

**Délibération n°2013-420 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc.**

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte sous la présidence de Mme Claire DAVAL ;

Etant aussi présents M. Jean-François CARREZ, M. Claude DOMEIZEL, Mme Marie-Hélène MITJAVILE et M. Dominique RICHARD, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et 46 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n°2013-025 du 13 juin 2013 de la Présidente de la Commission nationale de l'informatique et des libertés mettant en demeure la société Google Inc. ;

Vu la délibération du bureau de la Commission nationale de l'informatique et des libertés n°2013-174 du 13 juin 2013 décidant de rendre publique la décision n°2013-025 du 13 juin 2013 de la Présidente de la Commission nationale de l'informatique et des libertés mettant en demeure la société Google Inc. ;

Vu la décision de la Présidente du 1<sup>er</sup> octobre 2013 désignant M. Jean MASSOT, Commissaire, membre de la CNIL, en qualité de rapporteur ;

Vu le rapport de M. Jean MASSOT, commissaire rapporteur, notifié à la société Google Inc. par courrier recommandé avec accusé de réception en date du 11 octobre 2013 ;

Vu les observations en réponse de cette dernière, en date du 13 décembre 2013 ;

Vu la décision de la Présidente de la formation restreinte de restreindre la publicité de l'audience conformément à la demande de la société, notifiée par courrier adressé aux conseils de celle-ci le 29 octobre 2013 ;

Vu la décision du Secrétaire général de la Commission en date du 11 décembre 2013 désignant les agents de la Commission devant être présents à l'audience de la formation restreinte ;

Vu les autres pièces du dossier ;

Après avoir entendu, lors de sa réunion du jeudi 19 décembre 2013 :

- M. Jean MASSOT, Commissaire, en son rapport ;

-

M. Jean-Alexandre SILVY, Commissaire du Gouvernement, n'ayant pas formulé d'observations ;

Les représentants de la société mise en cause ayant pris la parole en dernier ;

Le rapporteur, le Secrétaire général et les représentants des services de la Commission, le commissaire du Gouvernement et les représentants de la société s'étant retirés ;

Après en avoir délibéré, a adopté la décision dont la teneur suit :

## **I. RAPPEL DES FAITS**

Le 24 janvier 2012, la société Google Inc. (ci-après « Google » ou « la société ») établie aux Etats-Unis à l'adresse 1600 Amphitheatre Parkway, Mountain View, CA 94043, a annoncé son projet de fusionner une soixantaine de règles de confidentialité applicables à autant de ses services dans un seul document intitulé « règles de confidentialité » ou « politique de confidentialité ». La société a indiqué son intention de mettre en ligne ces nouvelles règles au 1<sup>er</sup> mars 2012.

A cette annonce, le groupe de coordination des autorités européennes de protection des données dit « groupe de l'article 29 » ou « G29 » a pris la décision d'apprécier les conséquences de ce projet sur la protection des données personnelles des citoyens de l'Union européenne au regard des dispositions de la directive 95/46/CE. Au cœur de ses préoccupations figurait la détermination de l'impact de ce projet de nouvelles règles quant à la combinaison des données que la société collecte sur ses utilisateurs.

A cet effet, le G29 a décidé de la création d'un groupe de travail *ad hoc* et confié à l'autorité française de protection des données (« la CNIL » ou « la Commission ») le soin de mener les discussions avec Google dans le cadre de ces travaux.

Le 2 février 2012, le G29 a informé la société de cette décision en lui demandant de suspendre ce projet de fusion dans l'attente de ses conclusions, ce que celle-ci a refusé.

De nombreux échanges sont intervenus, notamment dans le cadre de deux questionnaires, envoyés à la société les 16 mars et 22 mai 2012.

A l'issue de ces discussions, le G29 a considéré que la société ne se conformait pas aux exigences de la directive 95/4/CE. Un courrier signé des 27 autorités composant le G29 a donc été adressé en ce sens à la société le 16 octobre 2012, formulant des recommandations pratiques visant à guider la société vers une mise en conformité. Le 21 novembre 2012, la CNIL a, au nom du G29, invité la société à se mettre en conformité avec les recommandations du G29 avant le 15 février 2013.

A l'issue d'échanges complémentaires, la société a rencontré, dans les locaux de la CNIL, des représentants de la « taskforce » constituée par les autorités de protection des données à caractère personnel britannique, espagnole, française, néerlandaise, italienne et du Land de Hambourg. Par un courrier du 26 mars 2013, la société s'est engagée à mettre en œuvre de nouvelles mesures pour améliorer la protection des données de ses utilisateurs.

Prenant acte de l'analyse du G29 et de ses conclusions, et considérant que les propositions de Google n'étaient pas de nature à assurer une mise en conformité au cadre législatif français, la Présidente de la Commission, par décision en date du 29 mars 2013, a décidé d'ouvrir une procédure de contrôle sur le fondement de l'article 44 de la loi n°78-17 du 6 janvier 1978 modifiée et chargé le Secrétaire Général de la Commission de faire procéder aux vérifications correspondantes.

A l'issue de celles-ci, la Présidente a estimé que la société contrevenait à plusieurs dispositions de la loi n°78-17 du 6 janvier 1978 modifiée. Elle l'a donc mise en demeure, le 10 juin 2013, de prendre un certain nombre de mesures afin de se conformer à ces dispositions dans un délai de trois mois.

Conformément à l'article 46 alinéa 2 de la loi, la Présidente a demandé au bureau de la Commission de se prononcer sur l'opportunité de rendre cette décision de mise en demeure publique.

Le 13 juin 2013, le bureau, régulièrement composé de la Présidente et des deux Vice-présidents de la Commission conformément aux dispositions de l'article 13-I de la loi, a ordonné la mesure de publicité sur le fondement de la gravité des manquements constatés et de l'atteinte consécutive aux droits fondamentaux des personnes concernées, en tenant également compte du statut et de la taille de l'organisme en cause, leader mondial sur le marché de la recherche d'information sur Internet et de la fourniture de services associés, et, par suite, du nombre de personnes concernées par ses traitements (plusieurs millions sur le territoire national).

Dans sa réponse à la mise en demeure, la société a soutenu que la loi française, en l'occurrence la loi du 6 janvier 1978 modifiée, n'était pas applicable aux traitements en cause et que la CNIL n'était donc pas compétente pour engager une procédure répressive dans cette affaire ; elle a par ailleurs contesté chacun des manquements qui lui étaient reprochés.

Sur la base de cette réponse, la Présidente de la Commission a désigné M. Jean MASSOT, membre de la CNIL, en qualité de rapporteur, afin qu'une procédure soit engagée contre la société sur le fondement du 1° du I de l'article 45 de la loi du 6 janvier 1978 modifiée, qui dispose :

*« I. - La Commission nationale de l'informatique et des libertés peut (...) mettre en demeure le responsable de faire cesser le manquement constaté dans un délai qu'elle fixe.*

*Si le responsable d'un traitement ne se conforme pas à la mise en demeure qui lui est adressée, la commission peut prononcer à son encontre, après une procédure contradictoire, les sanctions suivantes :*

*1° Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'État ; (...) ».*

A l'issue de son instruction, le rapporteur a notifié à la société un rapport demandant à la formation restreinte de la CNIL de prononcer à son encontre une sanction pécuniaire de 150 000 €, dont il demandait par ailleurs qu'elle soit rendue publique. Ce rapport a été notifié par courrier en date du 11 octobre 2013, reçu le 14 octobre 2013, dont copie a également été notifiée à la société Google France par courrier en date du 11 octobre 2013, reçu le 14 octobre 2013.

A l'appui de sa proposition, le rapporteur a considéré que la société n'avait pas satisfait à la mise en demeure prononcée par la Présidente de la CNIL, et qu'elle était responsable de plusieurs manquements à la loi du 6 janvier 1978 modifiée.

Le courrier de notification qui accompagnait le rapport informait par ailleurs la société que son dossier était inscrit à l'ordre du jour de la formation restreinte du jeudi 19 décembre 2013 à 14h30.

La société a fait part de ses observations écrites sur le rapport par un courrier de ses conseils, en date du 13 décembre 2013. Lors de la séance de la formation restreinte de la CNIL du jeudi 19 décembre 2013, elle a en outre réitéré oralement ses observations en défense.

La société a pour l'essentiel conclu à l'inapplicabilité de la loi du 6 janvier 1978 modifiée aux faits de l'espèce et à l'incompétence de la CNIL pour la mettre en demeure et initier à son encontre une procédure de sanction. Sans remettre en cause la matérialité des faits constatés, elle a par ailleurs contesté que l'ensemble des données qu'elle traite soient des données à caractère personnel au sens de la loi, ainsi que l'ensemble des manquements lui ayant été reprochés sur le fond.

Au vu du rapport et des éléments de l'instruction, des écritures de la société et des observations orales ayant été formulées à l'audience, la formation restreinte a adopté la décision dont la teneur suit :

## II. MOTIFS DE LA DECISION

### 1. **Sur la contestation de la société quant à l'applicabilité de la loi n°78-17 du 6 janvier 1978 modifiée et à la compétence de la CNIL**

L'article 5 de la loi n°78-17 du 6 janvier 1978 modifiée soumet à l'application de la loi n°78-17 du 6 janvier 1978 modifiée « *les traitements de données à caractère personnel* :

- 1°) *Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;*
- 2°) *Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne ».*

Dans ses écritures comme en séance, la société Google Inc. conteste que la loi n°78-17 du 6 janvier 1978 modifiée lui soit applicable. Elle soutient que les traitements mis en œuvre dans le cadre de la politique de confidentialité litigieuse relèvent de sa seule et unique responsabilité et que les conditions d'applicabilité de la loi définies par cet article ne sont pas constituées.

