

Institutions financières
Énergie
Infrastructure, mines et commodités
Transport
Technologie et innovation
Sciences de la vie et santé

NORTON ROSE FULBRIGHT

Protection des données

PREMIERE AMENDE RGPD DE PLUSIEURS MILLIONS D'EUROS

Janvier 2019

GDPR



Google LLC condamnée à une amende de 50 millions d'euros pour infraction à ses obligations en matière de transparence et de consentement relatives à l'utilisation de données personnelles dans le cadre de publicités personnalisées

Le 21 janvier 2019, la Commission Nationale de l'Informatique et des Libertés (CNIL) a infligé une amende consécutive à l'entité américaine de Google, Google LLC. Cette sanction fait suite aux plaintes déposées dès l'entrée en vigueur du Règlement (UE) 2016/679 sur la protection des données (RGPD) par deux associations de défense des droits des consommateurs, None of Your Business et La Quadrature du Net.

Nous nous concentrons ici sur quatre aspects clés de la décision : a) pourquoi la Commission irlandaise de protection des données (Irish Data Protection Commission - DPC) n'a pas traité l'affaire ; b) les manquements relatifs au mécanisme de consentement mis en place ; c) les manquements relatifs à la politique de confidentialité ; et d) le montant de l'amende.

Autorité chef de file

Google a fait valoir que la DPC irlandaise aurait dû traiter les plaintes qui ont mené à cette décision.

La CNIL :

- a clairement indiqué que, pour que le guichet unique soit une option, l'établissement prétendant être l'établissement principal au sein de l'UE et donc situé dans l'État membre de l'autorité chef de file, doit avoir un pouvoir de décision vis-à-vis des traitements de données à caractère personnel en cause ;
- a laissé de côté une série d'activités entreprises en ou depuis l'Irlande, y compris la vente de prestations publicitaires, pour se concentrer sur la question de savoir si Google Irelande Ltd avait un pouvoir de décision sur les opérations de traitement couverts par la politique de confidentialité présentée à l'utilisateur lors de la création de son compte, à l'occasion de la configuration de son téléphone mobile sous Android ;
- a conclu que de telles décisions ont été prises par Google LLC aux États-Unis, notant de plus

que Google Ireland Ltd n'est pas mentionnée dans les Règles de confidentialité comme l'entité qui prend les décisions relatives aux traitements concernés, qu'elle n'a pas désigné de délégué à la protection des données qui serait en charge des traitements de données personnelles qu'elle pourrait mettre en œuvre dans l'Union européenne, et qu'elle n'a pas participé à l'élaboration du système d'exploitation Android.

- En conséquence, toute autorité européenne de protection des données (APD) avait la capacité d'enquêter et de faire appliquer la loi en ce qui concerne les infractions commises sur son territoire, et la CNIL pouvait traiter les infractions commises en France. L'amende a été infligée à Google LLC mais envoyée à Google France pour sa mise en œuvre (probablement en tant que représentant présumé ou agréé de Google LLC auprès de l'UE).

Notre point de vue

Il est conseillé aux responsables de traitement de revoir les décisions prises en matière d'autorité chef de file, en se rapportant aux lignes directrices du groupe de travail de l'article 29¹. Il est possible qu'il y ait différentes autorités chefs de file pour différentes activités de traitement au sein d'une même entité ou d'un même groupe, ce qui peut rendre la tâche complexe.

Si le traitement est contrôlé en dehors de l'UE, il est nécessaire de désigner un représentant au sein de l'UE (ce qui permet de notifier les violations de données personnelles uniquement à l'autorité située dans l'État membre du représentant). Une position claire à ce sujet est essentielle pour la notification des violations, étant donné que la décision quant à l'autorité à laquelle notifier (voire parfois, les autorités auxquelles notifier) doit être prise dans les 72 heures.

Manquements relatifs au mécanisme de consentement mis en place

Lors de la configuration d'un appareil Android, l'utilisateur est invité à créer ou à se connecter à un compte Google. Pour éviter de créer un compte, l'utilisateur doit cliquer sur "Ignorer", puis est

¹ https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

informé des avantages à utiliser un compte Google avec l'appareil Android avant de pouvoir continuer.

