Date de publication sur legifrance: 23/10/2018

Commission Nationale de l'Informatique et des Libertés

Décision n°MED-2018-043 du 8 octobre 2018
Décision n° MED 2018-043 du 8 octobre 2018 mettant en demeure la société SINGLESPOT

La Présidente de la Commission nationale de l'informatique et des libertés,

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

Vu le règlement (UE) 2016/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu le code pénal ;

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

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° 2018-118C du 30 mars 2018 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de la société SINGLESPOT ;

Vu le procès-verbal de contrôle n° 2018-118/1 du 29 mai 2018 ;

Vu les autres pièces du dossier ;

· Constate les faits suivants

La société SINGLESPOT (ci-après la société), sise 33, rue Lafayette à Paris (75009) est une société par actions simplifiée spécialisée dans la programmation informatique et notamment l'édition et la vente d'outils informatiques. Elle emploie environ 27 salariés et a réalisé en 2017 un chiffre d'affaires d'environ 4,2 millions d'euros pour un résultat net de 418 mille euros.

L'activité de la société SINGLESPOT est d'afficher des publicités pour le compte d'annonceurs, sur les ordiphones de personnes dont le profil est déterminé à partir de leurs données de géolocalisation. La société a également pour activité de mesurer les visites des mobinautes[1]dans les points de vente de ses clients.

La société a effectué, le 9 mai 2018, auprès de la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) une déclaration n° 1943129 relative à un traitement dont la finalité est de *créer des segments d'audience que nous adressons avec de la publicité mobile. […] sur la base des segments d'élaborer des études à destination de clients de divers industries (retail, immobilier, etc.) en vue, en particulier, de les aider à avoir une meilleure compréhension du marché et de ses tendances et de les aider à analyser la performance de leurs magasins .*

La société a désigné, le 12 avril 2018, une déléguée à la protection des données .

En application de la décision n° 2018-118C du 30 mars 2018 de la Présidente de la Commission, une délégation de la CNIL a procédé le 29 mai 2018 à une mission de contrôle sur place auprès de la société SINGLESPOT. La mission a notamment eu pour objet de vérifier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée) et au Règlement général sur la protection des données n° 2016/679 du 27 avril 2016 (ci-après RGPD ou Règlement sur la protection des données), de l'ensemble des traitements de données à caractère personnel mis en œuvre par la société.

L'objectif de la société SINGLESPOT est d'établir des profils de mobinautes afin de leur adresser de la publicité ciblée.

Dans ce cadre, la société a conclu des contrats avec 15 sociétés partenaires (essentiellement des éditeurs de presse tels que […]) qui éditent environ 25 applications mobiles. Elle a également déterminé des points d'intérêts (ci-après POIs) qui correspondent à des coordonnées géographiques de lieux permettant de révéler un profil de consommateur, tels que les points de vente physiques que celui-ci visite régulièrement ou a visité ponctuellement. Sont ainsi, par exemple, ciblés les mobinautes s'étant rendus dans des magasins concurrents et ceux ayant visité le magasin d'un client au cours des 15 derniers jours. Par la suite, la société SINGLESPOT réalise des campagnes marketing à travers l'achat d'espaces publicitaires pour le compte de clients annonceurs, sur la plateforme de la société […] de ventes aux enchères d'espaces publicitaires en temps réel.

Afin de réaliser ce service, la société a indiqué, lors du contrôle, avoir développé un logiciel SDK
, intégré par ses partenaires dans leurs applications et qui permet de collecter les données de géolocalisation ainsi que l'identifiant publicitaire mobile, le nom et la version de l'application mobile et le système d'exploitation utilisé (ANDROID ou IOS). Les données collectées grâce au SDK sont ensuite croisées avec les POIs déterminés avec les clients annonceurs de la société SINGLESPOT, ce qui permet de qualifier le profil de l'utilisateur pour le ciblage publicitaire souhaité. Ces données sont conservées par la société au sein de la base de données utilisant la solution […] , un service de stockage et d'hébergement de données en nuage proposé par la société […].

Lors du contrôle, la délégation a été informée que le SDK collecte les données de géolocalisation des personnes :

- tous les 200 mètres pour les applications installées sur le système d'exploitation IOS ;
- toutes les cinq minutes sur le système d'exploitation Android.

La délégation a constaté la présence dans la base de données de la société de 14 344 670 identifiants publicitaires distincts dont 5 529 383 identifiants sont associés à des données de géolocalisation. Chacun de ces identifiants publicitaires est directement lié à l'ordiphone d'une personne ayant téléchargé l'application d'un des éditeurs partenaires de la société.

Par ailleurs, la délégation a constaté, lors du téléchargement d'une application mobile – en l'espèce […] – intégrant le SDK de la société, que lorsque l'utilisateur d'un ordiphone valide l'autorisation système d'accès à ses données de géolocalisation pour le fonctionnement de l'application, ses données sont également transmises à la société SINGLESPOT sans qu'il en soit spécifiquement informé et sans que son consentement ne soit recueilli pour cette transmission.

En outre, la délégation a été informée que toutes les données de géolocalisation des mobinautes sont collectées et conservées dans la base de données de la société, même lorsqu'ils sont situés en dehors des points d'intérêts géographiques déterminés.

Elle a également été informée et a constaté que les données de géolocalisation des personnes, collectées à partir des applications mobiles des partenaires, sont conservées pendant treize mois à compter de la date de la collecte.

Enfin, la délégation a constaté que le compte administrateur qui permet d'accéder à la base de données […] utilise un mot de passe de 16 caractères. Elle a également été informée que des tests de développements sont réalisés dans cette base.