La société soutient que les services auxquels ont recours les utilisateurs installés sur le territoire français sont exclusivement fournis par la société Google Inc. établie aux Etats-Unis. Elle soutient que la société Google France n'exerce aucune activité effective dans le cadre de laquelle Google Inc. traite des données personnelles ; elle ne saurait donc constituer un « établissement » au sens de l'article 5-I-1°) de la loi. Elle soutient également que, dans cette hypothèse, elle ne recourt pas à des moyens de traitements situés en France.

#### *a) Sur la notion d'établissement*

La formation restreinte relève tout d'abord que la société Google France SARL participe de manière effective à des activités liées aux traitements de données relatives aux utilisateurs de ses services.

Elle relève à cet égard que l'activité de publicité en ligne, qui constitue une contrepartie à la mise à disposition gratuite par la société de ses services aux utilisateurs, et qui génère la majeure partie de ses revenus, est indissociable du traitement des données des utilisateurs. En effet, c'est précisément grâce à la quantité considérable de données dont elle dispose sur eux qu'elle peut garantir aux annonceurs des prestations de ciblage publicitaire d'une grande précision, au plus proche des centres d'intérêt des personnes.

La formation restreinte relève à cet égard que parmi les activités de la société Google France déclarées en 2003 au Registre du commerce et des sociétés figurent notamment « *l'intermédiation en matière de vente de publicité en ligne, la promotion sous toutes ses formes de la publicité en ligne et la promotion directe de produits et services et la mise en œuvre de centres de traitement de l'information* ».

C'est à l'aune de l'importance que revêtent ces activités localisées en France que la société Google France peut être regardée comme un établissement au sens de l'article 5 de la loi n°78-17 du 6 janvier 1978 modifiée, pour les traitements ayant pour finalité la publicité. La circonstance que les opérations techniques de traitement des données aient lieu hors de France, en l'occurrence aux Etats-Unis, est sans incidence sur cette qualification.

*b) Sur la notion de moyen de traitement*

En tout état de cause, si l'on considère, comme le soutient la société, que seule la société Google Inc. est responsable de traitement, sans que ses autres établissements participent au traitement, la formation restreinte considère que la loi du 6 janvier 1978 est applicable, dès lors que la société Google Inc. recourt à des moyens de traitement sur le territoire national.

La société soutient qu'elle n'a pas « recours à des moyens de traitement » sur le territoire français.

- De manière générale, elle soutient que l'interprétation du rapporteur quant à la notion de moyen de traitement serait excessive. Selon elle, la directive 95/46/CE ne couvre que les responsables de traitement non-européens dont les activités sont réellement centrées sur le territoire d'un Etat membre. A ce titre, elle soutient qu'elle n'a pas vocation à s'appliquer à des traitements effectués sur les ordinateurs et terminaux mobiles des utilisateurs par le biais des cookies ou de dispositifs similaires.

A cet égard, la formation restreinte relève que la notion de « moyen de traitement » doit être interprétée à la lumière du considérant 18 de la directive 95/46/CE, qui précise l'intention du législateur communautaire quant à l'insertion de cette notion dans le texte : « *considérant que l'établissement, dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'Etat membre dans lequel des moyens utilisés pour le traitement de données en cause sont localisés et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés (...)* ».

Le législateur communautaire visait donc à éviter le contournement de la protection accordée aux résidents européens du fait de l'établissement du responsable de traitement dans un pays non-membre de l'Union Européenne. A cet effet, il a fait le choix d'une législation technologiquement neutre, considérant que « *le champ de cette protection ne doit pas (...) dépendre des techniques utilisées, sauf à créer de graves risques de détournement* » (considérant 27).

C'est au regard de l'ensemble de ces dispositions que la formation restreinte doit apprécier les faits de l'espèce.

- En l'espèce, la société conteste spécifiquement que les **cookies**, pris isolément, puissent être considérés comme des moyens de traitement. Selon elle, un cookie ne serait qu'un fichier texte, un type de marqueur qui serait lu, et qui ne correspondrait pas à un moyen de traitement proprement dit. Il ne pourrait donc procéder à aucun traitement de données sur l'ordinateur de l'utilisateur ni exercer un contrôle sur lui.

Il est certain qu'un fichier texte ne constitue pas, en lui-même, un traitement. Cependant, la formation restreinte relève que tant la lecture que l'écriture d'informations sur le navigateur installé sur le terminal de l'utilisateur s'effectuent par l'intermédiaire de cookies, dans le but de collecter des informations dont la société sera l'unique destinataire.

Or, l'article 2 de la loi n°78-17 du 6 janvier 1978 modifiée attribue la qualification de traitement notamment à toute opération de collecte, enregistrement, consultation, extraction, communication par transmission, diffusion ou toute autre forme de mise à disposition. Ainsi, l'accès aux informations relatives à l'utilisateur par le vecteur du cookie et leur lecture constituent bien des traitements au sens de cet article.

En outre, l'article 32-II de la loi n°78-17 du 6 janvier 1978 modifiée fait explicitement peser une obligation d'information préalable sur le responsable de « *toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement* », celui-ci étant expressément qualifié de responsable de traitement par le texte. Par suite, tout moyen permettant de procéder à de telles actions doit être qualifié de « moyen de traitement » au sens de la loi n°78-17 du 6 janvier 1978 modifiée.

Cette disposition traduit le souhait du législateur européen exprimé à l'article 5, paragraphe 3 de la directive 2002/58/CE modifiée par l'article 2 de la directive 2009/136/CE qui dispose que « *le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement* ». Le champ d'application de la directive 95/46/CE étant limité aux traitements de données à caractère personnel, à l'exclusion de tout autre traitement, la référence à ce texte ainsi qu'aux finalités des traitements opérés conduit à interpréter cette disposition comme qualifiant toute activité de stockage ou de lecture d'informations par l'intermédiaire de cookies de traitement de données à caractère personnel.

Par conséquent, l'ensemble des équipements et logiciels participant à ces actions d'écriture ou de lecture – y compris les cookies et les outils similaires - doivent être considérés comme des moyens de traitement.

- La société soutient que la référence au terme de « moyens de traitement » dans les textes applicables implique par ailleurs **l'exercice d'un degré de contrôle substantiel**, c'est-à-dire la capacité de diriger l'utilisation des moyens de traitement pour son propre compte.

Or, selon elle, ce sont les utilisateurs eux-mêmes qui ont recours à leurs moyens de traitement, c'est-à-dire leurs terminaux, pour accéder aux services en ligne qu'elle fournit, dans la mesure où ils contrôlent les composants de leurs terminaux et la connexion/déconnexion à Internet, de même qu'ils décident de la composante du service qu'ils vont utiliser et de la finalité de cette utilisation.

La formation restreinte considère que cet argument est infondé.

En effet, il est certain que la société exerce un degré de contrôle suffisant, voire substantiel, sur les moyens de traitement évoqués plus haut, quel que soit le service qu'elle fournit aux utilisateurs concernés.

Si ceux-ci peuvent effectivement choisir d'éteindre leur terminal ou suspendre leur connexion Internet, la société a en revanche la totale maîtrise des dispositifs de stockage ou d'accès à des informations qui, tels que les cookies, sont déposés dans le terminal de l'utilisateur. Le dépôt de ces dispositifs procède bien de la décision de la seule société, qui détermine également la finalité de la collecte et la nature des données qui lui remonteront par ce vecteur. Elle exerce donc un degré de contrôle substantiel et suffisant sur ces moyens de traitement.

- Enfin, la société reproche à la Commission de chercher à étendre l'application de la directive 95/46/CE et de la loi n°78-17 du 6 janvier 1978 modifiée en s'appuyant sur le critère de la **localisation des utilisateurs** qui, s'il est prévu par la proposition de règlement du Parlement européen et du Conseil du 25 janvier 2012, n'est pour l'heure pas applicable en droit français.

Ce reproche est également infondé. En l'espèce, la localisation des utilisateurs ne constitue pas un critère d'application de la loi mais un élément de fait permettant de déterminer la localisation des moyens de traitement, l'une et l'autre étant, eu égard aux technologies utilisées, indissociables.

La société Google Inc. a donc recours à des moyens de traitement sur le territoire français.

- Il résulte de ce qui précède que la société est soumise à l'application de la loi française et par conséquent à la compétence de la CNIL, que ce soit au titre des moyens qu'elle met en œuvre en France pour traiter les données des utilisateurs ou de son établissement sur le territoire national.

## **2. Sur la qualification préalable des données soumises aux règles de confidentialité, de données à caractère personnel au sens de la loi n°78-17 du 6 janvier 1978 modifiée**

La société conteste que l'ensemble des données des utilisateurs qu'elle traite sous l'égide des règles de confidentialité litigieuses constituent invariablement des données à caractère personnel au sens de l'article 2 de la loi n°78-17 du 6 janvier 1978 modifiée, qui dispose que *« constitue une donnée à caractère personnel 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »*.

A son sens, seules les données qu'elle collecte auprès des détenteurs de comptes Google seraient des données à caractère personnel au sens de la loi. Les autres données qu'elle collecte et traite pour les besoins de son service en ligne ne relèveraient pas de cette qualification et n'entreraient donc pas dans le champ d'application de la loi.

Elle conteste spécifiquement que les adresses IP constituent des données à caractère personnel, y compris en étant associées aux données issues des cookies PREF, dès lors qu'elle ne disposerait d'aucun moyen raisonnable lui permettant de relier ces éléments à une personne identifiée ou identifiable.



Il appartient donc à la formation restreinte de se prononcer sur cette qualification qui conditionne l'application de la loi n°78-17 du 6 janvier 1978 modifiée aux faits de l'espèce.

