cette dernière hypothèse selon l'étude

« Salariés et médias sociaux » de la société Viavoice). La compagnie Singapour Airlines a ainsi été obligée de restreindre strictement l'utilisation de Facebook et Tweeter parmi ses personnels, ceux-ci ayant apparemment l'habitude de tweeter leurs commentaires peu amènes concernant leurs clients pendant les vols.

Incidemment, une problématique annexe se pose, qui sort du cadre de notre sujet et que je ne développerais pas pour cette raison ici : les propos tenus le sont-ils au nom de l'entreprise ou sont-ils propres au salarié ? Et si les propos sont tenus dans le cadre d'un groupe créé ou non au nom de l'entreprise, par un de ses salariés (ou de quelqu'un se faisant passer comme tel) ?

Une chose apparaît acquise : Facebook est l'hébergeur et, à ce titre, sa responsabilité ne peut être engagée qu'en conformité avec les règles posées par l'article 6 de la LCEN (voir par ex. ord. Réf. TGI Paris 24 novembre 2010).

Mais qu'en est-il de la preuve ? Comment l'employeur peut-il savoir que des salariés tiennent des propos désobligeants à son encontre ? En consultant par exemple le mur Facebook ouvert à tout vent à des « amis » qui ne l'étaient pas, comme dans l'affaire tranchée par le Conseil de prud'hommes de Boulogne Billancourt le 19 novembre 2010 ? Comment poser la limite entre sphères publique et privée dans un outil tel que Facebook ? A priori par la gestion du degré de confidentialité des pages, souvent dépendante en pratique de ce que nos « amis » eux-mêmes décident de communiquer à d'autres… sachant que les « amis » ne sont souvent au mieux que des connaissances, voire des collègues et plus seulement un cercle intime de proches qui gardent le secret sur nos débordements verbaux à l'encontre de notre employeur… ou de nos autres amis ! En effet, dans le cas de l'affaire précitée, c'est un autre salarié de l'entreprise qui a indiqué à l'employeur que trois salariés appelaient à la révolte contre leur hiérarchie.

De façon générale, les faits commis dans la vie personnelle du salarié peuvent être utilisés à l'appui d'un licenciement pour motif personnel (le trouble caractérisé que ces faits doivent alors générer constituant une cause réelle et sérieuse), ou pour fonder un licenciement disciplinaire, à la condition dans ce dernier cas que les faits fautifs se rattachent à la vie professionnelle du salarié. Dans le cadre de l'affaire citée ci-dessus, les propos protestataires et dénigrants avaient été tenus par des salariés de la direction des ressources humaines de l'entreprise, et pouvaient être consultés par des salariés de l'entreprise ou de possibles candidats du fait de la très large diffusion de la page, ce qui explique la position des conseillers prud'homaux. L'employeur doit toutefois prendre garde à l'interprétation des propos qui lui seraient rapportés : la Cour de cassation a plusieurs fois réaffirmé ces derniers mois que le salarié conserve sa liberté d'expression dans l'entreprise, ce qui peut justifier certains propos qui, s'ils sont critiques, ne seraient pas spécialement dénigrants ou diffamatoires (Cass. Soc. 10 nov. 2009 et 21 sept. 2010, v. également l'affaire du blog de « petite anglaise »).

II. Le réseau social (interne) d'entreprise… le meilleur des mondes ?

Le réseau social d'entreprise peut consister en un « annuaire + », une communauté interne relayant les messages institutionnels, un outil marketing ou encore un outil d'échange d'idées, de partage d'informations et de données, de communication en temps réel, qui, quand il est réellement utilisé, permet un réel gain de productivité. Raison pour laquelle les projets se multiplient en ce sens au sein des entreprises.

Reste qu'il ne faut pas le considérer avec le même regard que celui que l'on porte avec un SRS classique de type Facebook qui serait simplement internalisé. En effet, le réseau social se situe presque par nature à l'opposé du droit du travail, un antagonisme fort existant entre les valeurs prônées par le réseau social (relations directes, convivialité, centrage sur l'individu) et les règles du droit du travail s'articulant autour du pouvoir de direction de l'employeur (hiérarchie) ou encore de