Le processus de création du compte exige que l'utilisateur accepte les « Règles de confidentialité et conditions d'utilisation » de Google. Le processus exige que l'utilisateur fasse défiler un bref résumé du traitement avec un lien "Plus d'options" vers une autre page, qui donne aux utilisateurs la possibilité de désactiver plusieurs opérations de traitement, y compris à des fins de personnalisation des annonces, par le biais de cases à cocher. La case à cocher pour la personnalisation des annonces est pré-cochée.

Une fois que l'utilisateur a accepté les « Règles de confidentialité et conditions d'utilisation », il reçoit un message électronique l'informant qu'il a le contrôle de ses paramètres de confidentialité et qu'il peut les modifier à tout moment et créer des rappels pour se souvenir de vérifier ces paramètres. Si l'utilisateur n'a pas modifié la case à cocher de personnalisation des annonces, une fenêtre pop-up s'affiche pour rappeler que le compte est configuré pour inclure des fonctionnalités de personnalisation.

La CNIL a refusé de reconnaître que ce mécanisme permet un consentement spécifique et univoque pour les raisons suivantes :

- L'utilisateur est invité à consentir à un très large éventail de traitements ;
- Afin de rendre le consentement plus granulaire, l'utilisateur est obligé de réaliser une action particulière (cliquer sur « Plus d'options ») pour accéder à une autre couche d'informations plus détaillée ; et
- La case de personnalisation des annonces est pré-cochée. Pour être conforme, le parcours menant au consentement aurait dû offrir à l'utilisateur la possibilité de consentir spécifiquement à chaque finalité, les options de consentement spécifique devant être décochées, avant d'offrir une case finale décochée permettant de consentir ou non à toutes les différentes fins.

Notre point de vue

La position de la CNIL sur le consentement fait écho à la décision Vectaury dans laquelle elle donnait les mêmes arguments relatifs à la collecte

du consentement, et aux cases pré-cochées. Si les méthodes de collecte de consentement pour le marketing par message électronique sont maintenant généralement conformes à ces exigences, la position est toutefois moins claire dans le domaine de la technologie publicitaire (« ad tech »), où il est courant de prévoir un consentement groupé à différentes finalités, par le biais d'un seul bouton "J'accepte".

Depuis l'entrée en vigueur du RGPD, la CNIL a adressé cinq mises en demeure à des entreprises de l'ad tech concernant leurs mécanismes de collecte de consentement. Ces sociétés et les éditeurs devraient donc à présent évaluer si d'éventuels changements sont nécessaires.

Manquements relatifs à la politique de confidentialité

La documentation Google relative à la protection de la vie privée doit couvrir un grand nombre de produits et d'usages de données et les efforts de la société pour rendre cette documentation digeste et accessible n'ont pas été jugés satisfaisants par la CNIL.

Cette dernière estime que les traitements de Google sont "particulièrement massifs et intrusifs" et susceptibles de révéler avec un degré de précision important de nombreux aspects parmi les plus intimes de la vie des personnes, ce qui exige que sa politique de confidentialité soit particulièrement claire et intelligible.

La CNIL a constaté les manquements suivants :

- La politique de confidentialité ne reflète pas l'ampleur des traitements et le degré d'intrusion dans la vie privée des utilisateurs qu'ils sont susceptibles d'emporter – Google utilise des descriptions générales et vagues ;
- L'architecture générale de l'information choisie par Google oblige l'utilisateur à multiplier les clics nécessaires pour accéder aux différents documents, puis à consulter attentivement un grand nombre d'informations, les recouper et les comparer afin de comprendre quelles données sont collectées en fonction des différents paramètres choisis. L'utilisateur doit accomplir de nombreuses actions et combiner plusieurs ressources documentaires (cinq actions sont nécessaires pour comprendre la

personnalisation des publicités et six pour comprendre la géolocalisation), ce qui rend impossible d'appréhender facilement la totalité des traitements ;