A cet effet, il convient de tenir compte de la nature et des caractéristiques des trois catégories d'utilisateurs ciblés par la société.

a) Catégories de personnes concernées

- Une première catégorie de données correspond aux utilisateurs dits « authentifiés », c'est-à-dire aux personnes qui, pour avoir accès à un service dont le fonctionnement repose sur la création d'un compte utilisateur (par exemple des comptes Gmail, Google+, Google Play ou Google Docs), se sont préalablement authentifiées au travers d'une interface *ad hoc* (le « compte Google »).

Les données contenues dans ce compte sont notamment les suivantes : nom, prénom, données de vérification du mot de passe, pseudonyme, date de naissance, sexe, pays, éventuellement adresse électronique alternative, numéro de téléphone, photo du profil public de la personne, carte de crédit, etc. La société a également accès à la liste des applications installées sur un terminal Android, la boîte mail et l'ensemble des messages associés, les photos (service « Picasa ») et les documents (service « Google Drive » ou « Docs ») détenus par l'utilisateur, les données de localisation du terminal mobile, les paramètres du terminal et du navigateur, les identifiants uniques comme le numéro IMEI, les visites de sites tiers, etc.

Les données générées par l'utilisation des services de Google par un utilisateur authentifié sont accessibles à l'ensemble de ceux-ci, y compris ceux ne requérant pas d'authentification préalable.

- Une seconde catégorie de données correspond aux personnes qui accèdent à un service offert par la société sans authentification préalable à travers un compte Google. Ces utilisateurs dits « non authentifiés » relèvent de deux sous-catégories :

- Les utilisateurs « actifs non authentifiés », qui ont recours à un service de la société sans que l'accès à celui-ci soit conditionné par une authentification préalable. Au premier rang de ces services figurent Google Search, Google Maps ou YouTube.

Les données issues de l'utilisation de ces services varient selon la nature de ceux-ci. Les données collectées sur les utilisateurs du moteur de recherche sont les termes de la recherche, l'adresse IP de l'utilisateur, ses préférences (option linguistique, etc.), les informations issues de deux cookies installés par le service (dénommés PREF et NID), qui contiennent eux-mêmes de nombreuses données, dont des identifiants uniques. Sont également collectées les données dérivées de fonctionnalités spécifiques du service, qui permettent d'apprécier les conditions de leur utilisation à distance (ex : la vitesse de frappe de l'utilisateur via la fonctionnalité « Google Suggest »). Des données de natures différentes seront issues des services YouTube et Google Maps (localisation, etc.).

A partir de l'adresse IP et des identifiants présents dans les cookies installés sur le terminal de l'utilisateur, la société reconnaîtra celui-ci automatiquement quand il utilisera d'autres services Google ultérieurement. Elle associera ainsi les données issues de ces services à celles issues de services utilisés précédemment.

Or, il est incontestable que les facultés d'identification des personnes s'accroissent au fur et à mesure que s'intensifie le croisement de leurs données, notamment les termes de leurs requêtes dans le service Google Search – comme l'a démontré l'affaire dite « AOL Stalker » de 2006. Il suffira notamment que l'utilisateur laisse apparaître son identité une seule fois lors de l'utilisation d'un des services librement accessibles de Google (par exemple dans l'hypothèse d'« egosurfing » ou « autogoogling », c'est-à-dire la recherche de son propre nom dans le moteur de recherche) pour que celle-ci soit définitivement associée aux données que sa navigation a précédemment générées.

- Les utilisateurs dits « passifs », c'est-à-dire ceux d'entre eux qui n'ont pas recours par eux-mêmes à un service Google, mais dont la société collecte néanmoins les données de manière indirecte. Lorsque ces utilisateurs naviguent sur des sites sur lesquels la régie publicitaire de Google est présente, la société va collecter leurs adresses IP, les sites sur lesquels ils se trouvent, ainsi que les identifiants uniques présents dans des cookies spécifiques alors dénommés DoubleClick.

Tel est le cas quand ces utilisateurs se connectent à des sites Internet tiers faisant appel aux services de Google pour mesurer leur fréquentation (Google Analytics), proposer de la publicité ciblée à leurs visiteurs en fonction de leurs profils (Google Adwords), fournir un plan de situation (Google Maps), etc.

Cette collecte a également lieu quand une personne adresse un courrier électronique à un utilisateur du service Gmail : quand bien même l'expéditeur ne serait pas un utilisateur Google, le contenu de son message sera scanné par la société, qui affichera de la publicité ciblée aux côtés des messages qu'il recevra de son correspondant.

De même, Google propose aux webmasters d'inclure un bouton « +1 » sur leurs sites pour permettre aux utilisateurs de recommander des articles ou des publications sur le réseau social Google+ sur lequel ils ont ouvert un compte. Lorsqu'un utilisateur se rend sur un de ces sites, la société en est informée du simple fait de l'affichage du bouton, qui conduit aussitôt au dépôt et à la lecture de cookies, sans même qu'il soit besoin pour l'utilisateur de cliquer. Cette information s'opère via les cookies NID, PREF et UserID pour les utilisateurs authentifiés, les cookies NID et PREF pour les utilisateurs actifs non-authentifiés, et le seul cookie NID pour les utilisateurs passifs. Les utilisateurs, quel que soit leur statut, seront ré-identifiés dès qu'ils visiteront ultérieurement le même site ou tout autre site sur lequel figure également le bouton +1.

Ainsi, les données relatives aux visiteurs de sites tiers sur lesquels la régie publicitaire de Google est présente (et que celle-ci collectera) sont l'adresse IP de l'utilisateur, le nom du site ainsi que l'identifiant unique présent dans le cookie DoubleClick, qui sert à améliorer la pertinence de la publicité affichée. Disposant de cet identifiant cookie et de son adresse IP, la société pourra reconnaître l'utilisateur à l'occasion de visites ultérieures de sites également partenaires de DoubleClick, afin de lui adresser des publicités personnalisées, notamment en fonction de l'analyse de son comportement de navigation.

- En outre, un utilisateur pourra posséder alternativement, voire cumuler les trois qualifications ci-dessus. Par exemple, les données relatives à une personne qui se sera « authentifiée » au début d'une session de navigation (ex : pour se connecter à son compte Gmail) seront associées à celles issues de l'utilisation de services Google ne requérant pas d'authentification préalable, cette association étant rendue possible par l'inscription dans le

navigateur de l'internaute du cookie PREF qui est commun aux services authentifiés ou non-authentifiés.

En accroissant sa connaissance sur l'utilisateur, la société peut lui proposer des services supplémentaires. A titre d'exemple, un utilisateur authentifié dont l'historique Web est activé pourra sélectionner des prédictions de requêtes basées sur les recherches qu'il aura précédemment effectuées dans les paramètres de la fonctionnalité Google Suggest. En contrepartie, la société valorisera l'information ainsi affinée dans son modèle publicitaire.

b) Sur l'application de la notion de données à caractère personnel au cas d'espèce

Au vu de ce qui précède, la formation restreinte considère que la société collecte bien des données à caractère personnel au sens de l'article 2 de la loi de 1978.

En premier lieu, elle relève que la société ne conteste pas traiter, dans de nombreux cas, des données directement identifiantes. Ainsi, les données figurant dans les comptes individuels ouverts en vue de la fourniture de services à des utilisateurs « authentifiés » constituent, sans discussion possible, des données à caractère personnel. Le lien existant entre ces informations d'identification de l'utilisateur et les cookies associés à son adresse IP a pour effet d'attirer l'ensemble des données correspondantes dans la sphère des données directement identifiantes.

En second lieu, il est exact que les données collectées à l'occasion de la navigation d'utilisateurs non authentifiés (actifs ou passifs) ne peuvent être automatiquement considérées comme « directement identifiantes » dès lors que, prises isolément, elles ne se rapportent qu'au seul terminal (fixe ou portable) ou au seul navigateur de l'utilisateur, non identifié.

Pour autant, il importe de rappeler que les législateurs européen et français ont consacré une conception large de la notion de donnée à caractère personnel, qui peut être directement ou indirectement identifiante. Ainsi, la possibilité « d'identifier » une personne déterminée à partir d'identifiants spécifiques ou d'un ou plusieurs éléments qui lui sont propres conduit à regarder ceux-ci comme des données à caractère personnel.

La formation restreinte relève, à cet égard, que le seul et unique objectif poursuivi par la société consiste à recueillir un maximum d'éléments sur des personnes singularisées afin d'optimiser la valorisation de leurs profils sur le plan publicitaire. Son modèle économique ne requiert donc pas de connaître les nom, prénom, adresse ou autres éléments directement identifiants sur les personnes, qui ne lui sont pas nécessaires pour les reconnaître lors de chaque nouvel usage qu'elles feront de ses services.

Cependant, les éléments qu'elle collecte à cette fin, qui peuvent être combinés entre eux comme la société l'a prévu en adoptant ses nouvelles règles de confidentialité, lui permettent de cerner avec une précision extrême le comportement d'une machine et, derrière celle-ci, de son utilisateur, à laquelle elle est capable *in fine* d'affecter les caractéristiques de son activité quotidienne, ses interactions avec autrui, ses centres d'intérêt, des éléments liés à sa personnalité, ses choix de vie, etc.

En d'autres termes, l'accumulation de données qu'elle détient sur une seule et même personne lui permet de la singulariser à partir d'un ou de plusieurs éléments qui lui sont propres. Ces données doivent, en tant que telles, être considérées comme identifiantes et non comme anonymes.