son pouvoir disciplinaire. Il doit également y avoir une parfaite étanchéité entre informations personnelles et informations que l'employeur peut demander et connaître. Or le réseau interne d'entreprise étant à la croisée des chemins, un tel projet ne peut être mis en chantier sans mener les audits juridiques et prévoir des études préalables se fondant sur les fonctionnalités offertes, ainsi que les données collectées. Un encadrement par le biais de règles précises, ainsi qu'un accompagnement du projet dans le temps sont par ailleurs nécessaires, au fur et à mesure que les fonctionnalités s'étofferont. Sans maintien du cadre professionnel et sans une réflexion précise sur les fonctionnalités prévues par rapport au cadre juridique (principes de la loi du 6 janvier 1978, droit à l'image, etc.), l'employeur risque de se mettre de lui-même dans des situations difficiles (par exemple dans le cas d'un questionnaire « portrait chinois » de l'employé).

D'autres problématiques afférentes à la protection des données à caractère personnel doivent être identifiées et résolues dans le cadre de tels projets, tel que par exemple celle de la géolocalisation souvent intégrée dans ces outils (v. à ce sujet l'intervention de Johanna Carvais ci-après) même si elle est encore balbutiante, celle de l'utilisation de prestataires externes d'hébergement du réseau d'entreprise (souvent en mode SaaS, parfois dans le Cloud avec les questions désormais habituelles sur les flux transfrontières de données), ou encore celle du contrôle de l'activité du salarié que permet ces outils via les statistiques de consultation de la page, le nombre de connexions ou les contributions apportées (les règles du Code du travail doivent alors être respectées).

III. Réseaux sociaux et violation de données à caractère personnel

Dans un réseau professionnel, décrire son poste, ses dossiers, ses réalisations, c'est aussi parfois révéler des informations confidentielles aux concurrents, ce qui peut se révéler très préjudiciable pour l'entreprise (sa compétitivité, sa réputation, son image, voire son cours de bourse). C'est aussi parfois révéler des informations à caractère personnel sur des clients, alors que l'art. 34 de la loi du 6 janvier 1978 ou encore les différents secrets professionnels (médical, bancaire, etc.) imposent à l'employeur de protéger ses données.

L'entreprise doit agir pour rappeler les règles applicables à ses salariés trop prolixes de façon générale sur les réseaux sociaux, les former à cette problématique et réduire ses risques, d'autant que la modification de la directive 1995/46/CE concernant la protection des données à caractère personnel, prévues en 2011, imposera a priori une lourde obligation de notification aux entreprises en cas de divulgation, et donc de violation, de données à caractère personnel.

CIL ET PROTECTION DES DONNÉES PERSONNELLES DANS L'ENTREPRISE

Par Marie-Gaëlle CHOISY, Correspondant Informatique et Libertés, Direction juridique Groupe ORANGE – FT, Membre de l'Association Française des Juristes d'Entreprise (AFJE)

La réglementation sur la protection des données personnelles est essentiellement d'origine européenne. L'activité du groupe Orange France Télécom concerne les communications électroniques, qui est un domaine sur-réglementé en matière de protection. Dès l'origine le groupe Orange France Télécom a été très attaché à la protection des données personnelles. Les administrations étaient soumises à un régime d'autorisation et il fallait demander un avis auprès de la CNIL avant la mise en œuvre de chaque nouveau traitement.

La protection des données personnelles dans le groupe Orange est une réalité pleine et entière. Mais c'est aussi une illusion car sa dimension internationale permet de constater que beaucoup de pays n'ont aucun régime de protection et ne savent pas ce qu'est une donnée personnelle.

Le Correspondant Informatique et Libertés (CIL) d'Orange a été mis en place facilement. Dans les administrations sa présence était obligatoire. La réglementation découlait d'une circulaire du premier ministre qui employait déjà le vocable CIL. Ainsi, lorsque la directive de 1995 et la loi du 6 août 2004 ont instauré la fonction de CIL, le groupe Orange France a pu facilement s'adapter.

I. La réalité des traitements de données à caractère personnel d'une entreprise telle qu'Orange

Quelle est la réalité des traitements de données à caractère personnel dans une entreprise telle qu'Orange ?

A. Fichiers classiques relatifs aux clients et aux personnels

Il s'agit de traitements de données concernant tant le personnel que les clients. Il ne s'agit pas de fichiers classiques, car dans le domaine des communications électroniques beaucoup de données peuvent être qualifiées de personnelles.

