Protection des données personnelles et moteurs de recherche: quels sont les réels enjeux?

Au cours de l'été 2007, les principaux moteurs de recherches sur internet 1 ont réalisé des annonces majeures pour la protection de la vie privée des internautes. Les délais de conservation de certaines informations enregistrées dans les systèmes à l'occasion des requêtes par mots clés seront considérablement réduits. Seraient concernées par ces mesures les informations produites à l'occasion des recherches effectuées par les usagers, telles que les mots clés, les données de connexions des usagers aux serveurs (logs permettant une traçabilité technique globale) mais également les témoins de connexion (cookies permettant une traçabilité technique précise).Cette limitation se doublerait, pour certaines informations, de conservations anonymisées. Des outils (privacy enhanced technologies) devraient également prochainement permettre aux usagers d'effectuer des recherches sans laisser de traces.Ce dossier a fait l'objet d'une médiatisation considérable.L'ensemble des acteurs de cette actualité sont mobilisés pour trouver des solutions constructives dans ce contexte complexe.Ces mesures font suite à une intervention en décembre 2006 du Groupe Article 29 réunissant les représentants des autorités de protection des données personnelles des pays de l'UE.Ce dernier avait publiquement et fermement appelé les moteurs de recherche à l'adoption de mesures de conformité aux directives européennes protection des données personnelles. Cette initiative avait été appuyée par une campagne d'usagers et de groupes de pression (stakeholders). Auparavant, dès 1998, des groupes de travail réunissant des autorités de protection des données de la planète avaient déjà adopté des recommandations allant dans le même sens.Les présentes colonnes ont pour objectif d'apporter un éclairage modeste et serein au débat, à la lecture des informations rendues publiques par les différentes parties (moteurs de recherche, autorités européennes).Quels sont les clés de compréhension et les enjeux de cette actualité? Il en existe de multiples. Essayons de les résumer.Le premier enjeu consiste à ce que les acteurs de l'industrie des moteurs de recherche et les autorités trouvent un accord sur le niveau de mesures à adopter. Il s'agit d'attester que sont effectivement garantis les principes de protection des données résultant au premier chef de la Directive protection des données personnelles 2 mais également d'autres législations de même nature hors UE ou de textes adoptés au sein des instances internationales (OCDE, Nations Unies, Conseil de l'Europe). Le second enjeu vise sans aucun doute à ne pas ignorer deux contraintes auxquelles doivent faire face les moteurs de recherche. Ces derniers doivent pouvoir réaliser des traitements d'une précision suffisante pour répondre aux attentes fortes des usagers en termes de personnalisation et d'optimisation des services. Ils exercent leurs activités dans un cadre juridique mondial qui les contraint à anticiper les attentes des législations multiples et potentiellement contradictoires qui n'ont pas définitivement envisagé leur statut, par exemple s'agissant de l'application ou non des exigences sur la rétention des données relatives au trafic. Le troisième consiste certainement à la nécessité, pour les acteurs de l'industrie comme pour les autorités, de maintenir un climat de confiance avec les usagers

eux-mêmes en protégeant leur vie privée (privacy).Quelles sont les logiques qui conduisent les autorités européennes à prendre position dans ce dossier face à des entreprises mondiales? Un peu d'histoire juridique permet de trouver un début de réponse. Depuis presque 30 années, l'UE a engagé des orientations de protection des personnes physiques face au risque d'intrusion des technologies dans la vie privée. Depuis 1995, elle sensibilise les acteurs aux précautions à prendre, adopte des recommandations, avec le souci déclaré de ne pas entraver le commerce mondial. L'arrivée de l'internet a bouleversé la donne et multiplié les risques, contraignant ce même législateur européen à adapter son approche par étapes 3. Deux fronts juridiques sont désormais ouverts autour de la question des moteurs de recherche: protection des données à caractère personnel des citoyens/ consommateurs face à toutes les technologies (internet, télécom, audiovisuel etc.) et tous les traitements; protection des choix de contenus des usagers dans un contexte de convergence des technologies et de lutte contre le terrorisme. Nous ne nous attarderons pas ici sur les difficultés conceptuelles et méthodologiques de ces évolutions : le moteur de recherche a-t-il le statut de service de communication au public, d'opérateur de communications électroniques, de kiosque à contenus? Sur le plan de la protection des données personnelles, les contraintes sont celles de textes répondant à des principes dits de neutralité technologique. Une donnée de recherche (motclé etc.) ou de connexion au service de recherche (log) constituerait une donnée identifiable dès lors que des moyens seraient mis en oeuvre pour permettre l'identification de la personne. Face à la puissance de traitement des technologies de l'information, les autorités européennes semblent considérer que la donnée acquiert de fait un statut de donnée personnelle latente. Il en résulte au moins deux exigences pour que leur traitement soit légal. La première concerne l'obligation d'établir la finalité et la proportionnalité du traitement (collecte, production d'un raisonnement informatique, conservation) d'informations liées aux requêtes ou des données de connexion associées aux allées et venues de l'internaute. La seconde tient au droit à l'oubli et consiste à déterminer le point à partir duquel les données dont la conservation ne serait pas justifiée devraient être effacées. Il existe ici une question particulièrement difficile à arbitrer: quelles doivent être les limites d'usage de technique susceptible de prolonger sur de longues durées la conservation de certaines informations de traçabilité (cookies)? Il convient de noter que le législateur de 2004 a souhaité lors de la modification de la loi Informatique et libertés protéger particulièrement les usagers en cas de collecte technique d'informations lors de la connexion aux services de communications électroniques (loyauté, proportionnalité, information des personnes). Ces dispositions s'appliquent-elles uniquement aux fournisseurs de services de télécommunication? Sur le plan de la protection des choix des usagers, dans le prolongement de directives européennes, le législateur français a ouvert une voie consistant à placer sous embargo électronique le traitement de données susceptibles de révéler les choix des utilisateurs de services de communication électronique.La loi relative aux communications électroniques et aux services de communication audiovisuelle du 30 septembre 1986 modifié en juillet 2004 précise que le secret des choix faits par les personnes parmi les services de communications électroniques et parmi les

