ANNEXE

REGLES DE CONFIDENTIALITE DE GOOGLE : PRINCIPALES CONCLUSIONS ET RECOMMANDATIONS

SOMMAIRE

I. PRINCIPALES CONCLUSIONS

1) CADRE JURIDIQUE

Les services de Google[1] sont mis à la disposition des personnes physiques dans l'Union européenne et les critères de la Directive européenne pour la détermination du droit applicable sont remplis. La législation européenne sur la protection des données s'applique donc aux traitements de données personnelles de Google.

Google met en œuvre plusieurs traitements de données personnelles dans le cadre de la fourniture de ses services : un traitement spécifique peut être associé à chaque service et Google met en œuvre d'autres traitements à des fins transversales, comme la sécurité, la recherche, etc.

Le Groupe de l'Article 29 a identifié trois types d'utilisateurs des services de Google :

- Les utilisateurs authentifiés (Gmail, Google Play, Docs, Google+, etc.)
- Les utilisateurs non authentifiés (Search, Maps, Youtube, etc.)
- Les utilisateurs passifs (DoubleClick, Analytics, boutons « +1 »)[2]

2) INFORMATION

Les Règles de confidentialité de Google ne respectent pas l'obligation d'information, énoncée à la section IV de la Directive sur la protection des données.

En premier lieu, Google fournit des informations incomplètes ou approximatives sur les finalités et les catégories des données collectées. Les Règles de confidentialité mêlent des engagements particulièrement larges et des exemples qui limitent la portée de ces engagements et faussent la perception des utilisateurs quant à la portée exacte des pratiques de Google. Des informations supplémentaires sont disponibles dans des notes de confidentialité intégrées aux produits (« in-product privacy notices »), dans le Centre d'aide ou dans des blogs, mais les informations figurant dans ces documents sont incohérentes d'une source ou d'une langue à l'autre, peuvent être modifiées à tout moment et sont parfois difficiles à comprendre. Les Règles

[1] Les services de Google sont fournis dans 22 des 23 langues officielles de l'Union européenne (toutes les langues à l'exception du maltais – d'autres langues régionales ou nationales officielles peuvent également être disponibles) et les services de Google sont disponibles dans 25 des 27 principaux domaines de premier niveau des États membres (tous les domaines à l'exception de .mt et de .cy – google.eu n'est pas disponible non plus). Outre les services de Google disponibles en ligne, des appareils exploitant des logiciels de Google (principalement des téléphones Android) sont commercialisés dans la majorité, si ce n'est la totalité des États membres. Google possède également des sociétés nationales établies dans plusieurs pays européens (par exemple au Royaume-Uni, en Irlande et en France), qui participent dans une certaine mesure à des opérations commerciales, de recherche et développement et de relations publiques. En Europe, le siège de Google est situé à Dublin, en Irlande. Google utilise des serveurs situés en Union européenne pour fournir ses services, dont deux grands centres de données en Belgique et en Finlande. Google emploie également des cookies et d'autres moyens, stockés sur les appareils des utilisateurs, pour fournir ses services.

[2] Les utilisateurs passifs, selon la définition figurant dans le questionnaire envoyé le 16 mars, sont des utilisateurs qui ne sollicitent pas directement un service Google, mais dont les données sont malgré tout collectées, généralement par le biais de plateformes publicitaires tierces, d'analyses ou de boutons +1.

de confidentialité principales constituent le seul document traçable (c'est-à-dire dont les versions antérieures demeurent disponibles). Le Groupe de l'Article 29 note en particulier que les plus de soixante Règles de confidentialité spécifiques à des produits qui ont été fusionnées dans les nouvelles Règles de confidentialité ne sont plus disponibles et que Google n'a pas fourni la liste de cette soixantaine de Règles de confidentialité.

Concernant l'information sur les finalités, les finalités présentées dans les Règles de confidentialité ne sont pas suffisamment détaillées et ne respectent pas le principe de limitation des finalités. Soit les finalités indiquées dans les Règles sont les finalités réelles des traitements de Google, auquel cas Google ne respecte pas l'article 6(b) de la Directive (parce que les finalités ne sont pas « déterminées et explicites »), soit les données personnelles sont traitées pour des finalités plus spécifiques qui ne sont pas mentionnées par Google dans les Règles de confidentialité ni dans ses réponses aux questionnaires : dans ce cas, Google ne respecte pas l'obligation d'information visée aux articles 10 et 11 de la Directive sur la protection des données.

Concernant l'information sur les catégories de données traitées par les services, les catégories décrites dans les Règles de confidentialité sont trop larges et ne fournissent pas une information appropriée à la personne concernée lorsque celle-ci utilise un service particulier.