- Il n'est pas possible pour l'utilisateur, avant la création de son compte Google, de mesurer la portée des principaux traitements, potentiellement extensive, sur sa vie privée. La CNIL a reconnu qu'une information exhaustive serait contre-productive dès le premier niveau d'informations, mais a suggéré que Google fournisse un meilleur aperçu des combinaisons de données et des activités de traitement réalisées à ce stade ;
- La CNIL constate un défaut de clarté quant à la base juridique des traitements de personnalisation de la publicité car, à la lecture des Règles de confidentialité, certains semblent être fondés sur le consentement (comme Google l'a déclaré à la CNIL), et d'autres (les annonces géo localisées par exemple) semblent être fondés sur des intérêts légitimes ;
- Le titre de la section des Règles de confidentialité portant sur les durées de conservation des données est "Exporter et supprimer vos informations". Pour la CNIL, les utilisateurs ne peuvent s'attendre à ce que cette section inclue les périodes de conservation. De plus, certaines catégories de conservation ne précisent pas la durée ni les critères utilisés pour déterminer la durée.
- Ces manquements signifient également que le consentement des utilisateurs pour les traitements de personnalisation de la publicité n'est pas suffisamment éclairé.

Notre point de vue

Il devrait être plus facile d'éviter de tels manquements pour les responsables du traitement dont les pratiques de collecte des données sont moins étendues et moins complexes.

Il convient de veiller (en rendant les politiques plus compréhensibles pour les consommateurs) à ce que les principales rubriques d'une politique de protection de la vie privée classique restent reconnaissables dans l'aperçu ou le résumé.

Les responsables de traitement qui utilisent la superposition des couches d'informations devraient envisager d'avoir un lien vers un document linéaire contenant l'ensemble de la politique de protection de la vie privée afin qu'il soit plus facile pour les organismes de réglementation de vérifier les points dont ils exigent qu'ils soient fournis.

Ne tentez pas d'obtenir l'accord des utilisateurs à la politique de confidentialité dans le but d'obtenir un consentement généralisé à tous les traitements. Veillez plutôt à ce que seuls les aspects du traitement nécessitant un consentement soient couverts par la clause de consentement.

La période de grâce (si elle existait) pour insérer les durées de conservation dans les politiques de confidentialité semble être terminée, et les responsables de traitement doivent maintenant envisager de détailler cette section dans leurs politiques.

Niveau de l'amende

Une amende de 50 millions d'euros est une amende massive au regard des normes de l'UE. La CNIL a expliqué ce montant par les raisons suivantes :

- Le caractère central des principes d'information, de transparence et de base légale pour la protection des données, et le fait que les dispositions du RGPD relatives à ces obligations figurent parmi les dispositions dont la méconnaissance est la plus sévèrement sanctionnée;
- L'atteinte n'est pas ponctuelle, spontanée ou passée : elle est continue et toujours en cours à la date de la décision de la CNIL ;
- Un très grand nombre de données à caractère personnel, concernant un très grand nombre de personnes (des millions d'utilisateurs en France), a été collecté à partir de multiples sources ;
- Les informations obtenues sont donc particulièrement éclairantes sur les habitudes de vie des personnes concernées, leurs opinions, leurs interactions sociales et, par conséquent, affectent étroitement leur identité et leur intimité ;
- Le défaut de transparence et l'absence de consentement aux traitements de personnalisation de la publicité va à l'encontre

des aspirations légitimes des personnes qui souhaitent conserver le contrôle de leurs données personnelles - ce contrôle étant l'un des axes majeurs du RGPD; et

- Le modèle économique de Google repose en partie sur les annonces personnalisées. Une responsabilité particulière incombe donc à la société au titre du RGPD.

Notre point de vue

L'amende ne concernant que les traitements français, reste à savoir si d'autres DPA chercheront à imposer des amendes pour leur territoire.

Aucune indication n'est donnée sur la manière dont l'amende a été calculée, ni sur l'importance de chacun des facteurs cités. Le jugement d'appel pourrait faire la lumière sur ces points².

Compte tenu de l'historique de la relation entre la CNIL et Google en ce qui concerne sa politique de protection de la vie privée et l'étendue de ses activités de traitement, cette amende ne signifie pas nécessairement que les amendes infligées aux petits acteurs augmenteront en fonction de facteurs similaires. Toutefois cette première "méga" amende RGPD représente une nouvelle référence pour les violations flagrantes ou massives.