En tout état de cause, des identifiants uniques comme l'adresse IP, bien qu'ils n'aient pas de lien direct avec l'identité proprement dite de la personne, permettent à la société d'attribuer à celle-ci l'ensemble des données issues de son utilisation de ses services, qu'elle ait été ou non authentifiée, dans des proportions telles qu'il est impossible de ne pas considérer que celles-ci ne sont pas identifiantes, à tout le moins indirectement.

La qualification de données à caractère personnel peut ainsi s'appliquer non seulement à l'adresse IP et aux données collectées par le vecteur des cookies, mais également à tous les types d'identifiants uniques, tels que celui du terminal ou d'un composant du terminal de l'utilisateur, le résultat du calcul d'empreinte dans le cas du « fingerprinting », ou encore l'identifiant généré par un logiciel ou un système d'exploitation.

Cette qualification s'impose d'autant plus que, comme indiqué précédemment, il suffit que l'utilisateur s'authentifie une seule fois auprès d'un service de la société (par exemple Gmail) pour que l'ensemble de sa navigation subséquente soit couplée à son profil directement identifiant.

La formation restreinte considère par conséquent que la société procède, sans distinction, au traitement de des données à caractère personnel au sens de l'article 2 de la loi n°78-17 du 6 janvier 1978 modifiée, que ce soit sur les utilisateurs authentifiés ou non-authentifiés.

### **3. Sur le manquement à l'obligation d'informer les personnes**

L'article 32-I de la loi du 6 janvier 1978 modifiée prévoit que « *La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :*

- 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;*
- 2° De la finalité poursuivie par le traitement auquel les données sont destinées ;*
- 3° Du caractère obligatoire ou facultatif des réponses ;*
- 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;*
- 5° Des destinataires ou catégories de destinataires des données ;*
- 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;*
- 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne (...).* »

Sur le fondement de cette disposition, la Présidente de la CNIL a mis la société en demeure de « *procéder à l'information des utilisateurs, quel que soit leur statut, en application des dispositions de l'article 32, en particulier s'agissant des finalités poursuivies par le responsable des traitements mis en œuvre* ».

- La société se défend de ne pas respecter la loi sur ce point.

Elle affirme que les règles de confidentialité et supports d'information qu'elle a mis en ligne sont suffisamment complets au sens des textes européens dès lors qu'ils permettent aux utilisateurs de connaître, outre l'identité du responsable de traitement, la finalité, les destinataires des données et l'existence d'un droit d'accès et de rectification. En tout état de

cause, elle reproche à la CNIL de ne lui fournir aucune indication concrète quant aux modifications à apporter pour que la société puisse répondre à ses attentes.

Elle soutient que la simplification de l'information opérée par la mise en ligne de sa politique de confidentialité a pour objectif d'informer les utilisateurs par un document unique, lui permettant de s'adresser à une palette d'utilisateurs particulièrement large.

Elle soutient enfin que la fourniture d'informations plus détaillées l'aurait conduite à donner un niveau de précision technique peu compréhensible pour la majorité des utilisateurs, par ailleurs non requis par le G29 et la CNIL, et qu'il serait contre-productif d'exiger le maintien de règles de confidentialité distinctes pour chacun des produits de la société, à moins que ceci ne soit justifié par une réglementation spécifique (ex : Google Wallet).

Sur ce point, la formation restreinte considère ce qui suit.

- L'obligation d'information des personnes prévues par l'article 32 de la loi n°78-17 du 6 janvier 1978 modifiée consiste à mettre celles-ci en mesure de comprendre la manière dont leurs données seront traitées, et ce de manière effective et complète au regard des circonstances de la collecte.

A cet égard, la manière dont cette information est fournie est sans incidence. Ainsi, il était parfaitement loisible à la société de décider de choisir de nouvelles modalités d'information des personnes en abandonnant le principe d'une politique de confidentialité distincte par service. La validité du choix de la société quant à la fourniture d'une information par « strate », c'est-à-dire dans un texte global auquel sont rattachées des informations supplémentaires, plus détaillées, délivrées sur des supports tiers, n'est pas contestable.

Cependant, comme le relève d'ailleurs l'avis n°10/2004 du 25 novembre 2004 du G29 (avis WP100), la délivrance de cette information par « strate » doit dissocier deux niveaux d'information : d'une part, les informations de premier niveau, qui sont les plus importantes à connaître pour les personnes ; d'autre part, des informations qui ne présentent vraisemblablement d'intérêt qu'en seconde intention. Ces informations doivent être formulées en un langage simple, direct et sans ambiguïté.

Parmi les informations essentielles de premier niveau figurent, outre l'identité du responsable de traitement, les finalités du traitement et toute information supplémentaire nécessaire afin de garantir un traitement loyal de l'information vis-à-vis des personnes concernées.

A cet égard, la société dit mettre en œuvre les traitements concernés avec une finalité unique, déterminée et légitime, conformément l'article 6-2° de la loi, à savoir « *la fourniture du service en ligne Google à ses utilisateurs* », qu'elle présente comme une « *expérience unique et unifiée pour l'utilisateur, le compte Google permettant aux utilisateurs d'accéder à tous les composants du service en ligne Google avec un identifiant et un mot de passe unique* ».

Elle présente cette finalité comme la « finalité première » des traitements induits par la fourniture de son offre de service intégrée, par ailleurs déclinée en différentes fonctionnalités, services, outils, produits, ou caractéristiques (c'est-à-dire les différents services qu'elle offre). Elle soutient que cette finalité première n'est pas évasive mais répond à l'obligation d'information des utilisateurs, dès lors qu'elle la présenterait de manière conforme, voire supérieure aux bonnes pratiques du secteur, conformément à l'article 32 de la loi.

Au préalable, la formation restreinte rappelle les obligations, qui pèsent sur la société, de déterminer les finalités des traitements de données qu'elle met en œuvre (article 6-1°) et d'en informer les utilisateurs (article 32).

La précision et la clarté de l'information communiquée aux personnes concernées sont essentielles pour leur permettre de comprendre les conditions dans lesquelles leurs données sont collectées et traitées, ainsi que, le cas échéant, d'exercer effectivement les droits qui leur sont reconnus par la loi : droit d'opposition (article 38), droit d'accès (article 39), droit de rectification ou d'effacement (article 40), notamment à travers les outils offerts à cet effet par la société (par exemple le « Google Dashboard »). Le Conseil d'Etat a d'ailleurs rappelé le lien entre information et possibilité d'exercice des droits dans sa décision n°327916 du 29 septembre 2001 (société Centrapel).

A cet égard, la formation restreinte relève que les traitements de données qui découlent de la fourniture des services extrêmement divers de la société sont tout aussi variés et ne se substituent pas les uns aux autres, compte tenu notamment de la diversité des données collectées (données de géolocalisation, échanges de mails, requêtes dans le moteur de recherche, paiement par Google Wallet, mises en ligne d'informations sur Google+, mise en ligne ou requêtage de vidéos sur YouTube, etc.), et des différents statuts d'utilisateurs concernés par la collecte de données.

Les services qu'offre la société sont donc diversifiés, même s'ils sont partiellement intégrés et présentés de manière unique. Les services Google Search, Wallet, Analytics, Maps, Drive, Youtube, etc. n'ont rien de commun, si ce n'est la possibilité (qui plus est pour les seuls utilisateurs authentifiés) de s'y connecter à travers un compte unique permettant la jonction fonctionnelle de services de natures différentes, et le fait que la société s'est autorisée à combiner les données issues de l'utilisation de ses services par les personnes, quel que soit leur statut, dans des conditions indéterminées.

Or, en prévoyant dans ses règles de confidentialité que *« les données que nous collectons par le biais de nos services nous permettent de les fournir, les entretenir, les protéger et les améliorer, tout en développant de nouveaux services et en protégeant Google ainsi que nos utilisateurs »*, la société n'évoque que la fourniture d'un service global, sans préciser les finalités des catégories de traitements opérés sur ses données.

Cette information générale ne permet pas à l'utilisateur, authentifié ou non, de prendre conscience des finalités réelles, et par conséquent de l'ampleur de la collecte des données le concernant. Par conséquent, elle ne lui permet pas davantage de mesurer l'intérêt que peut revêtir, pour lui, tant la recherche d'informations complémentaires quant à la manière dont ses données sont traitées et/ou combinées que l'exercice de ses droits, afin de maîtriser l'usage de ses données.

Ainsi, faute de définir des finalités déterminées et explicites pour l'ensemble des traitements qu'elle met en œuvre au sens de l'article 6-1°), la société ne respecte pas l'obligation qui lui incombe d'informer ses utilisateurs des finalités des traitements opérés sur leurs données.

- En outre, au-delà de ce déficit substantiel de l'information de « premier niveau », il s'avère difficile pour l'utilisateur de comprendre l'utilisation qui sera faite de ses données dans le cadre d'un service précis et d'ajuster ses choix en conséquence.

Au contraire, pour parvenir jusqu'à ce niveau d'information, l'utilisateur devra consulter des rubriques diverses, dont les intitulés ne permettent pas une navigation fluide.

Par exemple, pour connaître les catégories de données que la société collecte sur lui dans le cadre d'un service précis, l'utilisateur devra partir de la rubrique « Règles et principes » pour accéder à la rubrique « Règles de confidentialité » (section « Données que nous collectons »). S'il souhaite en revanche savoir quels mécanismes lui permettent de garder la maîtrise sur ses données conformément à la loi, il lui faut accéder, en remontant à la rubrique « Règles et principes », à la rubrique intitulée « Technologies et principes ». Celle-ci fait alors référence, entre autres, à l'outil Google Dashboard qui permet de « *signaler la collecte d'informations de manière transparente* » pour les utilisateurs titulaires d'un compte Google.