L'utilisation réelle des données par Google dans le cadre de chaque service peut ne pas être excessive mais, dans ce cas, les informations fournies sont insuffisantes au regard des prescriptions imposées par les articles 10 et 11 de la Directive. Google n'a également pas fourni d'éléments susceptibles de vérifier le respect du principe de minimisation de données. En particulier, Google n'a pas indiqué quelles données sont partagées entre quels services.

Concernant les utilisateurs passifs, les utilisateurs ne sont généralement pas informés que Google traite des données personnelles, comme les adresses IP et les cookies. Les informations dépendent des règles de confidentialité propres à chaque site web et spécifient rarement en détail le traitement opéré par Google.

3) COMBINAISON DE DONNEES ENTRE LES SERVICES

Google utilise de nombreux outils pour combiner les données entre les services :

- Le Compte Google associé à chaque utilisateur authentifié
- Le cookie PREF associé à chaque interaction avec un site web du domaine google.com (y compris les boutons « +1 » sur les sites web tiers)
- Le cookie DoubleClick associé aux interactions sur des sites web tiers affichant des annonces DoubleClick
- Le cookie Google Analytics utilisé par des sites web tiers
- Les identifiants mobiles utilisés pour remplacer des cookies sur certaines applications mobiles

La combinaison de données mise en œuvre par Google est très large, car elle couvre l'ensemble de l'activité des personnes concernées sur les sites Google[3] et de l'activité sur des sites web tiers (boutons « +1 », DoubleClick). En outre, Google stocke les données sur de longues périodes de temps : 18 mois d'historique de recherche pour le cookie PREF, 2 ans pour le cookie publicitaire. Enfin, les risques associés à la combinaison de données entre services sont élevés pour les personnes concernées : violation de données, malveillance interne, réquisitions judiciaires, etc.

Le Groupe de l'Article 29 a identifié huit différentes finalités pour la combinaison de données entre les services de Google :

- La fourniture de **services où l'utilisateur demande la combinaison des données (cas n° 1)** (ex. : Contacts et Gmail)
- La fourniture de services demandés par l'utilisateur, mais où la combinaison des données s'applique **sans que l'utilisateur n'en soit directement informé (cas n° 2)** (ex. : personnalisation de résultats de recherche)
- **Finalité de sécurité (cas n° 3)**
- **Finalité de développement de produits et d'innovation marketing (cas n° 4)**
- La mise à disposition du **Compte Google (cas n° 5)**
- **Finalité de publicité (cas n° 6)**
- **Finalité d'analyse de fréquentation (cas n° 7)**
- **Finalité de recherche universitaire (cas n° 8)**

Cependant, les outils employés par Google, comme le Compte Google ou le cookie PREF, ont des règles d'utilisation qui sont indépendantes des finalités, par exemple l'anonymisation des journaux de serveur au bout de 18 mois. Google ne distingue pas les différentes finalités pour la combinaison de données et ne souscrit pas explicitement au principe de limitation des finalités.

Par ailleurs, le Groupe de l'Article 29 a examiné la légitimité de la combinaison de données au regard des bases légales exposées à l'article 7 de la Directive, en l'occurrence le « consentement », l'« exécution d'un contrat » et « l'intérêt légitime ».

Pour quatre des huit finalités susvisées, le Groupe de l'Article 29 a établi l'absence de base légale **pour la combinaison de données entre services**[4]. C'est le cas de la fourniture de services où la combinaison des données s'applique sans que l'utilisateur n'en soit directement informé (cas n° 2) et des finalités de développement de produits et d'innovation marketing (cas n° 4), de publicité (cas n° 6) et d'analyse de fréquentation (cas n° 7).

Pour ces finalités, il n'y a pas de **consentement valable** de l'utilisateur, ne serait-ce que parce que l'utilisateur n'a pas connaissance de la portée exacte de la combinaison de données. **Les droits fondamentaux et les libertés des personnes concernées prévalent sur l'intérêt qu'a Google** de mettre en œuvre la combinaison extensive des données susvisée et, par conséquent, la base légale de l'intérêt légitime ne peut pas s'appliquer, sauf si Google limite clairement la portée et la durée de la combinaison de données et garantit aux personnes concernées des droits simples et effectifs. Enfin, Google n'a pas fourni d'exemples significatifs de combinaison de

[3] Google a en Europe une part de marché d'environ 90 % sur les moteurs de recherche et d'environ 50 % sur les systèmes d'exploitation de smartphones.
[4] L'enquête n'évalue pas la base légale des traitements de Google en dehors de la combinaison de données.

données réalisée pour l'exécution d'un contrat qui auraient pu justifier une collecte et une combinaison de données aussi larges.

