Les Smartphones au regard du Droit des Personnes

publié le **05/10/2010**, vu **3925 fois**, Auteur : Murielle Cahen

Un smartphone, ou « téléphone intelligent » est un téléphone mobile disposant des capacités d'un téléphone portable habituel, mais aussi des fonctions d'un assistant numérique personnel. Il peut aussi fournir les fonctionnalités d'agenda, de calendrier, de navigation Web, de consultation de courrier électronique, de messagerie instantanée, de GPS, etc.

Un smartphone, ou « téléphone intelligent » est un téléphone mobile disposant des capacités d'un téléphone portable habituel, mais aussi des fonctions d'un assistant numérique personnel. Il peut aussi fournir les fonctionnalités d'agenda, de calendrier, de navigation Web, de consultation de courrier électronique, de messagerie instantanée, de GPS, etc.

Ce type de téléphone portable peut également permettre d'installer des applications additionnelles sur l'appareil. Les applications peuvent être développées par le fabricant, par l'opérateur ou par n'importe quel autre éditeur de logiciel. La forte valeur ajoutée d'un smartphone est donc sa logithèque.

Aujourd'hui, les plus répandus sont les Iphones d'Apple, les Blackberrys de RIM, ou encore les « Androids » de Google. Les smartphones sont véritablement en vogue et proposent bien entendu des applications et des services variés, dont beaucoup ne se méfient pas. En l'occurrence, le pistage (géolocalisation GPS) et pertes de données inquiètent particulièrement la Cnil.

Alors, peut-on être pisté lorsqu'on utilise un smartphone ou certaines de ses applications ? Et comment protéger les consommateurs ?

A cet égard, il conviendra d'abord d'exposer les risques liés à l'utilisation d'un smartphone (1), pour ensuite en déduire des moyens de protection (2).

Géolocalisation et smartphone : l'obligation de vigilance de l'utilisateur

Quels sont donc les risques vis-à-vis de la vie privée du possesseur d'un smartphone (A) ? Et dans quelle mesure la vie privée peut-elle être limitée (B)

Les risques relatifs à la vie privée de l'utilisateur

Les Smartphones récents sont pratiquement tous équipés d'une puce GPS. Il est ainsi techniquement possible de pister un téléphone. Il existe par exemple des applications, nommées « trackers », permettant de localiser très précisément son téléphone en cas de perte, celui-ci transmettant des e-mails avec ses coordonnées GPS. La localisation permise est très précise.

Néanmoins ces applications doivent être installées et activées par les utilisateurs, ce qui réduit le risque d'une utilisation malveillante. Reste que le smartphone est donc potentiellement un « mouchard » en tant que tel.

Il existe également un risque de vol d'informations personnelles (localisation, mails, contacts, pièces jointes, donnés bancaires …) si l'utilisateur installe des applications malveillantes qui accèdent aux données du téléphone.

Il existe également un risque « marketing », notamment en raison du concept de « réalité augmentée » qui prend de plus en plus de place dans notre société, en mêlant images virtuelles et réelles.

Par ailleurs, les « trackers » (applications utilisant la géolocalisation pour « pister » un utilisateur via son numéro de mobile) sont sources d'autres conflits pour la vie privée des possesseurs de smartphones. D'abord du point de vue familial, mais également vis-à-vis de son employeur. Ainsi, il existe un risque potentiel qu'une personne puisse « suivre » son conjoint grâce au « tracker » placé dans son téléphone mobile à son insu.

Enfin, il existe également un risque lié à l'employeur. En transposant la situation familiale, au monde de l'entreprise, il est parfaitement envisageable qu'un employeur utilise la géolocalisation du smartphone de l'un de ses collaborateurs pour savoir sa situation exacte, ce qu'il fait durant son temps de travail, s'il est bien à son poste ou non, ce qu'il peut faire en déplacement professionnel etc.

La tolérance à l'égard des risques : la vie privée limitée au profit de la sécurité

Le recours à un système de géolocalisation ne doit pas contribuer à une filature électronique. Les dispositifs et logiciels de géolocalisation, tels les « trackers », permettent en effet une traçabilité des déplacements des conducteurs des véhicules professionnels. Ici encore, une entreprise suspectant des salariés commerciaux, amenés à effectuer de nombreux déplacements, pourrait être tentée de les « tracer » pour connaitre ainsi leurs moindres faits et gestes.

De tels dispositifs pouvant entraîner des risques d'atteinte à la vie privée des salariés, la CNIL a été conduite à encadrer leur mise en œuvre et a dégagé des conditions : désormais, la mise en place du système de géolocalisation peut faire l'objet d'une déclaration simplifiée si elle est conforme aux conditions posées par la norme n° 51 ; les personnes concernées doivent faire l'objet d'une information préalable ; et, la mise sous surveillance permanente des déplacements des salariés est justifiée lorsque l'activité du salarié est principalement itinérante.