Ces mêmes informations ne sont pas disponibles dans les FAQ accessibles à partir de la rubrique « Mentions légales ». En revanche, celles-ci indiquent à l'utilisateur comment demander la suppression des données à caractère personnel des résultats de recherche Google, ainsi qu'une nouvelle référence au Google Dashboard, auquel il n'est toutefois pas possible d'accéder directement par un lien cliquable. Celui-ci n'est accessible qu'à partir d'une autre rubrique, « Bon à savoir », elle-même accessible à partir de la rubrique « Règles et principes ».

Les informations fournies aux utilisateurs de ces services ne sont donc pas diffusées de manière suffisamment claire et recentrée pour satisfaire aux exigences de l'article 32-I de la loi.

La société ne s'est donc pas conformée aux termes de la mise en demeure sur ce point.

#### **4. Sur le manquement à l'obligation d'obtenir le consentement de la personne avant d'inscrire des informations dans son équipement terminal de communications électroniques ou d'accéder à celles-ci par voie de transmission électronique**

Aux termes du II de l'article 32 de la loi du 6 janvier 1978 modifiée « *tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable de traitement ou son représentant :*

- *de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;*
- *des moyens dont il dispose pour s'y opposer.*

*Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après en avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.*

*Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur*

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique,
- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ».

Il ressort des dispositions précitées que l'utilisateur doit recevoir, préalablement au dépôt et à la lecture de cookies ou de toute autre technologie visée par l'article 32-II, une information claire et complète sur les finalités de ceux-ci ainsi que sur les moyens dont il dispose pour s'y opposer, et que son consentement préalable est requis pour que le cookie puisse être déposé.

Les dispositions des alinéas 5 à 7 de l'article 32-II prévoient par ailleurs des exceptions à l'exigence du consentement préalable de l'utilisateur dans des cas limitatifs excluant tout dépôt de cookie à des fins publicitaires.

La Présidente de la CNIL, considérant que l'information fournie par la société aux utilisateurs ne remplissait pas les impératifs de clarté et de complétude exigés par la loi et que l'utilisateur n'était pas en mesure d'exprimer valablement son accord préalablement au dépôt de cookies Google sur des sites tiers, a mis la société en demeure « d'informer les utilisateurs, quel que soit leur statut, puis d'obtenir leur accord préalable avant d'inscrire des informations dans leur équipement terminal de communications électroniques ou d'accéder à celles-ci par voie de transmission électronique ».

En réponse, la société fait au contraire valoir que l'information fournie aux utilisateurs est satisfaisante, voire excède les pratiques du marché. Elle reproche par ailleurs au rapporteur de faire reposer son argumentaire sur une interprétation erronée de la loi et de ne pas avoir pris en compte des mesures d'information complémentaires mises en œuvre sur ses sites Google.fr et YouTube.com, si bien que sa position reposerait sur des faits inexacts.

Elle fait également valoir que des difficultés d'interprétation persistent quant aux modalités d'information prévues par l'article 32-II de la loi, telles qu'elles résultent de l'ordonnance du 24 août 2011 transposant la directive 2009/136/CE modifiant certaines dispositions de la directive 2002/58, dite directive « e-privacy ».

Elle estime, à cet égard, que les exigences de la Commission sont telles qu'elles équivalent à requérir un consentement explicite de l'utilisateur en vue de l'inscription ou de l'accès aux informations présentes sur son équipement terminal. Elle soutient au contraire que les textes prévoient que le consentement peut résulter « de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle », si bien que la CNIL commettrait sur ce point une erreur d'interprétation de la loi et de la directive.

- Au vu de ce qui précède, la formation restreinte relève, au préalable, que le considérant 66 de la directive 2009/136/CE prévoit que « lorsque cela est techniquement possible et effectif, conformément aux dispositions pertinentes de la directive 95/46/CE, l'accord de l'utilisateur en ce qui concerne le traitement peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application ».

Le considérant 17 prévoit quant à lui que « le consentement d'un utilisateur ou d'un abonné, que ce dernier soit une personne physique ou morale, devrait avoir le même sens que le consentement de la personne concernée tel que défini et précisé davantage par la directive



95/46/CE. Le consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet ».

Dès lors, la notion de consentement au sens de l'article 32-II de la loi doit s'apprécier tant au regard des termes de cet article que de l'article 2-h) de la directive 95/46/CE, qui dispose que le consentement s'entend de « toute manifestation de volonté, libre, spécifique et informée ».

Ainsi, s'il est exact que le consentement requis en l'espèce peut résulter des paramètres appropriés du dispositif de connexion ou de toute modalité appropriée, il doit pour autant remplir les trois conditions prévues par les textes, c'est-à-dire : 1) être obtenu préalablement à l'enregistrement ou à la lecture de toute information sur le poste de l'utilisateur, 2) après délivrance d'une information claire et suffisante à la personne, 3) et manifester sans ambiguïté l'accord de celle-ci à l'opération réalisée par le responsable de traitement.

En l'espèce, la formation restreinte doit vérifier que les utilisateurs sont bien mis en mesure d'exprimer un consentement conforme aux exigences de la loi avant que des informations ne soient enregistrées ou lues sur leur terminal. Il lui incombe donc d'apprécier la qualité, la temporalité et les modalités de l'information délivrée par la société sur les finalités poursuivies par les témoins de connexion et les autres techniques qu'elle utilise.

Sur ce point, la formation restreinte considère ce qui suit.

- En premier lieu, il est établi que le dépôt des cookies est réalisé dès la connexion au service en ce qui concerne les utilisateurs des services de la société qui ne sont pas préalablement authentifiés au travers d'un compte Google (« **utilisateurs actifs non-authentifiés** »).

De ce fait, la société ne communique pas les éléments d'information prévus par la loi *avant* tout action d'enregistrement ou de lecture d'informations stockées sur le terminal de l'utilisateur. Elle ne respecte donc pas les exigences d'information préalable posées par l'article 32-II de la loi sur ce point.

- En second lieu, la société fait valoir que l'information qu'elle délivre à l'utilisateur de ses services satisfait aux exigences de clarté et de complétude posées par la loi. Elle estime que la présence d'un bandeau d'information relatif aux cookies associé à des notices permet de fournir une information complète et suffisante des utilisateurs, et en tout état de cause conforme, voire supérieure aux pratiques du secteur.

La formation restreinte, cependant, constate que le bandeau dont la société affirme qu'il est une « pratique du secteur » apparaît sur deux de ses services, certes majeurs (Google Search et Youtube), mais qu'il fait défaut sur des services tout aussi importants tels que Google Maps, Google+, Google Drive ou Google Analytics.

En outre, l'information fournie sur ce bandeau ne permet pas aux utilisateurs des services de la société d'être informés de manière suffisamment précise des finalités poursuivies par la société quant à l'utilisation des cookies. En effet, celle-ci ne fait mention que du fait que des cookies sont déposés en vue d'assurer le « *bon fonctionnement des services* ». L'information ainsi délivrée, par sa généralité, ne peut en tant que telle satisfaire à l'objectif d'information claire et complète des utilisateurs fixé par la loi.

Il est par ailleurs exact qu'en application de la méthode d'information dite « multi-strate » retenue par la société, les utilisateurs peuvent prendre connaissance d'informations complémentaires en cliquant sur le lien correspondant à la rubrique « *En savoir plus* », dans laquelle plusieurs finalités et diverses informations complémentaires sont mentionnées. Pour autant, l'information ainsi fournie à l'utilisateur, tout aussi générale, ne permet pas à celui-ci d'associer un type de cookie et une finalité au service qu'il utilise. Dès lors, cette information n'est pas suffisamment circonstanciée quant aux cookies liés au service que l'utilisateur va utiliser.

En outre, la présence d'un bouton « OK » dans ce bandeau laisse penser aux utilisateurs qu'ils peuvent décider du dépôt de cookies sur leur terminal. Or, il est établi que ce dépôt est réalisé indépendamment de l'expression de ce choix, contrairement à ce que la société laisse suggérer.

- En troisième lieu, la société reproche au rapporteur de ne pas prendre suffisamment en compte les différences significatives existant entre les différents types de cookies.

Elle soutient que cette distinction lui permettrait de revendiquer le bénéfice des dispositions des alinéas 5 à 7 de l'article 32-II, qui dérogent à l'obligation de consentement préalable de l'utilisateur dans l'hypothèse où le cookie ou tout autre dispositif d'effet similaire « *a pour finalité exclusive de permettre ou faciliter la communication par voie électronique* » ou « *est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur* ».

Cependant, la formation restreinte constate qu'à tout le moins le cookie PREF est déposé sur le terminal de l'utilisateur dès qu'il se connecte sur le site concerné. Or, comme la société l'indique dans sa rubrique « *En savoir plus* », ce cookie est certes affecté à une finalité d'ergonomie, mais également de suivi publicitaire.

Le respect de l'article 32-II implique donc que le dépôt de ce cookie soit réalisé postérieurement à la délivrance d'une information sur cette seconde finalité et à l'expression du consentement de l'utilisateur. Les mêmes conditions sont requises préalablement au dépôt de tout autre cookie qui, n'étant pas couvert par l'exception précitée, poursuit une autre finalité, sans qu'il soit nécessaire de rechercher l'existence ou la présence de tels cookies.

- En quatrième lieu, la formation restreinte relève que le paramétrage du navigateur ne peut être valablement invoqué comme constituant une modalité d'expression du consentement au sens de l'article 32-II de la loi que dans la mesure où l'utilisateur a été préalablement mis en mesure de comprendre la portée de ce consentement.

Or, tant le caractère générique de l'information délivrée dans le bandeau que le dépôt concomitant de cookies sur le terminal de l'utilisateur privent ce dernier de la possibilité d'exprimer son choix quant à l'enregistrement des cookies sur son terminal.