Google ne peut pas prétendre utiliser les données issues d'un service donné pour ces finalités sans base légale valable. Afin de remédier à cette situation, **Google devrait demander le consentement des personnes concernées pour la combinaison de données réalisée pour ces finalités et prévoir pour les utilisateurs des mécanismes supplémentaires de contrôle de cette combinaison.**

Les nouvelles Règles de confidentialité s'appliquent également aux utilisateurs finaux de l'offre Google Apps (Free). Dans ce cas, le consentement peut ne pas être valable, car la personne concernée est probablement un salarié du client de Google qui choisit de recourir à cette offre.

Plus généralement et quelle que soit la finalité, **la combinaison de données entre services doit respecter les principes de la proportionnalité, de limitation des finalités, de minimisation de données et du droit d'opposition**. **Google ne souscrit pas publiquement à ces principes** et n'a pas apporté de réponse précise et définitive à ces questions : rien ne garantit que seules les données nécessaires à la finalité sont combinées, l'information des personnes est insuffisante (*cf.* la section « Information ») et les mécanismes actuels d'opt-out sont trop complexes et inefficaces. Par exemple, un utilisateur mobile authentifié de Google+ qui ne veut pas d'annonces personnalisées doit aujourd'hui réaliser six actions différentes pour désactiver cette fonctionnalité. En outre, certains de ces mécanismes ne suppriment pas la collecte de données, mais empêchent uniquement l'affichage de contenus personnalisés. Enfin, il n'y a pas de mécanismes d'opt-out pour les finalités de recherche, d'innovation marketing et de développement de produits, hormis en n'utilisant pas les services.

Pour les **utilisateurs passifs,** Google ne respecte pas l'article 5(3) de la Directive relative à la vie privée et aux communications électroniques concernant les cookies envoyés par DoubleClick, les boutons « +1 » ou les services Google Analytics sur des sites web tiers. Un consentement informé est nécessaire avant que ces cookies ne puissent être utilisés à des fins de combinaison de données entre services.

En ce qui concerne **Google Analytics** et la combinaison de données à des fins d'analyse de fréquentation, des mécanismes spécifiques de protection ont été mis en place pour les utilisateurs allemands : la combinaison de données entre services est exclue, un contrat spécifique est signé entre Google et le site web et les clients peuvent automatiquement anonymiser l'adresse IP partagée avec Google. Ces conditions peuvent assurer une protection adéquate des données personnelles et devraient être étendues à tous les États membres européens.

4) DUREE DE CONSERVATION

En dépit des questions précises et réitérées soumises par le Groupe de l'Article 29, Google n'a pas été en mesure de fournir une durée maximale ou habituelle de conservation des données personnelles traitées. Cette absence de réponse remet en cause l'efficacité des mécanismes d'opt-out et des actions de suppression sollicitées par les utilisateurs.

Le Groupe de l'Article 29 encourage Google à respecter le principe d'une durée de conservation strictement limitée au regard des finalités.

II. RECOMMANDATIONS

Compte tenu des conclusions de l'enquête, Google devrait mettre en œuvre les recommandations suivantes pour se conformer à la législation relative à la protection des données.

1) INFORMATION

Afin de remédier à l'insuffisance d'information sur les traitements de Google, **Google doit fournir des informations complètes sur ses traitements en détaillant pour chaque traitement les finalités exactes et les données collectées (y compris les données provenant d'autres services).**

Cette information doit spécifier les finalités et les catégories de données traitées de manière claire et précise. Le traitement en soi doit être réalisé dans le strict respect des règles de proportionnalité et de minimisation des données, lesquelles règles doivent être reflétées dans l'information fournie.

En outre, les documents d'information relatifs aux différents traitements ne doivent pas être modifiés sans le consentement de l'utilisateur et, dans ce cas, une information claire et complète doit être communiquée à l'utilisateur sur les modifications prévues, entre autres ; de surcroît, ces avis devraient être traçables.

En pratique, le Groupe de l'Article 29 recommande de **définir une architecture des politiques de confidentialité** capable de fournir une information simple et complète sur tous les traitements. Les utilisateurs doivent avoir une bonne visibilité sur cette architecture et être en mesure d'y naviguer d'une façon conforme à leurs attentes.

