Le développement de la publicité personnalisée, nouveau graal de la publicité numérique, passe par une exploitation accrue des données des internautes dans un écosystème de services. L'importance prise par ces pratiques conduit le gouvernement américain et la FTC, comme les autorités européennes, à imaginer des dispositifs plus contraignants pour garantir les droits des internautes en matière de données personnelles.

De la publicité comportementale à la publicité personnalisée

Connaître l'internaute est devenu un facteur abandonnent progressivement la recherche automatique au profit de résultats personnalisés, refermant le Web sur l'individu et ses activités en ligne (voir *infra*). Cette évolution concerne également l'économie des services en ligne, notamment pour les plates-formes de dimension mondiale (Google, Microsoft, Yahoo!, Facebook ou AOL) qui toutes dépendent des performances de la publicité pour financer leur offre. En contrôlant plus précisément les données personnelles laissées par chaque internaute sur le Web, par l'intermédiaire du système d'exploitation et du navigateur, par l'intermédiaire du moteur de recherche et des « profils » créés, qu'il s'agisse d'un compte de messagerie ou d'un profil sur un réseau social, les acteurs du Web sont en effet en mesure de proposer des publicités dites « personnalisées », c'est-à-dire d'une précision – et donc d'un coût – largement supérieure au ciblage classique dit contextuel (en fonction du mot clé tapé ou du contenu du site où est affichée la bannière), ainsi qu'au ciblage comportemental reposant sur l'étude de la navigation d'un internaute (voir *REM* n°6-7, p.48).

Avec la personnalisation, la publicité va au-delà du ciblage comportemental. Avec le ciblage comportemental, il s'agit à chaque fois de connaître, notamment grâce à des cookies, l'individu qui se cache derrière une adresse IP, l'équation étant parfois difficile quand il s'agit de l'adresse d'un PC utilisé par tous les membres du foyer, à l'inverse de l'adresse IP d'un smartphone, le téléphone mobile étant un objet éminemment personnel. Les *cookies* – installés par les régies lors d'une connexion à un site dont elles ont la gestion – vont enregistrer les sites visités par l'internaute et en déduire ses centres d'intérêt. La régie va alors placer des publicités adéquates sur les sites web que visitera l'internaute, dès lors qu'elle a ces sites en gestion. Ce ciblage comportemental dans la publicité représenterait déjà, à titre d'exemple, entre 10 et 15 % des publicités affichées par la régie de Yahoo! en France. En ajoutant un compte personnel à l'adresse IP espionnée par les *cookies*, la personnalisation peut passer à la vitesse supérieure : il ne s'agit plus seulement de pister les déplacements de l'internaute sur le Web, mais de croiser ces données avec des données personnelles communiquées par l'internaute, en particulier sa véritable identité, comme cela apparaît avec les comptes *mails* ou les profils de réseaux sociaux.

C'est cette capacité à s'adresser à l'individu sur le Web qui explique en grande partie la

raison pour laquelle Facebook, avec ses 850 millions d'utilisateurs fin 2011, est parvenu à devancer Yahoo! sur le marché américain des bannières en juin 2011, donc à détrôner la régie qui a probablement été, ces dix dernières années, la plus en pointe dans le ciblage comportemental, quand Google s'est historiquement concentré sur le ciblage contextuel, bien mieux adapté à son moteur de recherche. Et c'est le succès de Facebook qui explique également que Google ait revu sa politique de confidentialité et unifié sous un identifiant unique les activités de l'internaute sur ses différents services depuis le 1er mars 2012 (voir *infra*) : en associant la navigation d'un internaute à un compte Gmail, Google+ ou YouTube, Google est capable de proposer des publicités personnalisées avec sa régie Double Click, et donc de riposter à Facebook sur ce segment de marché, lequel devrait, à l'avenir, avec la publicité locale sur mobile, tirer la croissance des investissements.

Dans cette nouvelle version, la publicité personnalisée a en outre ceci de particulier qu'elle utilise des données personnelles volontairement communiquées par l'internaute dans le cadre de l'adhésion à un service. Elle peut donc être considérée comme une offre liée à un service, même si celui-ci essaime sur l'ensemble des activités de l'internaute, ainsi d'un profil Facebook qui sert de porte d'entrée à une exploration du Web par l'intermédiaire de la recommandation sociale, ou d'un compte Gmail qui permet d'activer une navigation et des recherches en mode personnalisé dans l'univers des services Google. L'accès aux données liées au service peut donc être verrouillée par l'éditeur du service et les données devenir, de ce fait, inaccessibles à des acteurs tiers, en particulier d'autres régies. C'est le cas avec Facebook qui bloque l'accès à ses profils. C'est désormais le cas chez Google qui crypte toutes les données des internautes utilisant ses services après s'être identifiés via un compte. Dans ce cas, les sites qui dépendent du moteur de recherche comme apporteur d'audience perdent les informations précieuses que Google leur communiquait jusqu'ici sur la nature de leurs visiteurs. Selon une étude AT Internet citée par *Les Echos*, la part des requêtes indéterminées dans les statistiques communiquées par Google aux éditeurs de sites représentait déjà 20 % du total des requêtes aux Etats-Unis en mars 2012, deux semaines après le lancement de la nouvelle politique de confidentialité de Google. En France, le regroupement des données utilisateurs réparties entre les services Google depuis le 1er mars 2012 a fait augmenter, ici encore, la part des requêtes indéterminées -donc cryptées-, qui a bondi de 3,2% début mars à 12,3% des requêtes mi-mars. Les mêmes enjeux se posent sur les services payants, par exemple les journaux numériques vendus depuis les marchés d'applications où, sur ce segment, Apple refuse de communiquer aux éditeurs les données relatives à leurs parcours d'achat (voir *supra*).