Dans ces conditions, l'acceptation du dépôt de cookies par l'utilisateur ne saurait être déduite d'un paramétrage préexistant en l'espèce.

- Par ailleurs, il est établi que plusieurs cookies de la société peuvent être enregistrés ou lus sur le terminal **des utilisateurs dits « passifs »**, dont les données sont communiquées à la société à l'occasion de leur navigation sur des sites tiers ayant recours à des outils tels que

DoubleClick. Ces utilisateurs passifs ne peuvent pas visualiser le bandeau d'information affiché par la société, ce que celle-ci ne conteste pas.

La société, à cet égard, estime que l'obligation d'information des utilisateurs et celle de recueil de leur consentement préalablement au dépôt de cookies issus de ses services pèsent exclusivement sur les éditeurs de site ; elle réfute donc toute idée de coresponsabilité sur ce point.

A cet effet, elle fait valoir que le responsable des traitements opérés au moyen des cookies dits Analytics est l'éditeur du site qui décide de recourir à ses services aux fins d'analyse statistique de son service, et qu'elle-même n'agissant à son endroit qu'en qualité de sous-traitant, au sens de l'article 35 de la loi, elle n'a pas à assumer les obligations qui incombent aux éditeurs en application de l'article 32-II.

En outre, elle invoque le fait que les contrats qu'elle conclut avec les éditeurs de site mettent précisément à la charge de ceux-ci une obligation de fourniture des informations requises aux utilisateurs de leurs services. Elle-même ne saurait donc être tenue responsable au cas où ses cocontractants fourniraient une information déficiente aux utilisateurs ou ne recueillerait pas leur consentement préalable.

Pour autant, la société ne conteste pas qu'elle rapproche les données des utilisateurs de son service Analytics pour produire des statistiques par secteur et exploiter ces données pour assurer l'amélioration de son propre service. Ainsi, il est établi dans les conditions générales du service Analytics que la société réserve l'usage des données produites dans le cadre de l'utilisation de son service par son client pour elle-même et ses filiales.

La société procède donc à un ou plusieurs traitements des données Analytics pour son propre compte, qui ne peuvent donc être considérés comme des traitements opérés dans le cadre d'une prestation de sous-traitance rendue à ses clients. Du fait de la qualité de responsable de traitement qu'elle revêt dans ces circonstances, il lui appartient d'assumer en propre les obligations de l'article 32-II pour la partie des traitements dont elle détermine les finalités et moyens, et qui ne relèvent donc pas de la compétence des éditeurs de site.

En leur qualité de commanditaires, les éditeurs des sites qui font appel aux fonctionnalités de statistique du service Analytics ne se voient pas imposer une obligation spécifique et distincte d'information des utilisateurs sur la ou les finalités et de recueil du consentement pour l'enregistrement ou la lecture d'information obtenues par l'intermédiaire des cookies Analytics.

S'agissant de ces finalités propres à la société, il est établi qu'aucune information n'est accessible à l'utilisateur passif. Pour autant, la société indique que celui-ci peut se référer à sa politique relative à l'usage des cookies à cet effet. Cependant, en l'absence d'une mention d'information figurant sur le site visité, et ce préalablement au dépôt de cookie, la société ne peut valablement soutenir que l'utilisateur a été informé de la finalité du traitement, ni *a fortiori* se prévaloir de son consentement.

Il résulte de ce qui précède que le dépôt de cookies ne relevant pas des exceptions prévues aux alinéas 5 à 7 de l'article 32-II, dès lors qu'il n'est pas préalable à l'expression d'un consentement spécifique de l'utilisateur, lui-même donné postérieurement à la délivrance

d'une information claire et complète quant aux finalités et aux moyens de s'opposer à ce dépôt, constitue un manquement aux obligations qui incombent à la société en l'espèce.

Dans ces conditions, il est établi que la société ne respecte pas son obligation d'obtenir le consentement de la personne avant d'inscrire des informations dans l'équipement terminal de communications électroniques de l'utilisateur ou d'accéder à celles-ci par voie de transmission électronique, ce manquement concernant tant les utilisateurs actifs non authentifiés que les utilisateurs passifs de ses services, c'est-à-dire la plus large majorité des utilisateurs concernés.

La société ne respecte donc pas les exigences de la mise en demeure sur ce point.

##### **5. Sur le manquement à l'obligation de définir une durée de conservation des données**

L'article 6-5°) de la loi n°78-17 du 6 janvier 1978 modifiée dispose que *« les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »*.

Le rapporteur considère que la société ne respecte pas ces dispositions ni les termes correspondants de la décision de la Présidente de la CNIL, qui la mettait en demeure de définir une durée de conservation des données qu'elle collecte auprès de ses d'utilisateurs en fonction des finalités poursuivies par les différents traitements mis en œuvre.

En effet, celle-ci n'avait pas accédé aux demandes déjà formulées en ce sens par le G29, bien qu'elle se soit d'ores et déjà engagée publiquement à respecter trois types de durées de conservation précises : l'effacement du dernier octet des adresses IP dans les journaux des serveurs de Google (9 mois); la validité des cookies déposés dans les navigateurs des utilisateurs (2 ans) ; l'anonymisation du numéro de cookie dans les journaux des serveurs de la société (18 mois). Elle n'a défini aucune durée de conservation précise pour les autres données qu'elle collecte et traite.

Pour le reste et concernant les autres données, la société soutient qu'elle respecte les dispositions de l'article 6-5°).

- A cet effet, elle considère, en premier lieu, qu'il ne lui incombe pas de définir des échéances fermes et préfixées concernant les durées de stockage des données. Elle soutient que la loi n'impose pas la définition de durées strictes, mais uniquement une obligation qu'elle respecterait de procéder à une analyse de proportionnalité en fonction des finalités pour lesquelles les données sont collectées.

La formation restreinte relève, cependant, que, faute d'éléments concrets, la réponse évasive de la société ne lui permet pas de décider si cette analyse de proportionnalité est correcte, ni même si elle existe. En tout état de cause, les durées de conservation devant être définies en fonction des finalités pour lesquelles les données sont collectées, et ces finalités n'ayant pas été préalablement définies par la société de manière adéquate, il est légitime de considérer que celle-ci ne respecte pas les dispositions de l'article 6-5°).

En outre, la société ne conteste pas n'avoir mis en place aucune politique de gestion des durées définies et des mécanismes de suppression automatiques correspondants. En revanche, elle soutient qu'elle a mis en place de systèmes de sauvegarde fiables pour protéger les utilisateurs contre la suppression accidentelle ou malveillante de leurs informations. Les périodes de conservation liées à la suppression des données dépendraient, avant tout, du service ou du système de sauvegarde concerné. Ainsi, les données de bande de sauvegarde de la société sont régulièrement supprimées par destruction des clés de chiffrement, rendant les données inaccessibles ; en procédant à une telle destruction, la société respecterait ainsi les dispositions de l'article 6-5°).

Sur ce point, il importe toutefois de rappeler que l'obligation légale imposant à la société de définir des durées de conservation précises constitue une garantie fondamentale en matière de protection de la vie privée des personnes. Il s'agit en effet de prévenir que des données révélant notamment leur intimité (fichiers, courriels, photos, etc.) soient conservées sans limitation, au-delà de ce que celles-ci peuvent légitimement attendre de la société.

Compte tenu de l'importance de cette exigence, la société ne peut arguer de la seule mise en place de politiques de sécurité informatique, non-étayées d'éléments concrets, pour revendiquer la conformité à la loi sur ce point. En effet, la loi prévoit expressément que ces durées de conservation doivent être fixées en fonction des *finalités* des traitements. Elles ne sauraient donc dépendre des échéances d'un calendrier de maintenance informatique, mais d'une prise en compte effective de la vie privée des utilisateurs.

La formation restreinte considère donc qu'il appartient au contraire à la société de définir des durées précises pour l'ensemble des données qu'elle traite. Une telle mesure s'imposait d'autant plus en l'espèce que les personnes ne sont pas clairement informées de l'ampleur de la collecte des données opérées sur elles.

- Par ailleurs, la société indique qu'elle communique les durées de conservation qu'elle met en œuvre aux utilisateurs lorsque cela est utile, comme elle l'a fait pour l'anonymisation des adresses IP au-delà de 9 mois et celle des cookies des fichiers journaux des serveurs au-delà de 18 mois.

Pour certaines composantes de son service, elle indique appliquer des durées de conservation bien plus courtes, compatibles avec la finalité du traitement - qu'elle ne précise cependant pas.

En tout état de cause, elle soutient que, bien que la relation qui lie la société à ses utilisateurs implique que ceux-ci en utilisent plus ou moins de composants, il est légitime qu'elle conserve leurs données tant qu'elle continue d'entretenir une relation avec eux, « *pour leur permettre de continuer à utiliser sans interruption les différentes composantes du service Google* ». La durée de conservation en découlant varie donc en fonction de la personne physique, si bien qu'une durée de conservation imposée de manière arbitraire serait inappropriée et irait même, selon elle, à l'encontre de la loi « informatique et libertés ».

La formation restreinte ne souscrit pas à cette interprétation.

En dépit de ce qu'affirme la société, les critères selon lesquels elle détermine les durées de conservation des données de ses utilisateurs demeurent flous et indéterminés ; de ce fait, ils ne satisfont pas aux exigences de la loi.

Certes, la fixation de durées de conservation définies ne saurait avoir pour objet ni pour effet de supprimer des données des utilisateurs alors qu'eux-mêmes en auraient encore l'usage. En effet, le point de départ d'une durée de conservation n'est pas fonction de la date de la collecte, mais bien de la suppression du compte utilisateur. La fixation de ce point de départ autorise donc la société à conserver ces données des années durant, si nécessaire. Contrairement à ce que soutient la société, elle ne présente donc aucun caractère d'arbitraire.