La directive du 24 octobre 1995 a élargi considérablement la notion de données à caractère personnel. Antérieurement, le terme employé était celui de « données nominatives ». La directive a introduit la notion de « données à caractère personnel ». Le champ s'est alors élargi pour aller des coordonnées d'une personne à la voix, l'image et la biométrie notamment.

B. Spécificité des communications électroniques : un domaine particulièrement riche en données à caractère personnel

Les fichiers de clients sont très complexes. Numéros de téléphone, adresses électroniques, adresses IP, logs de connexion, données de trafic, données de navigation, données de géolocalisation etc.…**, c**onstituent des données à caractère personnel.

La loi définit en effet la notion de donnée à caractère personnel comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou

indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Concernant les traitements relatifs au personnel, le groupe Orange a utilisé dès l'origine les normes simplifiées de la CNIL, et notamment celles relatives à la paie du personnel et à la gestion proprement dite du personnel. Des déclarations spécifiques ont été faites au fur et à mesure au fil des évolutions techniques et juridiques, par exemple pour l'accès aux locaux par badge.

De plus, Orange effectue des enregistrements entre le service client et le client. C'est une finalité précise de coaching ou de qualité qui est visée. Le client est prévenu que la discussion est susceptible d'être enregistrée à cette fin. L'enregistrement de la conversation peut aussi avoir lieu afin de sécuriser la fourniture du service et de s'assurer du consentement du client. L'enregistrement permet à ce titre de confirmer la commande du produit ou service par le client.

II. La protection de ces données dans un groupe mondial, illusion au niveau international

A. Réglementation essentiellement européenne assortie d'une sur réglementation dans le domaine des communications électroniques

La protection des données à caractère personnel se trouve dans un corpus de règles européennes assorties d'une sur-réglementation dans le domaine des communications électroniques via la directive dite « vie privée et communications électroniques ». Cette sur-réglementation n'est pas indispensable. Les grands principes de la loi Informatique et Libertés, repris de la directive de 1995, suffisaient amplement pour mettre en place de nouveaux services comme la présentation de l'identification de la ligne appelante ou le service d'annuaire inversé (connaitre l'identité d'une personne avec son numéro).

B. Interdiction des transferts de données hors UE, sauf exceptions

Cette réglementation existe à l'intérieur de l'Union européenne où les transferts de données personnelles sont libres. En revanche, le transfert des données à caractère personnel est interdit par principe hors de l'Union européenne. Il existe cependant des exceptions à cette interdiction comme le principe du consentement exprès de la personne. Par exemple, en matière de recherche et de développement, les personnes qui font partie du panel signent un accord dans lequel elles s'engagent à avoir pris connaissance des modalités concernant les expérimentations et consentent à ce que leurs données puissent être transférées hors de l'Union européenne. Il est également possible de déroger à cette interdiction en signant des contrats types établis par la Commission de l'UE pour certaines activités pérennes de l'entreprise, comme le transfert de données clients vers des prestataires hors UE (par exemple en Inde pour des prestations techniques un peu pointues).

Le transfert hors UE de ces informations nécessite une autorisation de la CNIL, ce qu'Orange a obtenu. C'est quelque chose de complexe à mettre en place pour une grande entreprise, mais Orange étant un groupe européen, il y a moins de transferts à effectuer qu'un groupe situé aux États-Unis par exemple. La directive européenne en cours de modification pourrait se pencher sur un assouplissement des règles de transfert hors UE.

C. Quid de la protection hors UE : vers une convention internationale ?

Au niveau international, beaucoup de personnes voyant que des entreprises comme Google ne sont pas assujetties aux règles de protection de données personnelles militent pour des normes internationales. Il existe une Résolution de Madrid en 2009 qui a adopté des standards

internationaux, ainsi qu'une Résolution de Jérusalem en 2010 qui prône la mise en place d'un instrument juridique international.

D. Quid de l'harmonisation des règles au sein même de l'UE : une reconnaissance mutuelle ?

Tous les États membres de l'Union européenne disposent d'une loi informatique et libertés et d'une CNIL. Lorsqu'un projet mondial est envisagé, il faut alors demander l'avis de chaque CNIL nationale concernée. Or, ce processus peut être assez long. Il faudrait harmoniser davantage les législations des États membres, et peut-être adopter un principe de reconnaissance mutuelle : si un traitement a été approuvé en France, cette approbation serait valable dans les autres États membres.