A ce sujet, une surveillance systématique des déplacements du salarié via la mise en œuvre d'un dispositif de GPS/GSM peut être assimilée à une filature électronique disproportionnée par rapport aux intérêts légitimes de l'employeur. C'est ce qu'a indiqué, la Cour de cassation dans une décision du 26 novembre 2002 (Cass. soc., 26 nov. 2002, Montaigu Meret c/ SA Wieth-Lederle).

Il demeure que l'utilisation de tels moyens risque fort de porter atteinte aux libertés du salarié et particulièrement à sa vie privée. Une jurisprudence désormais établie considère en effet que ce dernier a droit au respect de sa vie privée au temps et au lieu de travail ; or, la sauvegarde de la sécurité du salarié peut malgré tout entraîner la mise en place de mesures restreignant significativement sa vie privée. Dans une décision du 31 mai 2007 (CA Rennes, 31 mai 2007, ch. prud'h. 8, 31 mai 2007, Delmon c/ SA DCN Log), la cour d'appel de Rennes a en effet considéré qu'était légal le licenciement d'un salarié, envoyé en mission en Arabie Saoudite, qui refusait de respecter les consignes de sécurité imposée par son employeur restreignant les conditions de séjour et de déplacement de ses salariés.

Les impératifs de sécurité peuvent donc permettre d'écarter la vie privée d'un salarié détenteur de smartphone. Aujourd'hui, les entreprises qui en fournissent à leurs collaborateurs sont légion. Il faudra donc veiller à ce que ce soit bien la sécurité qui mène à la surveillance des salariés, et non un but illégitime de contrôle de leurs activités et déplacements.

La nécessité de protéger le consommateur

La Cnil a rappelé en 2010 que les consommateurs détenteurs de smartphones devaient se prémunir contre les risques précédemment évoqués (A), et a particulièrement ciblé les Blackberrys concernant la sécurité (B).

La protection des utilisateurs de smartphones

Après avoir adopté, le 16 mars 2006, une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules utilisés par les employés des administrations et des entreprises, la Cnil a poursuivi sa réflexion générale sur les traitements de géolocalisation, envisageant notamment ceux qui sont opérés par liaisons avec des téléphones portables.

Pour se prémunir de les risques évoqués, le premier réflexe à avoir est de faire attention aux applications que l'on installe sur son téléphone ; il faut aussi lire en détail les conditions d'utilisation. Dans un contexte professionnel, les administrateurs ont la possibilité de limiter l'installation des applications à celles autorisées par l'entreprise. Et surtout, tous les utilisateurs doivent garder à l'esprit qu'un téléphone portable peut facilement se perdre, et qu'il doit donc impérativement être protégé par un code de verrouillage, après une courte période d'inactivité. Le code PIN de la carte SIM ne suffit pas.

Aussi, les fabricants de Smartphones s'engagent désormais vis-à-vis des applications disponibles sur leurs systèmes car bien évidemment les contrats qui lient les développeurs d'applications et les fabricants encadrent les collectes de données personnelles. Apple par exemple analyse les applications avant diffusion sur l'Appstore et a la possibilité d'effacer les applications à distance en cas de besoin.

Ainsi, la Cnil, consciente du « danger » entourant les smartphones, a agi avec pragmatisme en encadrant directement leur faculté à permettre la surveillance, le contrôle, voire même la filature de leurs utilisateurs.
Elle a néanmoins pointé particulièrement les Blackberrys comme « sujets à risques ».

Le Blackberry dans la ligne de mire de la Cnil

Les Blackberrys sont les téléphones les plus répandus dans le monde professionnel, par rapport aux autres Smartphones. Ils sont très appréciés dans le monde de l'entreprise pour leur capacité à

recevoir des mails. Ils permettent également la consultation de pièces jointes. Pour cela, la plateforme RIM fait transiter les informations par le réseau du fabricant. Cette façon de faire est spécifique à RIM. En effet, les autres fabricants de smartphones ne font pas transiter les informations par leur propre réseau.

Les informations transmises depuis un BlackBerry transitent ainsi par les serveurs de leur fabricant. Une polémique a d'ailleurs éclaté en 2007 sur le fait que RIM pouvait potentiellement accéder aux informations et même les transmettre à la NSA, l'agence de renseignement américaine en charge des communications électroniques.

Néanmoins, il est permis de s'interroger sur cette curieuse accusation à l'égard du fournisseur canadien. Parmi tous les smartphone du marché, seul le BlackBerry de RIM est pointé du doigt par la Cnil, alors que les autres smartphones sont tous aussi potentiellement nuisibles pour la vie privée des personnes.