En tout état de cause, il appartient bien à la Commission de vérifier dans quelles conditions la société traite des données dont des utilisateurs n'ont plus la maîtrise et dont on peut valablement penser qu'elles ont été supprimées. C'est pourquoi la société est tenue d'indiquer à la Commission quelles durées de conservation elle applique aux données qu'elle collecte, quand bien même elle ne les indiquerait pas aux utilisateurs eux-mêmes, comme elle pourrait le faire.

- Enfin, la société soutient que si la CNIL considère qu'elle ne respecte pas les dispositions de l'article 6-5°) de la loi, il lui appartient de démontrer, pour chaque catégorie de données personnelles, le fondement juridique de sa position.

Or, en l'absence de détermination de finalités précises pour chacun des traitements qu'elle met en œuvre, la société ne peut requérir de la Commission qu'elle lui indique de telles durées de conservation.

Au vu de ce qui précède, la formation restreinte constate que la société ne respecte ni les dispositions de l'article 6-5°) de la loi ni les termes de la mise en demeure sur ce point.

## **6. Sur le manquement à l'article 7 de la loi du 6 janvier 1978 modifiée**

Les règles de confidentialité de la société, dans leur version applicable à l'issue du délai imparti par la mise en demeure, c'est-à-dire au 27 septembre 2013, prévoient que « *les informations personnelles que vous fournissez pour l'un de nos services sont susceptibles d'être combinées avec celles issues d'autres services Google (y compris des informations personnelles), par exemple pour faciliter le partage de vos informations avec des personnes que vous connaissez. Le recoupement de données en provenance de cookies DoubleClick avec des données permettant de vous identifier n'est possible qu'avec votre accord explicite* ».

Cette disposition autorise la société à procéder à la combinaison de l'intégralité des données qu'elle collecte sur ses utilisateurs à travers l'ensemble de ses services, qu'ils soient authentifiés, non authentifiés ou passifs, que ce soit sur les données d'un même utilisateur ou entre les données de plusieurs utilisateurs.

Ainsi, concernant les **utilisateurs authentifiés**, les données renseignées dans un compte utilisateur peuvent être associées aux données dérivées de l'utilisation de tous ses services par ce même utilisateur ; ces données pourront alors être utilisées par l'ensemble de ceux-ci, qu'ils ne soient accessibles qu'aux utilisateurs authentifiés ou à toutes les catégories d'utilisateurs des services de la société. Les données relatives aux **utilisateurs actifs non-authentifiés** que la société collecte notamment à travers les cookies PREF et Analytics sur l'ensemble de ses sites, les cookies NID sur les services Google Search et Google Maps, les

cookies DoubleClick sur YouTube, etc., seront également combinées entre elles, de même que les données issues des cookies DoubleClick et Analytics qui la renseigneront sur les visites de l'utilisateur sur des sites tiers. Ces données seront associées entre elles et utilisées par tout autre service, par exemple pour personnaliser des résultats de recherche. Quant aux jeux de données que la société recueillera à travers ces cookies sur les seuls **utilisateurs passifs**, ils seront combinés entre eux à des fins d'analyse, d'affichage de publicités personnalisées ou de développement produit.

- De telles combinaisons sont soumises à l'application de l'article 7 de la loi n° 78-17 du 6 janvier 1978 modifiée dont les dispositions pertinentes prévoient que, pour être mis en œuvre, de tels traitements doivent « avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes : (...) 4°) L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ; 5°) La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ».

La Présidente de la Commission a estimé que la société procédait à cette combinaison de données sans respecter ces impératifs. Elle l'a donc mise en demeure de « ne pas procéder, sans base légale, à la combinaison potentiellement illimitée des données des utilisateurs, quel que soit leur statut ».

- La société, pour sa part, se défend de ne pas respecter la loi sur ce point. Elle soutient au contraire qu'elle peut se fonder sur plusieurs des critères de l'article 7 de la loi pour prouver la légitimité des traitements auxquels elle procède, ceux-ci variant en fonction de la nature des données, du traitement et de la relation qu'elle entretient avec l'utilisateur, et, de manière plus générale, des circonstances. Dans de nombreux cas, elle considère qu'elle peut même s'appuyer sur plusieurs de ces critères pour légitimer une opération de traitement de données.

Il appartient donc à la formation restreinte de se prononcer sur la validité de chacun des fondements que la société invoque pour légitimer la combinaison des données à laquelle elle procède sur ses utilisateurs.

- En premier lieu, la société soutient qu'elle peut s'appuyer sur le recueil du **consentement des utilisateurs** dans de nombreux cas.

Concernant les utilisateurs authentifiés, le consentement se manifesterait par le fait que l'utilisateur coche la case matérialisant son accord aux conditions d'utilisation et aux règles de confidentialité. Ce consentement serait éclairé du fait que les informations données dans les règles seraient suffisamment précises sur les opérations de traitement des données.

La formation restreinte rappelle que la validité du consentement de l'utilisateur est soumise à la triple condition que celui-ci soit libre, spécifique et informé, comme le prévoit l'article 2(h) de la directive 95/46/CE.

En l'espèce, elle relève que la mention de cette faculté de combinaison n'apparaît qu'au milieu des règles de confidentialité, dans le dernier tiers de la rubrique intitulée « *Comment nous utilisons les données que nous collectons* ». Cette information, alors qu'elle a trait à une modification essentielle de la politique de confidentialité de la société, n'est donc pas accessible aux utilisateurs en première intention. Par ailleurs, elle ne se distingue pas des

développements qui l'entourent, eux-mêmes formulés en termes généraux, notamment quant à la description des traitements de données, comme il a été dit plus haut. Il est donc impossible de considérer en l'espèce que le fait de cliquer sur la case « *J'accepte* » des conditions d'utilisation puisse être considéré comme un accord explicite et spécifique à cette combinaison.

Par ailleurs, en se contentant de prévoir que « *les informations personnelles que vous fournissez pour l'un de nos services sont susceptibles d'être combinées avec celles issues d'autres services Google (y compris des informations personnelles), par exemple pour faciliter le partage de vos informations avec des personnes que vous connaissez* », la société n'a pas suffisamment précisé la nature de la combinaison qu'elle compte opérer sur les données personnelles de ses utilisateurs pour que ceux-ci puissent être réputés avoir compris la portée de leur accord.

En particulier, il est établi que les données qu'un même utilisateur générera alors qu'il sera successivement authentifié, actif non-authentifié (y compris après s'être déconnecté de son compte) ou encore passif (c'est-à-dire quand il visitera des sites tiers intégrant un outil de Google comme DoubleClick ou le bouton +1) seront cumulées entre elles. Or, il est impossible de soutenir que la formulation générale figurant dans les règles de confidentialité permet à l'utilisateur authentifié qui se sera déconnecté de comprendre que ses données continueront cependant d'être traitées puis combinées par la société avec celles figurant dans son compte personnel.

La société est d'autant moins légitime à soutenir que l'utilisateur est clairement informé de la portée de son accord qu'elle ne diffuse plus la liste intégrale des services qu'elle propose et qui seront concernés par cette combinaison.

De surcroît, la formation restreinte relève que la société revendique le fait que « *le recoupement de données en provenance de cookies DoubleClick avec des données permettant de vous identifier n'est possible qu'avec votre accord explicite* ». Or, la société traitera l'ensemble des données de navigation issues de sites tiers intégrant l'outil DoubleClick pour créer des profils utilisateurs à des fins de ciblage publicitaire, que les personnes concernées soient ou non des utilisateurs authentifiés. Les données collectées par ce biais seront associées aux données figurant dans les comptes utilisateurs Google quand les personnes concernées accéderont ultérieurement à des services requérant leur authentification préalable, et ce alors même que leur consentement spécifique n'aura pas été recueilli en amont. Il est donc inexact de la part de la société, qui n'apporte aucun élément probant en défense sur ce point, de se prévaloir du contraire dans ses règles de confidentialité.

Concernant les utilisateurs non-authentifiés, la société soutient que le consentement des utilisateurs se matérialise à travers leur utilisation continue du service Google, en conformité avec les conditions d'utilisation, que leur consentement concernant les cookies serait recueilli par le biais de notices et de mécanismes spécifiques et qu'un consentement plus détaillé peut occasionnellement être requis au moment de la collecte ou de l'utilisation des données quand elle l'aura estimé nécessaire et/ou approprié.

Sur ce point, la formation restreinte ne considère pas que la seule utilisation d'un service puisse valoir consentement d'un utilisateur non-authentifié aux traitements de ses données ni, *a fortiori*, à leur combinaison, dès lors que, par construction, il n'aura pas été préalablement



mis en mesure de prendre connaissance des conditions d'utilisation ou des règles de confidentialité sur ce point.

De même, il est impossible de revendiquer le moindre consentement de la part des utilisateurs passifs qui n'auront aucune conscience du fait que leurs données seront recueillies à l'occasion de leur navigation sur un site tiers faisant appel à un outil Google ou de l'envoi d'un message à un utilisateur de Gmail.

Ainsi, l'information relative à la combinaison des données des utilisateurs n'est pas suffisamment visible ni explicite pour que la validation des règles de confidentialité puisse être considérée comme un consentement explicite et éclairé de la part des utilisateurs authentifiés, et la société ne recueille aucun consentement de la part de ses utilisateurs actifs non authentifiés et passifs.

Le critère du consentement des utilisateurs ne peut donc pas être revendiqué par la société pour légitimer la combinaison de leurs données, quel que soit leur nature.

