

16/10/12

REGLES DE CONFIDENTIALITE DE GOOGLE : UNE INFORMATION INCOMPLETE ET UNE COMBINAISON DE DONNEES INCONTROLEE

Après plusieurs mois d'enquête menée par la CNIL sur les nouvelles règles de confidentialité de Google entrées en vigueur le 1er mars dernier, les autorités de protection des données européennes publient leurs conclusions communes. Elles recommandent une information plus claire des personnes et demandent à Google d'offrir aux utilisateurs un meilleur contrôle de la combinaison de données entre les nombreux services qu'elle propose. Enfin, elles souhaitent que Google modifie les outils utilisés afin d'éviter une collecte excessive de données.

Le 24 janvier dernier, Google annonçait l'entrée en vigueur de nouvelles règles de confidentialité et de nouvelles conditions d'utilisation applicables à la quasi-totalité de ses services à partir du 1er mars 2012.

Face aux nombreuses questions soulevées par ces changements, la CNIL a été mandatée par le groupe des CNIL européennes (G29) pour conduire l'enquête sur les nouvelles règles. Deux questionnaires successifs ont été envoyés et Google a fourni ses réponses les 20 avril et 21 juin, plusieurs d'entre elles s'étant avérées incomplètes ou approximatives. En particulier, Google n'a pas fourni de réponses satisfaisantes sur des points essentiels comme la description de tous les traitements de données personnelles qu'il opère ou la liste précise des plus de 60 politiques de confidentialité qui ont été fusionnées dans les nouvelles règles.

L'analyse des réponses de Google ainsi que l'examen de nombreux documents et mécanismes techniques par les experts de la CNIL ont toutefois permis aux autorités européennes de tirer leurs conclusions et de formuler des recommandations à Google.

Tout d'abord, l'analyse menée ne permet pas de s'assurer que Google respecte les principes essentiels de la Directive sur la protection des données personnelles que sont la limitation de finalité, la qualité et la minimisation des données, la proportionnalité et le droit d'opposition. En effet, les nouvelles règles de confidentialité suggèrent l'absence de toute limite concernant le périmètre de la collecte et les usages potentiels des données personnelles. *Les autorités européennes demandent à Google de s'engager publiquement sur le respect de ces principes.*

1. Google ne fournit pas suffisamment d'informations aux utilisateurs sur ses traitements de données personnelles

Avec les règles actuelles, l'utilisateur d'un service Google est incapable de déterminer quelles sont les données personnelles utilisées pour ce service et les finalités exactes pour lesquelles ces données sont traitées.

Exemple : les règles de confidentialité ne font pas de différence de traitement entre le contenu anodin d'une recherche et le numéro de carte de crédit ou les communications téléphoniques de l'utilisateur ; toutes ces données peuvent être utilisées indifféremment pour toutes les finalités mentionnées dans les règles.

De plus, certains utilisateurs comme les utilisateurs passifs (c'est-à-dire ceux qui interagissent avec des services de Google comme la publicité ou les boutons '+1' à partir de sites tiers), ne disposent d'aucune information.

Les CNIL européennes rappellent à Google et aux acteurs de l'internet en général, que des politiques de confidentialité plus courtes ne justifient pas de réduire l'information fournie aux personnes.

- **Les autorités européennes demandent à Google de fournir une information plus claire et plus complète sur les données collectées et les finalités de chacun de ses traitements de données personnelles. Par exemple, les autorités européennes recommandent la mise en place d'une présentation avec trois niveaux de détails qui assurera une information conforme aux exigences de la Directive sans dégrader l'expérience des utilisateurs. L'ergonomie de la lecture des règles pourrait également être améliorée grâce à des présentations interactives.**

2. Google ne permet pas le contrôle par les utilisateurs de la combinaison de données entre ses nombreux services

La **combinaison de données entre services** a été généralisée avec ces nouvelles règles de confidentialité : concrètement toute activité en ligne liée à Google (l'utilisation de ses services, de son système Android ou la consultation de sites tiers utilisant des services Google) peut être rassemblée et combinée.

Les CNIL européennes relèvent que cette combinaison poursuit des finalités différentes comme la fourniture du service demandé par la personne, le développement de nouveaux produits, la sécurité, la publicité, la création du compte Google ou encore la recherche académique. L'enquête a également montré que cette combinaison de données est extrêmement étendue en termes de périmètre et d'historique des données.

Exemple : la simple consultation d'un site tiers comprenant un bouton '+1' est enregistrée et conservée pendant 18 mois au moins et peut être associée aux utilisations des services de Google ; les données collectées par DoubleClick sont associées à un numéro identifiant d'une validité de 2 ans renouvelable.

La législation européenne de protection des données prévoit un cadre précis pour les traitements de données personnelles. Google doit disposer d'une base légale pour réaliser la combinaison de données pour chacune de ces finalités. La collecte doit également demeurer proportionnée aux finalités poursuivies. Or, pour certaines de ces finalités, notamment la publicité, Google ne peut pas s'appuyer sur le consentement de la personne, l'intérêt légitime de Google ou l'exécution d'un contrat.

- **Google doit donc modifier ses pratiques quand les données sont combinées pour ces finalités. Il s'agit notamment de :**
 - **renforcer le consentement des personnes pour la combinaison des données pour les finalités d'amélioration de service, de développement de nouveaux services, de publicité et d'analyse de fréquentation. Cela pourrait être fait en donnant la possibilité aux utilisateurs de choisir quand leurs données sont combinées, par exemple avec des boutons dédiés sur les pages des services (cf. bouton « Search Plus Your World ») ;**
 - **offrir un meilleur contrôle des utilisateurs sur la combinaison de données en centralisant et simplifiant le droit d'opposition (opt-out) et en leur permettant de choisir pour quels services leurs données sont combinées ;**
 - **adapter les outils utilisés par Google pour la combinaison de données afin de limiter cette combinaison aux finalités autorisées, par exemple en distinguant les outils utilisés pour la sécurité et ceux utilisés pour la publicité.**

3. Google ne précise pas les durées de conservation

Google a refusé de s'engager sur des durées de conservation pour les données personnelles qu'il traite.

L'ensemble des recommandations des CNIL européennes a été remis à Google afin de lui permettre de **mettre à niveau ses pratiques en matière de politique de confidentialité**. Ce courrier est signé individuellement par 27 Autorités de protection des données européennes, ce qui constitue une première et une avancée considérable dans la mobilisation des autorités européennes.

Plusieurs de ces recommandations sont également soutenues par des autorités membres de l'APPA (Asia Pacific Privacy Authorities) et la Commissaire à la protection de la vie privée du Canada a fait part des préoccupations similaires au sujet de diverses activités de Google.

La CNIL, l'ensemble des autorités de protection des données européennes et les autorités d'autres régions du monde attendent de Google qu'il prenne des mesures effectives et publiques pour se mettre en conformité rapidement et s'engage sur la mise en œuvre de ces recommandations.