Peu d'États membres ont prévu la fonction du CIL dans leur législation. Elle existe en Suède, aux Pays-Bas, au Luxembourg et en France (où la fonction est facultative) ainsi qu'en Allemagne, (où la fonction est obligatoire).

III. Désignation du CIL d'Orange : nouveauté dans la continuité

A. Un CIL historique avant l'heure dès 1982 conservé au cours des différents changements de statut de France Télécom devenue société anonyme

Orange est le seul opérateur de communications électroniques à avoir un CIL. C'est un CIL historique désigné dès 1982 suite à une circulaire du premier ministre pour les administrations. Compte tenu des enjeux médiatiques de la protection des données à caractère personnel, la fonction a été conservée au cours des différents changements de statut de France Télécom devenue société anonyme.

B. Un CIL officiel mutualité à compétence étendue désigné depuis 2006 auprès des comités d'entreprise et de la CNIL

Il s'agit d'un CIL officiel mutualisé à compétence étendue, désigné depuis 2006 auprès des comités d'entreprise concernés et de la CNIL. En effet, il exerce ses fonctions à la maison mère ainsi que pour d'autres filiales du groupe et agit dans tous les domaines de l'entreprise. Le CIL doit avoir une bonne connaissance de l'entreprise et fonctionner en réseau. Le CIL d'Orange est expert en droit de l'informatique et du multimédia et est rattaché directement au directeur juridique groupe.

Dans la mesure où le traitement de données à caractère personnel est très présent dans le domaine des communications électroniques, le CIL doit savoir trouver les bons interlocuteurs au sein de l'entreprise.

C. Un intermédiaire dédié à la protection des données personnelles pour l'entreprise et pour la CNIL.

Le rôle du CIL est celui d'un intermédiaire dédié à la protection des données personnelles à la fois pour l'entreprise et pour la CNIL, chargé de diffuser la culture « informatique et libertés » au sein d'Orange et d'établir des relations constructives et pérennes avec la CNIL.

Entre le CIL officieux d'il y a 20 ans et le CIL officiel d'aujourd'hui il n'y a pas beaucoup de différences. Le CIL entretenait déjà des relations suivies avec la CNIL.

IV. Rôle et missions du CIL d'Orange, illusion devenue réalité

A. Une apparence de « mouton à 5 pattes » mais une fonction officiellement reconnue par la loi ainsi qu'en interne et à l'extérieur

La loi française a prévu que le CIL peut être licencié à la demande de la CNIL. Mais l'employeur ne peut pas le licencier du fait de l'accomplissement de ses missions, alors même qu'il n'est pas protégé par le droit du travail. De plus, les entreprises le considèrent comme l'œil de la CNIL au sein de l'entreprise.

Tout de même, depuis que cette fonction officielle a été mise en place, elle est beaucoup plus reconnue dans l'entreprise. Avant, le CIL était un juriste parmi d'autres. À présent il a plus d'assises, ce qui a également bénéficié à la protection des données à caractère personnel.

B. Un rôle de conseil et de définition de la politique d'Orange en matière de Privacy

Le CIL a également un rôle de conseil et définit la politique d'Orange en matière de Privacy.

Néanmoins, beaucoup de personnes ne veulent pas être nommées par peur d'une responsabilité pénale étendue en raison du nombre de traitements dans l'entreprise. Cette crainte expliquerait qu'il y ait peu de CIL dans le domaine des communications électroniques. La présence du CIL donne pourtant une bonne image de marque pour l'entreprise, et permet de façon efficace de détecter quels sont les nouveaux traitements sensibles, de donner des avis et des alertes.

C. Une centralisation bénéfique pour une meilleure application des règles grâce aux missions de gestionnaire des registres de déclarations des traitements de l'entreprise et de gestionnaire des plaintes, bon baromètre pour détecter les dysfonctionnements et y remédier.

Enfin, le CIL centralise toutes les plaintes, ce qui est important pour savoir s'il y a des dysfonctionnements dans tel ou tel système.

Lorsqu'il n'y avait pas de centralisation, des plaintes étaient envoyées à l'entreprise par la CNIL sans que le CIL en ait obligatoirement connaissance. Le même problème se posait en matière de déclarations qui étaient parfois effectuées à l'insu du CIL. Cette décentralisation était beaucoup moins évidente à gérer.