Le contrôle des données personnelles devient donc un enjeu crucial, pour le marché publicitaire comme pour les activités de commerce en ligne, sa contrepartie étant une meilleure pertinence des services apportés à l'internaute, et des publicités qui lui sont

adressées. Sauf que la surenchère actuelle pourrait menacer l'équilibre fragile entre les différents acteurs d'Internet, susceptibles de verrouiller plus encore leur écosystème, voire menacer les grands équilibres du Web si les internautes, au lieu d'apprécier la personnalisation, y voient au contraire le résultat de processus opaques et une effraction faite à leur vie privée. Au reste, les études récentes montrent une réelle inquiétude des internautes. Ainsi, aux Etats-Unis, une étude du Pew Research Center présentée le 9 mars 2012 révèle que 73 % des internautes américains sont hostiles à la personnalisation des résultats des moteurs de recherche, un processus désormais courant qui repose sur l'analyse des habitudes de navigation. 68 % des internautes américains sont hostiles aux publicités ciblées et seulement 28 % y sont favorables, les considérant comme plus pertinentes. En Europe, les chiffres donnés par Viviane Reding, vice-présidente de la Commission européenne chargée de l'Agenda numérique, sont encore plus significatifs : dans un point de vue publié dans l'édition des *Echos* du 14 mars 2012, Viviane Reding indique que 74 % des internautes européens sont inquiets à l'idée de communiquer trop de données à caractère personnel et que seuls 26 % des utilisateurs de réseaux sociaux et 14 % des cyberacheteurs considèrent maîtriser l'utilisation faite de leurs données personnelles par des tiers.

Cette crise de confiance des internautes pourrait avoir des conséquences néfastes, notamment freiner le développement des services et du commerce en ligne, d'autant qu'une des grandes évolutions du Web est le *cloud computing* (informatique en nuage, voir *REM* n°9, p.43). Si la gestion délocalisée, à distance, des activités en ligne des internautes doit se développer, il faudra en effet qu'elle repose sur la confiance de l'internaute à l'égard des prestataires techniques et des éditeurs de services sur Internet. C'est notamment pour cette raison que les autorités américaines et européennes se mobilisent pour mieux encadrer le traitement des données personnelles sur Internet.

La solution américaine : une loi anti-cookies et une charte du droit à la confidentialité

Aux Etats-Unis, la question des données personnelles est traitée à la fois au plus haut niveau de l'Etat et par la Federal Trade Commission (FTC), l'autorité américaine de concurrence. Cette dernière a suggéré, en décembre 2010, de généraliser une option baptisée « Do not track » sur les navigateurs, permettant à l'internaute qui l'active de refuser l'installation de cookies sur son ordinateur. Une fois activée, cette option interdit aux régies en ligne comme aux *data brokers*,- ces intermédiaires spécialisés dans la collecte et la revente de données personnelles,- de pister l'internaute. Installée dès mars 2011 sur le navigateur Firefox, cette option a été vivement critiquée par certaines régies qui ont reproché à Mozilla, qui édite le navigateur Firefox, de mettre en péril le fonctionnement du Web en dégradant l'intérêt des publicités. Le 26 mars 2012, l'option « Do not track » faisait toutefois encore partie des

mesures proposées par la FTC dans un rapport sur les moyens d'améliorer la protection des données personnelles. A vrai dire, elle s'impose progressivement sur tous les navigateurs, Google étant le dernier à l'avoir proposée dans ses paramètres le 29 février 2012. A l'instar de Yahoo! qui proposera désormais une fonction « Do not track » sur l'ensemble de ses services, ce dispositif pourrait être généralisé à l'ensemble des sites du Web. Restera à savoir si cette option est suffisamment visible pour l'internaute ou s'il ne s'agit que d'un alibi des éditeurs de services pour éviter une régulation plus contraignante. En effet, la réglementation américaine en matière de données personnelles repose sur l'opt out. Autant dire que l'internaute doit activer l'option « Do not track » pour refuser la collecte de ses données personnelles qui s'effectue par défaut, alors que la réglementation européenne repose à l'inverse sur l'*opt in*, c'est-à-dire le consentement préalable de l'internaute, avant toute activation de service.