programmes offerts par ceuxci ne peut être levé sans leur accord (art.3). La loi du 23 janvier 2006, pour d'autres raisons liées à la lutte contre le terrorisme et à la transposition de disposition de directive européenne portant sur la protection de la vie privée des usagers des services de communication électronique 4, a introduit des dispositions fondamentales dans le Code des postes et les communications électroniques (art. L. 34-1). Ce dernier précise désormais en substance que les opérateurs de communications électroniques et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne doivent effacer au terme d'une année de conservation les données relatives au trafic et celles susceptibles de révéler sous quelque forme que ce soit les informations consultées par les usagers dans le cadre des communications avec ces services 5. Seul l'accord des personnes autorise le traitement de telles données dans le cadre de finalités déterminées.Aucune de ces législations ne vise expressément les moteurs de recherche.Quels enseignements tirer de cette actualité? La position des autorités de protection des données traduit l'adoption d'un véritable principe de précaution. Dès 2006, elles mettaient en avant la place particulière occupée par les moteurs de recherche dans la société de l'information en ce qu'ils se situent au carrefour à la fois de données relatives aux choix des usagers mais également concernant leurs allers et venues (données relatives au trafic ou logs). Constatant l'offre exponentielle de services à valeur ajoutée aux usagers (ex : messagerie gratuite etc.), elles craignent que se crée un contexte à risques en termes d'interconnexion globale de données de différentes natures face à l'émergence de technologies qui pourraient à l'avenir faciliter de telles démarches.Ce dossier révèle également la difficulté d'appliquer le principe de finalité du traitement posé par le droit de la protection des données. Il s'agit par essence d'une notion mise en oeuvre par les autorités dans une logique de réalité. Autrement dit, en l'absence de possibilité d'établir une finalité poursuivie, il ne pourrait y avoir ni traitement, ni conservation de données etc. Quand bien même une ou plusieurs finalités pourraient être établies, la question se pose de l'apposition de frontières entre les données qui pourraient être traitées et celles qui ne le pourraient pas. La question se pose également des garanties techniques qui pourraient être mises en oeuvre de façon effective. En résumé, les moteurs de recherche semblent eux-mêmes conserver des données au titre de principe de précaution opérationnel (ex: une donnée peut être utile ou nécessaire pour améliorer ou optimiser le service aux usagers) ou juridiques (ex: faire face aux cas de fraudes, anticiper d'éventuelles évolutions des réglementations européennes sur la rétention des données aux fins de lutte contre le terrorisme, répondre à des demandes judiciaires de communication d'information). Ce dossier n'est pas clôturé.À ce stade ne sommes-nous pas en présence d'un face-à-face de principes de précaution? Une chose est certaine, ce faceà- face se fait au bénéfice du consommateur citoyen mondial.Un autre enjeu se pose pour ce dernier. Est-il dans son intérêt, eu égard à la nécessité de préserver par ailleurs un service personnalisé et performant, d'ouvrir une voie massive de suppression et d'anonymisation de données d'utilisation des moteurs de recherche? La solution tient sans aucun doute dans l'adoption d'une approche graduée et équilibrée prenant en compte un dialogue transparent avec l'internaute. Si une conclusion générale était

possible, elle nous amènerait à constater qu'en quelques années l'industrie de l'internet et du commerce électronique international n'a pas manqué de développer des bonnes pratiques en matière de protection de la vie privée. Ces dernières constituant désormais un pilier majeur de la confiance dans la société de l'information et donc dans la réussite économique de ses entreprises, chaque actualité sur ces sujets contient les germes d'une véritable affaire. Dans ce débat, marqué par l'effacement des barrières culturelles/juridiques continentales, l'UE démontre qu'elle est désormais un interlocuteur incontournable du commerce électronique mondial sur ces questions.

Auteur(s) :

Laurent CARON - Avocat au Barreau de Paris Lamy & Associés, Paris/Lyon

Notes de bas de page :

2. Google, MSN, Yahoo, Ask.com

3. Directive 95/46/CE du Parlement et du Conseil du 24 octobre 1995relative à la protection des personnes physiques à l'égard des traitementsde données à caractère personnel et à la libre circulation de ces données.

4. Le respect de la vie privée sur Internet, « Une approche européenneintégrée sur la protection des données en ligne », Groupe Article 29,21 novembre 2000.

5. Directive 97/66/CE du 15 décembre 1997 concernant le traitementdes données à caractère personnel et la protection de la vieprivée dans le secteur des télécommunications, modifiée par laDirective 2002/58/CE du 12 juillet 2002 concernant le traitementdes données à caractère personnel et la protection de la vie privéedans le secteur des communications électroniques et la Directive2006/24/CE du 15 mars 2006 sur la conservation de données généréesou traitées dans le cadre de la fourniture de services de communicationsélectroniques accessibles au public ou de réseaux publicsde communications.

6. Par arrêt du 7 août 2007, le Conseil d'État a validé le décret du 24 mars2006 sur la conservation des données des communications électroniques.