- S'agissant en deuxième lieu des données nécessaires à **l'exécution d'un contrat**, la société précise que la relation avec ses utilisateurs est régie par les conditions d'utilisation qui constitueraient le cadre contractuel global entre Google et ses utilisateurs. Ce faisant, elle ne fait aucune distinction entre les trois catégories d'utilisateurs dont les données sont collectées à travers ses services sur le seul fondement de ses règles de confidentialité.

A cet égard, la formation restreinte constate que ni les utilisateurs actifs non authentifiés ni les utilisateurs passifs n'ont jamais accepté les conditions d'utilisation de la société. En l'absence de tout contrat les liant à la société, leurs données ne peuvent donc être considérées comme pouvant être traitées et combinées dans le cadre de l'exécution d'un contrat.

En outre, la formation restreinte relève que l'éventuelle combinaison des données des utilisateurs n'est aucunement nécessaire à l'exécution du contrat dont la société revendique qu'il la lie à eux. En effet, comme l'indiquent les règles de confidentialité, la combinaison des données des utilisateurs n'est que « *susceptible* » de se produire, « *par exemple pour faciliter le partage de vos informations avec des personnes que vous connaissez* ». Cet exemple illustre clairement que le traitement de ces données n'est pas « *nécessaire* » pour que la société puisse exécuter un contrat qui la lierait aux utilisateurs.

Le critère de l'exécution d'un contrat ne peut donc pas davantage être invoqué par la société pour légitimer la combinaison des données des utilisateurs, quel que soit leur statut.

- La société fait enfin valoir qu'il relève de son **intérêt légitime** de pouvoir procéder à la combinaison des données de ses utilisateurs (qu'ils soient authentifiés ou non) afin de leur garantir la meilleure qualité de service possible. Elle soutient que ses intérêts convergent avec ceux de l'utilisateur qui souhaite pouvoir utiliser ses services et bénéficier de la meilleure qualité disponible, si bien que, leurs intérêts respectifs se rejoignant, les siens propres ne peuvent qu'être qualifiés de « *légitimes* ».

De fait, l'amélioration de la qualité de ses services relève incontestablement des intérêts de la société qui peuvent être qualifiés de légitimes au sens de la loi.

Pour autant, la formation restreinte relève que la société a prévu de procéder à la combinaison potentiellement illimitée de toutes les données qu'elle collecte sur chacun de ses utilisateurs, quel que soit leur statut, et alors même qu'elle n'a pas déterminé les durées de conservation qui leur seraient applicables. Cette combinaison est donc de nature à méconnaître les intérêts des utilisateurs et à porter atteinte à leur droit au respect de la vie privée.

Il appartient donc à la formation restreinte de juger si l'intérêt ou les droits et libertés fondamentaux des personnes concernées sont suffisamment préservés en l'espèce pour que l'équilibre qu'a prescrit le législateur entre ces deux catégories d'intérêts soit atteint.

Pour sa part, la société soutient que son intérêt légitime n'outrepasse pas les droits et intérêts de ses utilisateurs dès lors qu'elle leur fournit des outils pour exercer leurs droits, ainsi que de l'information détaillée dans ses règles de confidentialité ou dans les notices contextuelles applicables à certains services.

Sur ce point, la formation restreinte relève que la société a effectivement développé des outils visant à permettre aux utilisateurs d'exercer un contrôle sur la collecte et le traitement de leurs données, mais que leur portée et leur présentation ne sont pas de nature à rendre ce contrôle effectif pour l'ensemble des utilisateurs, quel que soit leur statut.

Ainsi, le « Google Dashboard » qui permet de visualiser les données associées à son compte Google n'est disponible qu'aux utilisateurs authentifiés. S'il permet à ceux-ci de désactiver ou de supprimer l'historique de leurs recherches dans leur compte, il ne leur permet en revanche pas d'effacer toutes les données les concernant dans les journaux des serveurs de Google.

L'outil dit de visualisation du profil publicitaire, s'il est quant à lui accessible à l'ensemble des utilisateurs de la société, tous statuts confondus, n'est cependant plus référencé sur la page principale de la politique de confidentialité, comme ce fut le cas jusqu'au 1<sup>er</sup> mars 2012. Pour y accéder, l'utilisateur doit naviguer à travers plusieurs rubriques successives, dont les intitulés ne permettent pas toujours de comprendre qu'elles mènent à l'outil qui permet de moduler la portée du ciblage dont les utilisateurs sont l'objet (« règles et principes », puis « publicité » dans la rubrique « quelques informations de nature technique », enfin « paramètres des annonces »).

En tout état de cause, ce module ne permet pas aux utilisateurs authentifiés de contrôler effectivement la combinaison de leurs données, encore moins de s'y opposer, puisque ceux-ci ne peuvent que supprimer ou désactiver l'historique de leur navigation et les centres d'intérêt que la société leur a elle-même attribués en fonction de leur comportement en ligne.

Quant aux utilisateurs non authentifiés (actifs ou passifs), ils ne peuvent que gérer les critères de ciblage publicitaire qui les concernent, c'est-à-dire désactiver le ciblage publicitaire ou s'opposer au dépôt de cookies DoubleClick. En outre, ce module ne fonctionne pas sur l'ensemble des appareils, notamment sur les smartphones, et, en tout état de cause, il ne permet pas aux utilisateurs de s'opposer à la combinaison de l'ensemble de leurs données.

Ainsi, contrairement à ce que soutient la société, les droits dont bénéficient les utilisateurs ne leur confèrent pas « *un large pouvoir de contrôle sur le principe même, le moment de la fourniture de données et sur la manière dont celle-ci sont utilisées* » et ne « *lui permettent (pas) de modifier, restreindre ou mettre un terme au traitement de ses données* ».

La formation restreinte estime donc que la société ne peut se prévaloir, pour chacun de ses utilisateurs, d'un recueil du consentement, de la nécessité d'exécution d'un contrat ou d'un juste équilibre entre son intérêt légitime et les droits fondamentaux de ses utilisateurs.

Elle ne respecte donc ni les dispositions de l'article 7 de la loi ni les termes de la mise en demeure sur ce point.

- **Sur les manquements constatés**

En conséquence, eu égard à la persistance des manquements précités, tels qu'ils ont été préalablement constatés dans la mise en demeure prononcée par la Présidente de la Commission le 10 juin 2013, la société Google Inc. verra prononcer à son encontre une sanction pécuniaire d'un montant de 150 000 € (*cent cinquante mille euros*).

La formation restreinte décide également de rendre sa décision publique sur le site Internet de la Commission.

En outre, compte tenu du caractère massif des données collectées par la société, du nombre important et indéterminé des personnes concernées, qui pour nombre d'entre elles ne sont pas en mesure de s'y opposer ni même d'en être informées, la formation restreinte estime nécessaire d'ordonner l'insertion de cette décision sur le site Google.fr.

## PAR CES MOTIFS

Conformément au I de l'article 45 de la loi du 6 janvier 1978 modifiée, la formation restreinte de la CNIL, après en avoir délibéré, décide de prononcer à l'encontre de la société Google Inc. une sanction pécuniaire de 150 000 € (cent cinquante mille euros).

Elle décide également de rendre cette décision publique sur le site de la CNIL.

Elle ordonne par ailleurs à la société de publier à sa charge, sur son service de communication au public en ligne accessible à l'adresse <https://www.google.fr>, le texte suivant :

**« Communiqué : la formation restreinte de la Commission nationale de l'informatique et des libertés a condamné la société Google à 150 000 euros d'amende pour manquements aux règles de protection des données personnelles consacrées par la loi « informatique et libertés ». Décision accessible à l'adresse suivante : <http://www.cnil.fr/linstitution/missions/sanctionner/Google/> ».**

La publication de ce communiqué sera effectuée selon les modalités suivantes :

- La publication est ordonnée pour une durée de quarante huit heures consécutives à compter de 8h00, heure de Paris (France), le septième jour suivant la notification de la présente délibération.
- Le communiqué figurera dans un encart spécifique localisé sur la page accessible à l'adresse <https://www.google.fr>. Cet encart sera inséré sous les boutons « Recherche Google » et « J'ai de la chance » et au dessus du pied de page incluant le bandeau d'information relatif à l'utilisation des cookies. Il sera centré verticalement et horizontalement.
- Le texte publié sera encadré selon le style employé par la société pour les informations présentées en pied de page.
- Le texte de l'encart sera publié dans une taille de caractères qui ne saurait être inférieure à la taille 13 points dans la police dite Arial, sans sheriff. La couleur rgb (177, 68, 54) sera employée pour le mot « Communiqué ». La couleur rgb (102, 102, 102) sera employée pour le reste du texte incluant le pointeur hypertexte.
- L'encart inséré reproduira avec fidélité le texte suivant : « Communiqué : La formation restreinte de la Commission nationale de l'informatique et des libertés a condamné la société Google à 150 000 euros d'amende pour manquements à la loi informatique et libertés. Décision accessible à l'adresse suivante : <http://www.cnil.fr/linstitution/missions/sanctionner/Google/>
- Le texte <http://www.cnil.fr/linstitution/missions/sanctionner/Google/> comportera un pointeur hypertexte activable par l'utilisateur.
- A l'issue de la période déterminée ci-dessus, la société procédera au retrait du texte de l'encart.

La société GOOGLE Inc. dispose d'un délai de deux mois à compter du jour de la notification de la présente décision pour exercer un recours devant le Conseil d'Etat à son encontre.

Fait à Paris, le     - 3 JAN. 2014

La Présidente de la formation restreinte

A handwritten signature in black ink, appearing to read 'DAVAL', with a horizontal line underneath the name.

Claire DAVAL