Outre le fait que l'entreprise est dispensée de déclarations auprès de la CNIL, lorsqu'elle a désigné un CIL, elle a moins de risques que tel ou te traitement n'ait pas été déclaré à la CNIL en temps voulu, ce qui était une hantise auparavant. Il est en effet beaucoup plus souple de pouvoir effectuer et modifier les déclarations dans les registres du CIL, au fur et à mesure que les traitements sont mis en œuvre et renouvelés.

D. Un rôle de recommandation et d'alerte auprès d'Orange

Le rôle du CIL est aussi de faire des recommandations et d'alerter lorsqu'il y a un problème dans l'entreprise. En effet, même s'il y a un CIL, la CNIL peut faire une enquête. D'ailleurs, il est prévu, dans le programme annuel de la CNIL de 2011 d'effectuer une enquête sur les CIL.

E. Un rôle de relai et d'interlocuteur privilégié auprès de la CNIL

Les rôles respectifs de la CNIL et du CIL sont complémentaires, et on s'aperçoit en discutant qu'on peut toujours améliorer et faire progresser la protection des données personnelles dans l'entreprise.

Conclusions : quel devenir pour le CIL et la protection des données personnelles ?

Dans un grand groupe, la principale difficulté est l'absence de CIL officiel dans les autres pays européens. Il est alors difficile de ne pas avoir un point d'entrée fixe pour la question des données personnelles.

Des chartes de protection des données à caractère personnel se multiplient dans les entreprises, dans le groupe, afin de diffuser la culture de la loi Informatique et libertés. Mais ce n'est pas évident, surtout dans les pays africains où tout est absolument nouveau. Il faut faire preuve de pédagogie et expliquer de quoi il s'agit. Pour un groupe d'entreprises comme Orange la protection des données à caractère personnel est un vrai plus. Il faut protéger le client et le personnel.

Le rôle du CIL est d'aider à diffuser la culture informatique et libertés.

Faut-il ainsi aller vers une fonction obligatoire du CIL dans la future directive européenne ? Cette obligation concernerait non seulement la France où la fonction de CIL est facultative mais aussi les autres États membres, à l'instar de l'Allemagne. Quid des États hors de l'UE et notamment du rôle du CPO (Chief Privacy Officer) ?

Faut-il aller vers une convention internationale sur la protection des données à caractère personnel ? Un premier pas a été fait avec la résolution de Madrid du 5 novembre 2009 portant adoption de standards internationaux en matière de Privacy et avec la résolution de Jérusalem du 28 octobre 2010 rappelant l'urgence d'une telle convention et appelant à la convocation d'une conférence internationale sur le sujet dès 2011. Ce sujet sera d'ailleurs probablement à l'ordre du jour du prochain G8.

Questions

La fonction de CIL est-elle envisageable vraiment pour une PME ou est-ce une fonction pour les grands groupes ?

M-G Choisy : il s'agit plutôt d'une fonction pour les grands groupes.

J. Carvais : Dans les grands groupes, les CIL ont une fonction différente que dans les petites structures. C'est une fonction à plein temps. Mais les CIL interviennent dans les PME. C'est conciliable avec la protection des données. Au-delà de l'exonération des formalités de déclaration normale, il y a un double avantage pour les PME : une mise en œuvre rapide des traitements (on peut mettre en œuvre le traitement dans la minute qui suit la déclaration), un avantage marketing.

Que pensez-vous du projet de modification de la loi tendant à rendre obligatoire la nomination d'un CIL ?

M-G Choisy : La question a été posée dans les consultations publiques concernant la directive-cadre. Imposer la présence d'un CIL n'est pas forcément une bonne idée. Elle devrait rester une simple faculté. La grande majorité des États membres n'a pas prévu d'en avoir dans leur propre loi. Il

faudrait donc au moins que dans les lois des États membres il y ait la possibilité d'avoir un CIL à titre facultatif. La rendre obligatoire dans des PME n'est peut-être pas souhaitable.

Le CIL n'est pas un salarié protégé. Est-ce qu'il devrait l'être vu ses fonctions ?

M-G Choisy : Non, le CIL reste un salarié à part entière de l'entreprise. La ressemblance avec un délégué du personnel n'existe pas.

C. Radé : il n'y a pas de rapport d'antagonisme entre les fonctions du CIL et celles de l'employeur. Les représentants du personnel prennent des risques dans leur fonction. Ce n'est pas le cas du CIL.