L'architecture pourrait adopter **les trois niveaux suivants :**

Premièrement, **des notes de confidentialité intégrées aux produits et des notes interstitielles** pourraient être rédigées pour indiquer aux utilisateurs que leurs données sont traitées lorsqu'ils utilisent les services et, en particulier, lorsqu'ils lancent un nouveau service pour la toute première fois. Certains outils, comme le bouton permettant de basculer sur « Search Plus Your World » ou les « butter-buttons » utilisés pour informer des modifications

des Règles de confidentialité, constituent de bons exemples d'information directe et opportune. Google devrait développer des procédures internes pour vérifier systématiquement le niveau d'information basique des utilisateurs en matière de protection des données personnelles pour chacun de ses services actuels et futurs.

Deuxièmement, les **Règles de confidentialité actuelles** devraient être présentées comme un guide général sur les traitements de Google et des renvois devraient être insérés vers des informations plus détaillées sur les différents traitements (« déclarations de confidentialité spécifiques aux produits »). En outre, le Groupe de l'Article 29 recommande de distinguer clairement les engagements des exemples illustratifs, car ces derniers ont tendance à induire les utilisateurs en erreur quant au périmètre exact des engagements. Dans l'idéal, les exemples devraient couvrir différents cas d'utilisation. Les Règles de confidentialité devraient inclure tous les types de catégories de données, y compris les données biométriques, car la reconnaissance faciale n'est pas mentionnée dans les Règles actuelles.

Troisièmement, des **notes de confidentialité spécifiques aux produits** devraient être mises à disposition. Ces notes devraient détailler pour chaque traitement et pour chaque service : les données qui sont traitées, les finalités du traitement, les destinataires et la manière dont les utilisateurs peuvent accéder à leurs données. Les finalités générales, comme la recherche et la sécurité, pourraient être présentées séparément avec des garanties détaillées pour ces finalités. Les versions précédentes des Règles de confidentialité et des notes de confidentialité spécifiques aux produits devraient être constamment tenues à la disposition des utilisateurs.

Plus généralement, Google devrait mettre au point des **présentations interactives** permettant aux utilisateurs d'explorer le contenu des notes de confidentialité sans avoir à lire de longs documents linéaires.

Enfin, Google devrait fournir des informations additionnelles et précises sur les données suivantes, qui peuvent avoir un impact important sur la vie privée des utilisateurs :

- Localisation géographique
- Données bancaires et sur les cartes de crédit
- Identifiant unique de terminaux
- Téléphonie

Il doit être clairement et simplement expliqué aux utilisateurs quand, pourquoi et comment ces données sont collectées et comment ils peuvent s'opposer à la collecte, au stockage ou à la combinaison de ces données.

i. CAS PARTICULIER DES UTILISATEURS MOBILES

Les utilisateurs mobiles rencontrent d'autres problèmes encore lorsqu'ils utilisent les services de Google sur de petits écrans, avec des interactions limitées. Un grand nombre des fonctionnalités susvisées peut ne pas apparaître ou ne pas être disponible sur des écrans mobiles, en particulier les notes de confidentialité intégrées aux produits ou les présentations interactives.

Google doit fournir des informations adaptées à ces utilisateurs, éventuellement au moyen d'outils spécifiques pouvant inclure des applications dédiées ou des réglages sur Android.

ii. CAS PARTICULIER DES UTILISATEURS PASSIFS

Concernant les utilisateurs passifs, les informations sont principalement fournies par des sites web tiers sur lesquels des services de Google sont mis en œuvre. Google doit donc s'assurer que ces utilisateurs sont correctement informés des traitements qui les concernent.

2) COMBINAISON DE DONNEES

Concernant la combinaison de données, Google ne dispose pas de fondement juridique pour certaines finalités. De plus, les informations sur la combinaison de données sont particulièrement minces et les recommandations de la section précédente s'appliquent : Google doit avant tout améliorer l'information afin de spécifier clairement les données qui sont combinées entre services et les finalités de ces combinaisons.

i. FINALITES AYANT UN FONDEMENT JURIDIQUE POUR LA COMBINAISON DE DONNEES (CAS N° 1, N° 3, N° 5, N° 8)

Pour utiliser les données en provenance d'autres services, Google doit adopter une **approche qui prend en compte le respect de la vie privée dès la conception (« Privacy by Design ») :** des ensembles limités de données personnelles devraient être utilisés et l'anonymisation devrait être mise en œuvre, dès que possible (principe de la minimisation des données).

Des **fonctions simples d'opt-out** doivent être mises à disposition pour des finalités appliquant le droit d'opposition, c'est-à-dire la fourniture de services demandés par l'utilisateur (cas n° 1), la recherche (n° 8) et le profil Google (n° 5). En général, la mise en place d'un opt-out pour les finalités de sécurité demande une approche prudente, afin d'éviter les abus.