Enfin, il semblerait que toute période non officielle d'amnistie quant à la mise en œuvre des dispositions du RGPD ait pris fin.

Pour plus d'informations

Vous trouverez le communiqué de presse de la CNIL sur la décision [ici](#) et la décision complète [ici](#).

Nous vous invitons à suivre nos articles sur cette affaire et plus largement, les actualités en matière de protection des données et cybersécurité sur notre blog www.dataprotectionreport.com

² Google a annoncé son intention de faire appel de la décision devant le Conseil d'Etat.

Contacts



Nadège Martin

Norton Rose Fulbright LLP
Associée, Avocat au barreau de Paris
Tel +33 1 56 59 53 74
Nadege.mamrtin@nortonrosefulbright.com



Cécile Auvieux

Norton Rose Fulbright LLP
Collaboratrice, Avocat au barreau de Paris
Tel +33 1 56 59 53 93
cecile.auvieux@nortonrosefulbright.com



Geoffroy Coulouvrat

Norton Rose Fulbright LLP
Collaborateur, Avocat au barreau de Paris
Tel +33 1 56 59 52 98
Geoffroy.coulouvrat@nortonrosefulbright.com



Nilofar Moini Shabestari

Norton Rose Fulbright LLP
Collaboratrice, Avocat au barreau de Paris
Tel +33 1 56 59 53 60
Nilofar.MoiniShabestari@nortonrosefulbright.com

Nos principes professionnels – Qualité, Unité, Intégrité

Partout à travers le monde, l'activité de Norton Rose Fulbright s'exerce d'après des valeurs professionnelles fortes et une exigence absolue de qualité, d'unité et d'intégrité. Nous sommes fiers de notre attachement à ces principes qui caractérisent notre entreprise et ceux qui la composent, et se reflètent dans les services que nous fournissons à nos clients tous les jours.

Norton Rose Fulbright

Norton Rose Fulbright est un cabinet d'avocats d'affaires international. Nous fournissons une gamme complète de services juridiques aux entreprises et institutions financières mondiales de premier plan. Notre cabinet rassemble au-delà de 4000 avocats à travers l'Europe, les Etats-Unis, le Canada, l'Amérique latine, l'Asie, l'Australie, l'Afrique et le Moyen-Orient.

Reconnus pour notre approche sectorielle, nos compétences couvrent l'ensemble des secteurs clés de l'industrie : institutions financières, énergie, infrastructures, mines et matières premières, transport, technologie et innovation ainsi que sciences de la vie et santé. Grâce à notre groupe mondial dédié à la prévention des risques, nous mettons à profit notre expérience sectorielle et la combinons à notre connaissance des enjeux en matière de droit, de réglementation, de conformité et de gouvernance afin de fournir à nos clients des solutions pratiques pour faire face aux risques juridiques et réglementaires auxquels ils sont exposés.

Partout dans le monde, nous agissons en accord avec nos principes fondateurs dans la conduite des affaires que sont la qualité, l'unité et l'intégrité. Notre ambition est de fournir à nos clients, dans chacun de nos bureaux, un service juridique répondant aux plus hautes exigences et de qualité uniforme.

Le Verein Norton Rose Fulbright, un Verein suisse, aide à coordonner les activités des membres de Norton Rose Fulbright, mais il ne fournit aucun service juridique aux clients. Norton Rose Fulbright a des bureaux dans plus de 50 villes partout dans le monde, y compris à Londres, Houston, Toronto, Sydney et Johannesburg. Pour de plus amples renseignements, veuillez consulter nortonrosefulbright.com/legal-notices. Cette communication est un instrument d'information au sujet des faits nouveaux en droit. Son contenu ne saurait en aucune façon être interprété comme un exposé complet du droit ni comme un avis juridique de toute entité Norton Rose Fulbright sur les points de droit qui y sont discutés. Vous devez obtenir des conseils juridiques particuliers sur tout point précis vous concernant. Pour tout conseil ou pour de plus amples renseignements, veuillez-vous adresser à votre responsable habituel au sein de Norton Rose Fulbright.