F. Coupez : en pratique, si le CIL devenait un salarié protégé, il faudrait imposer la nomination d'un CIL car les employeurs ne voudraient pas en employer un.

GÉOLOCALISATION DES SALARIÉS

Par Johanna CARVAIS, Juriste aux affaires Juridiques de la CNIL

Une bonne compréhension des problématiques de la géolocalisation nécessite de définir préalablement la notion de géolocalisation. L'exposé présentera ensuite le cadre juridique et la position de la CNIL en la matière. L'intervention portera sur la géolocalisation du véhicule et abordera ainsi le cas précis des systèmes embarqués dans les véhicules mis en place par les assureurs et les constructeurs.

Cependant, la géolocalisation peut passer par beaucoup d'autres moyens comme par le téléphone. Mais dans la sphère professionnelle, les dispositifs de géolocalisation sont surtout mis en place via les véhicules.

I. La notion de géolocalisation

Une donnée de géolocalisation a une définition précise donnée par la directive de 2002 « vie privée et communications électroniques » (art. D. 2002/58/CE). Cette dernière la définit comme « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessibles au public* »

Une donnée de géolocalisation est obtenue grâce au satellite via le système GPS (Global Positioning System) mis au point par l'armée américaine. Les données de localisation sont calculées par trilatération. C'est une technologie utilisée depuis plus de dix ans pour le civil.

Comment ça marche ?

Le boitier embarqué envoie des informations au satellite qui renvoie au boitier sa position géographique. La donnée va ensuite être communiquée à l'employeur via des réseaux de communication électroniques (GSM/GPRS).

II. Le cadre juridique spécifique à la géolocalisation des salariés

Le cadre juridique se compose des textes suivants :

- Les directives européennes : 95/46/CE du 24/10/1995 relative à la protection des données personnelles ; 2002/58/CE du 12 juillet 2002, directive vie privée et communications électroniques (article 34-1 IV du Code des postes et des communications électroniques) ;
- La loi informatique et liberté du 6 janvier 1978 modifiée en août 2004 ;
- L'article L.1121-1 du Code du travail : « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ».
- L'avis 5/2005 du G29 sur l'utilisation des données de localisation aux fins de fourniture de services à valeur ajoutée adopté le 25 novembre 2005

Ce cadre juridique est clair. Lorsque l'employeur collecte, utilise, conserve ces informations, il met en place un traitement. Dès lors, la loi Informatique et libertés s'applique

III. La position de la CNIL

A. La position de la CNIL sur la géolocalisation des salariés via les véhicules mis à leur disposition.

La position de a CNIL se traduit par une délibération de la CNIL n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public (position calquée sur celle adoptée au niveau européen par le G29).

Le 23 juillet 2009, la CNIL a réexaminé cette délibération afin de préciser certaines notions. Elle n'a pas, pour autant, modifié sa délibération de 2006. Elle a simplement constaté qu'elle avait un nombre de plaintes important, sans pouvoir dégager une doctrine claire sur les déplacements libres des salariés.

B. La position de la CNIL sur les finalités

La loi Informatique et libertés impose de déterminer la finalité de chaque traitement. Pour la géolocalisation des salariés, ces finalités peuvent être la gestion en temps réel des interventions auprès des clients, le suivi des marchandises en raison de leur nature particulière (matières dangereuses, produits alimentaires, etc.), la lutte contre le vol de véhicules, l'assistance de navigation, ou encore le suivi de l'activité des employés. La recommandation précise que cette dernière finalité est acceptée si elle est accessoire et qu'il n'existe pas d'autres systèmes pour contrôler l'activité du salarié. Un système de badgeuse, beaucoup moins intrusif, pourrait être envisagé pour le contrôle de l'activité des salariés par exemple.

Un employeur qui utiliserait un dispositif de géolocalisation pour contrôler l'activité de ses employés, alors que la finalité initiale du traitement est la lutte contre le vol, commettrait un détournement de finalité puni par le Code pénal de 5 ans d'emprisonnement et de 300 000 euros d'amende.

C. La position sur la proportionnalité du dispositif.

La CNIL rappelle qu'on ne peut pas géolocaliser un employé qui dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP…). Elle a réexaminé cette question le 23 juillet 2009. L'employé qui dispose d'une liberté dans l'organisation concerne les salariés disposant de manière certaine d'une liberté d'organisation de leurs déplacements professionnels, avec un véhicule de service ou de fonction. Cela signifie que le salarié organise sa journée de travail et ses déplacements auprès de ses clients ou fournisseurs de manière libre, l'employeur étant informé postérieurement par le salarié de son activité du jour ou de la semaine.