Les **durées de conservation** doivent être adaptées à la finalité.

ii. FINALITES N'AYANT PAS DE FONDEMENT JURIDIQUE POUR LA COMBINAISON DE DONNEES (CAS N° 2, N° 4, N° 6, N° 7)

Google doit obtenir le consentement indubitable des personnes concernées pour ces finalités et limiter clairement le périmètre de la combinaison de données de manière proportionnée au regard des finalités poursuivies.

Dans ce contexte, l'inclusion d'un nouveau service dans la combinaison de données ou dans une nouvelle finalité requiert un consentement explicite (exemple : Google Now), qui peut être aisément obtenu la première fois qu'un utilisateur souhaite utiliser le nouveau service.

Le Groupe de l'Article 29 conseille également à Google de concevoir de nouveaux outils permettant aux utilisateurs de contrôler les services susceptibles de combiner des données. Ces contrôles peuvent inclure :

- Des paramètres spécifiques dans Google Dashboard pour les utilisateurs authentifiés
- Un consentement explicite et un contrôle amélioré sur les cookies (et les données collectées) pour les utilisateurs non authentifiés et passifs

iii. RECOMMANDATIONS PRATIQUES

Les recommandations pratiques suivantes pourraient donc être mises en œuvre par Google afin de garantir la conformité légale de la combinaison de données :

1. Google devrait **simplifier les mécanismes d'opt-out** et prévoir de nouveaux outils pour appliquer le droit d'opposition à la combinaison de données pour certaines des finalités susvisées. À cet égard, les utilisateurs devraient avoir une compréhension claire des finalités de la combinaison de données.

2. Google devrait **différencier les finalités de la combinaison de données** au moyen d'outils appropriés : l'utilisation de l'identifiant du cookie PREF pour différentes finalités devrait être abandonnée et des cookies (ou autres outils) pourraient être créés pour chaque finalité (sécurité, publicité, améliorations du service) avec des règles de conservation et des droits d'accès liés aux finalités.

3. Google devrait **collecter le consentement explicite pour la combinaison de données** pour les finalités d'améliorations de service sans que l'utilisateur n'en soit directement informé, de développement de produits et d'innovation marketing, de publicité et d'analyse de fréquentation.

4. Google devrait centraliser **les mécanismes d'opt-out dans un emplacement unique** pour les utilisateurs authentifiés et non authentifiés.

5. Google devrait proposer aux utilisateurs authentifiés la possibilité de **contrôler dans quel service ils sont authentifiés** lorsque des services sont disponibles sans authentification (exemple : Search, Maps ou Youtube), par exemple en définissant un paramètre dans leur compte.

6. Google devrait limiter la collecte et la combinaison de données provenant des utilisateurs passifs, excepté pour des finalités de sécurité.

7. Google doit **appliquer l'article 5(3)** de la Directive relative à la vie privée et aux communications électroniques pour les utilisateurs passifs, notamment les instructions formulées dans l'Avis du G29 sur l'exemption de consentement pour les cookies.

8. Concernant les finalités d'analyse de fréquentation, Google devrait aussi **étendre à tous les utilisateurs européens le processus mis au point en Allemagne** (information améliorée des personnes concernées par le site web, utilisation limitée des données pour les finalités d'analyse de fréquentation et anonymisation des adresses IP).

iv. CAS PARTICULIER DES UTILISATEURS DE GOOGLE APPS (EDITION GRATUITE)

Pour les utilisateurs finaux de Google Apps, l'utilisation d'un Compte Google est décidée par le client de Google Apps (généralement la société employeur des utilisateurs finaux) : le consentement peut donc ne pas être valable. Google devrait appliquer des restrictions à la combinaison de données entre les services et cette combinaison devrait être limitée aux services inclus dans l'offre Google Apps.

3) DUREE DE CONSERVATION

Google devrait définir plus clairement la durée de conservation des données personnelles, notamment pour les actions suivantes : suppression d'un contenu particulier, désabonnement à un service spécifique, suppression du compte.

III. AUTRES

1) REGLES CONCERNANT LES NOMS

Google doit informer plus clairement les nouveaux utilisateurs de la possibilité d'ouvrir un compte Google sans fournir son vrai nom.

2) RECONNAISSANCE FACIALE

Google doit compléter les Règles de confidentialité en mentionnant que les données biométriques peuvent être traitées, et préciser les conditions de la collecte et du stockage des gabarits faciaux.

3) TRANSFERTS INTERNATIONAUX ET SPHERE DE SECURITE

La présente analyse n'a pas examiné la conformité de Google aux règles européennes en matière de transferts internationaux et à l'accord « Safe Harbor » entre les États-Unis et l'Union européenne.