Sur ce sujet, la position du gouvernement américain tend vers une autorégulation du secteur avec la préservation de l'*opt-out*. Proposée par Barack Obama le 23 février 2012, la charte du droit à la confidentialité ou « déclaration des droits de la vie privée sur Internet », en effet, ne se veut pas contraignante. Les entreprises sont incitées à la suivre volontairement, ce qui revient essentiellement à informer les internautes sur l'usage fait de leurs données personnelles, leur laisser le choix des données qu'ils souhaitent communiquer, et enfin accepter des limites raisonnables à la collecte et à la conservation des données à caractère personnel. De nombreuses régies américaines se sont d'ailleurs engagées, au sein de l'alliance pour la publicité numérique (Digital Advertising Alliance), à signer une charte plus contraignante qui inclut par exemple le « Do not track », un moyen d'inciter le gouvernement à ne pas légiférer et d'éviter ainsi une entrave potentielle au développement de nouveaux services.

La solution européenne : l'opt-in et une nouvelle directive sur la protection des données Défendue par Viviane Reding, la réforme du cadre européen en matière de protection des données à caractère personnel devrait aboutir à une nouvelle directive assurément plus contraignante que celle de 1995. Cette dernière est aujourd'hui dépassée par l'évolution des usages et des pratiques et, surtout, se révèle incapable d'atteindre son objectif de protection. En effet, la diversité des législations nationales nées de la transposition de la directive a créé une sorte de *dumping* réglementaire en faveur du « moins disant » pour localiser certains services du Web dans les Etats les plus conciliants de l'Union. La nouvelle directive sera donc l'occasion d'harmoniser et de moderniser le cadre européen en matière de protection des données personnelles avec, à l'évidence, un renforcement de la protection souhaité par Viviane Reding.

Les données personnelles seront désormais propriété de la personne et non de l'entreprise

qui les a collectées, ce qui comporte de multiples conséquences. La première d'entre elles est le renforcement de l'*opt in*, à savoir que la collecte de données devra passer partout en Europe par un consentement préalable de l'internaute. A cela s'ajoute le fait que l'internaute peut demander l'effacement des données collectées par un service – une possibilité appelée « droit à l'oubli » – ou le transfert de ces données à un service concurrent. Au cas où le prestataire de services perd certaines données personnelles ou se les fait voler ou constate une utilisation abusive, il doit en informer l'internaute sans délai. Enfin, la nouvelle directive donnera un pouvoir élargi aux autorités européennes chargées de la protection de la vie privée sur Internet, à l'instar de la CNIL en France.

De ce point de vue, le projet de directive européenne va renforcer le dispositif d'*opt-in* déjà mis en place depuis la révision du paquet télécom, transposé en France par une ordonnance du 24 août 2011 modifiant la loi informatique et libertés. Le paquet télécom impose en effet que les « *tracking cookies* », c'est-à-dire les cookies espionnant la navigation de l'internaute pour lui proposer ensuite de la publicité ciblée, ne puissent être installés qu'à la suite d'un consentement explicite de l'internaute. Cette dernière notion impose que l'information préalable de l'internaute soit clairement effectuée, ce qui n'est pas le cas dans les interminables conditions d'utilisation des services. Ne sont pas concernés, en revanche, par l'ordonnance du 24 août 2011 les *cookies* dont la finalité exclusive est de faciliter la navigation, par exemple les *cookies* servant à enregistrer un panier d'achat sur un site de *e-commerce*, à identifier la langue de l'internaute ou les *cookies* évitant de s'authentifier systématiquement pour accéder à des services protégés par un mot de passe. Or ce sont les cookies d'authentification qui se développent aujourd'hui, via les comptes Gmail qui activent Android et certains services de Google, via les profils Facebook. Autant dire que la future directive européenne, pour véritablement redonner a l'internaute le contrôle de ses données et des informations ou publicités ciblées qui lui sont proposées, devra impérativement donner une réponse plus complète à la question de l'authentification et de son périmètre.

Sources :

- « Obama veut instaurer une déclaration des droits de l'internaute », latribune.fr, 23 février 2012.
- « Réforme en Europe de la protection des données personnelles », Marc Cherki, *Le Figaro*, 24 janvier 2012.
- « La CNIL veut encadrer l'usage des cookies, ces outils qui pistent les internautes », Cécile Ducourtieux, *Le Monde*, 20 février 2012.
- « Pub en ligne : le casse-tête des cookies », Jacques Henno, *Les Echos*, 28 février 2012.
- « Etats-Unis : 73 % des utilisateurs hostiles à la personnalisation des moteurs de recherche basée sur la mémorisation de leurs habitudes de navigation, selon une étude Pew Research Center », *La Correspondance de la Presse*, 12 mars 2012.
- « Pourquoi nous réformons la protection des données numériques », Point de vue de Viviane Reding, *Les Echos*, 14 mars 2012.
- « Google et la vie privée des internautes », Nicolas Rauline, *Les Echos*, 20 mars 2012.
- « L'Amérique veut mieux défendre la vie privée sur le Net », Pierre de Gasquet, *Les Echos*, 28 mars 2012.
- « Etats-Unis : le régulateur du commerce (FTC) prône des mesures permettant plus facilement aux utilisateurs d'internet qui le souhaitent que leurs données personnelles ne soient pas "tracées" en ligne », *La Correspondance de la Presse*, 30 mars 2012.

N°22-23 Printemps - été 2012