D. La position de la CNIL sur le contrôle des salariés

Le contrôle permanent des salariés est interdit. La CNIL recommande une fonction de désactivation. Comment utilise-t-on cette fonction de désactivation ? La fonction de désactivation doit également être prévue sur les systèmes embarqués dans les véhicules de service dans la mesure où l'employeur a laissé une tolérance d'utilisation à des fins privées (exemple : trajets domicile-travail).

La CNIL laisse libre l'employeur de fixer sa manière de désactiver les dispositifs.

La désactivation doit avoir lieu à l'issue du temps de travail et lors des temps de pause.

Enfin, il ne peut y avoir de géolocalisation des employés investis d'un mandat électif ou syndical lorsqu'ils agissent dans le cadre de l'exercice de leur mandat.

E. La position de la CNIL sur les données collectées.

Les données collectées sont nombreuses : le nom de l'employé, l'immatriculation du véhicule, les kilomètres parcourus, les temps d'arrêt, la vitesse moyenne, les données de géolocalisation…

Le focus doit être fait sur la vitesse. En effet, il n'est pas possible pour un employeur, organisme privé, de collecter une donnée relative à une infraction (art. 9 loi informatique et libertés). Ainsi, l'employeur ne peut pas collecter une vitesse maximale susceptible de faire apparaître une infraction au Code de la route, mais seulement une vitesse moyenne.

F. La position de la CNIL sur la durée de conservation.

La durée de conservation doit être adéquate au regard de la finalité. Si l'objet du dispositif est l'optimisation des tournées, le traitement des données de géolocalisation doit se faire en temps réel : il n'y a pas de conservation. Si le dispositif de géolocalisation a été mis en place pour contrôler l'activité des salariés, la CNIL recommande que ces données ne soient conservées que 2 mois maximum.

Il y a des exceptions à des fins de preuves. La conservation est d'un an si elle est nécessaire à des fins de preuve des interventions effectuées, lorsqu'il n'est pas possible de rapporter la preuve de cette intervention par un autre moyen. La durée de conservation est de 5 ans pour les données relatives aux horaires effectués dans le cadre du suivi du temps de travail.

G. La position de la CNIL sur l'information des personnes.

La recommandation va plus loin que les textes concernant les obligations d'information des personnes. L'article 32 de la loi Informatique et liberté ne précise pas les modalités d'information, c'est à dire la manière dont il faut informer. Il exige simplement l'information des salariées. Un affichage dans les locaux est-il suffisant ? Faut-il porter l'information dans le contrat ? Un mail suffit-il ?

La CNIL recommande une information individuelle (note d'information, affichage dans l'habitacle des véhicules…).

Les manquements à l'obligation d'information sont sanctionnés dans le Code pénal. Il s'agit de contraventions de 5^{e} classe. En cas de défaut d'information, l'employeur ne peut pas utiliser les données de géolocalisation d'un salarié pour démontrer le caractère justifié d'un licenciement (cf. CA Dijon 14/09/2010).

IV. Les nouvelles finalités de la géolocalisation des salariés.

A. la lutte contre le vol, l'éco-conduite, l'appel d'urgence

Les dispositifs de géolocalisation sont mis en place par les assureurs et les constructeurs essentiellement pour la sphère privée. Mais l'utilisation de ces systèmes présente un intérêt pour l'employeur.

La géolocalisation peut présenter un intérêt en matière d'infotrafic, de lutte contre le vol (tracking). Concernant ces derniers, la commission a validé une telle utilisation mais a attiré l'attention sur certains risques. Afin d'éviter toute justice privée, en cas de vol elle attire l'attention sur les personnes pouvant avoir accès aux données, les propriétaires des véhicules ne doivent pas avoir connaissance des informations issues du boitier.

L'éco-conduite se développe également. Il y a un intérêt pour l'employeur à connaitre la méthode de conduite de son employé. Une conduite « sportive » consomme davantage.

Enfin, les services d'e-call (appel d'urgence) représentent une nouvelle finalité intéressante pour l'employeur. Le dispositif de géolocalisation se déclenche manuellement ou automatiquement. La désactivation ne peut être imposée, dès l'instant que ce système aura été acquis librement, et que le propriétaire du véhicule se sera engagé à en informer les utilisateurs du véhicule ainsi équipé.

B. Le PAYD (« Pay As You Drive »)

Concernant les systèmes embarqués dans les véhicules mis en place par les assureurs et les constructeurs, la CNIL a pu se prononcer au sujet du PAYD. Le dispositif permet dans ce cadre de vérifier le kilométrage, le temps de conduite et les périodes de conduite afin de moduler le calcul des primes d'assurance

En 2005, la CNIL a refusé le traitement de la MAAF pour deux motifs. D'abord, il permettait le traitement des infractions avec la collecte de la vitesse. Ensuite, cette localisation était de nature à porter atteinte au principe d'aller et venir anonymement dans des proportions injustifiées).

En 2010, outre l'exclusion du traitement d'infraction, la CNIL insiste, dans sa recommandation de la CNIL 2010-096 du 8 avril 2010, sur deux éléments :

- le consentement éclairé des intéressés (puisque ces dispositifs de calcul de prime ne prévoient pas de fonction de désactivation).
- l'agrégation des données de localisation au niveau des boitiers, afin de limiter la remontée de ces informations au prestataire.

Questions :

Qui contrôle la désactivation ?

Plusieurs systèmes sont envisageables : plages horaires prédéfinies (pendant ces périodes, la géolocalisation ne remonte pas vers les serveurs), un bouton de désactivation dans les véhicules… La CNIL a ensuite la possibilité de contrôler l'employeur.

CLÔTURE DE LA MATINÉE

Par Jérôme HUET, Professeur à l'Université Panthéon-Assas Paris 2, Directeur du CEJEM et du Master 2 Professionnel Droit du Multimédia et de l'Informatique (M2 DMI)

Il faut remercier les étudiants qui ont organisé cette manifestation qui s'inscrit avec beaucoup de brio dans le cycle des conférences du DMI mais également les orateurs qui nous ont instruits sur la géolocalisation et les réseaux sociaux. Comment parler sur le sujet quand on n'est ni employeur, ni salarié, ni inscrit à aucun réseau social ? Cela rend difficile la conclusion de cette matinée. L'orateur français aime dire qu'il n'est pas qualifié, l'orateur américain lui aime commencer par une plaisanterie pour détendre l'atmosphère.

On a beaucoup appris ce matin bien que certaines choses aient été oubliées. L'entreprise est un gigantesque consommateur de données, mais pas seulement de données sur les salariés qui ont concentré la plupart de notre attention ce matin : l'entreprise collecte également des données sur ses clients. Or, le clientélisme de l'entreprise est sans limite, ainsi que son illégalité : l'entreprise truffe notre ordinateur de cookies variés pour mieux connaitre ses clients, et c'est totalement illégal. La CNIL le dit peu et se concentre sur une protection dont certaines entreprises, dont les banques, se moquent. Le cookie, c'est une intrusion dans un système de protection de données. Cela rejoint sur ce point l'opinion du professeur Radé : les immenses sanctions de la loi informatique et libertés ne doivent pas faire peur, car elles ne sont jamais appliquées… aller mettre en prison pendant 8 ans un chef d'entreprise, c'est ridicule et parait peu probable. Tout au plus peut on infligera une peine d'amende. Et sur ce point, il faudrait y aller plus fort, particulièrement pour les banques sur lesquelles les amendes n'ont que peu d'impact.

Il faudrait généraliser le CIL, qui était jadis appelé correspondant à la protection des données : est-ce que les pays qui n'en ont pas pourraient en faire un ? Il n'y a pas d'inconvénient pour les entreprises à spontanément créer ce poste.

Ce dont on a peu parlé, c'est le Whistle Blowing : le fait que les employés se dénoncent entre eux, l'alerte professionnelle. On s'arrange que les employés se battent entre eux pour mieux les dominer. La CNIL a réussi à limiter les dégâts causés par les États-Unis, puis repris par l'Angleterre, qui ont pour philosophie que tout le monde peut dénoncer tout le monde, notamment sur le plan de la vie privée. La CNIL a dit que seules les données comptables, bancaires, financières peuvent être collectées et ne pouvaient être conservées que pour un temps limité, puis effacées en l'absence de poursuite.