À la suite de demandes formulées par la délégation, la société a apporté des éléments additionnels par courriel du 6 juin 2018, portant notamment sur l'intégration du SDK, la politique interne d'accès au système d'information, ainsi qu'une liste des traitements mis en œuvre par la société.

· Sur la notion de responsable du traitement et de données à caractère personnel

Sur la qualité de responsable du traitement

Aux termes de l'article 4 (7) du Règlement sur la protection des données, le responsable de traitement est *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement […].*

Au regard des constats effectués par la CNIL et des éléments communiqués postérieurement au contrôle, il apparaît que la société SINGLESPOT détermine dans une large mesure les finalités et les moyens des traitements mis en œuvre dans le cadre de l'utilisation du SDK.

En effet, il ressort des pièces transmises à la délégation que la société traite pour son propre compte les données à caractère personnel collectées *via* le SDK pour vendre des services d'analyse ou de profilage auprès de ses clients annonceurs.

En outre, la délégation a été informée que les données des utilisateurs des différentes applications mobiles collectées sont enregistrées au sein de la même base de données,

[…], ce que la délégation a constaté.
Enfin, la société SINGLESPOT a indiqué à la délégation se considérer comme responsable de traitement.

La société SINGLESPOT doit, par conséquent, être regardée comme responsable du traitement mis en œuvre dans le cadre de l'utilisation du SDK.

Sur la collecte de données à caractère personnel

Aux termes de l'article 4 (1) et (2) du RGDP, constitue une donnée à caractère personnel *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée personne concernée); est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale..*

Constitue en outre un traitement de données à caractère personnel *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. .*

La délégation a constaté que la société SINGLESPOT collecte, *via* le SDK installé au sein des applications mobiles, l'identifiant publicitaire de l'ordiphone associé à des données de géolocalisation de la personne ainsi qu'à des données techniques relatives à l'ordiphone.

L'identifiant publicitaire est un identifiant unique généré par le système d'exploitation de l'ordiphone permettant d'identifier le terminal de l'utilisateur de façon stable dans le temps. Par défaut, il est mis à disposition de l'ensemble des applications mobiles installées sur celui-ci et est également accessible aux différents SDK installés dans les applications mobiles.

Cet identifiant publicitaire est stocké de façon pérenne dans l'ordiphone de l'utilisateur et permet donc d'identifier l'utilisateur de façon indirecte. Dans le cadre du traitement réalisé par SINGLESPOT, il a vocation à identifier l'utilisateur afin de lui associer un profil publicitaire constitué à partir de ses données de géolocalisation. Il permet ensuite d'identifier l'utilisateur lors de son utilisation ultérieure d'autres applications mobiles sur son téléphone afin de le cibler pour lui afficher des publicités spécifiquement choisies en fonction de ses habitudes de déplacement.

Il en résulte que la société traite des données à caractère personnel en application de l'article 4 du Règlement sur la protection des données.

· Sur les manquements constatés au regard des dispositions de la loi du 6 janvier 1978

Un manquement à l'obligation de disposer d'une base légale pour la mise en œuvre du traitement

La délégation a été informée que la société procède à la collecte des données de géolocalisation des personnes à l'aide du SDK intégré dans les applications mobiles téléchargées par les mobinautes. Par la suite, les données de géolocalisation sont croisées avec les points d'intérêts afin de qualifier le profil des personnes et de procéder à des campagnes d'affichages de publicités sur leur ordiphone.

Or, une telle combinaison des données à caractère personnel des mobinautes, à des fins publicitaires, ne peut intervenir que si la société peut se prévaloir de l'une des conditions prévues à l'article 6 du Règlement général sur la protection des données qui dispose que :
le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :
a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Lors du contrôle, la société a indiqué à la délégation que le traitement des données de géolocalisation aux fins de ciblage publicitaire est fondé sur le consentement des personnes concernées.

Par ailleurs, le registre des traitements de la société communiqué par courriel du 6 juin 2018 indique que *la base du traitement pour cette finalité [diffusions de campagnes digitales ciblées sur mobiles] est le consentement*.

En vertu de l'article 4 (11) du Règlement général sur la protection des données, le consentement s'entend comme *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* .

L'article 7 de ce même texte prévoit les conditions applicables au consentement :
1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait

du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée.

Or, il ressort du contrôle et de l'analyse des pièces transmises à la Commission qu'aucun mécanisme n'est proposé aux utilisateurs ayant téléchargé les applications des partenaires de la société pour consentir valablement aux traitements réalisés par la société SINGLESPOT.

En premier lieu, le consentement des personnes doit être informé.

Le G29 indique, dans ses lignes directrices du 10 avril 2018 sur le consentement au sens du Règlement 2016/679, que le *responsable du traitement doit s'assurer que le consentement est fourni sur la base d'informations qui permettent aux personnes concernées d'identifier facilement qui est le responsable des données et de comprendre ce à quoi elles consentent. [Il] doit clairement décrire la finalité du traitement des données pour lequel le consentement est sollicité.*

Il est également précisé que *pour que le consentement soit éclairé, il est nécessaire d'informer la personne concernée de certains éléments cruciaux pour opérer un choix. [..] Au moins les informations suivantes sont nécessaires afin d'obtenir un consentement valable :*
(i) l'identité du responsable du traitement,
(ii) la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité,
(iii) les (types de) données collectées et utilisées,
(iv) l'existence du droit de retirer son consentement,
(v) des informations concernant l'utilisation des données pour la prise de décision automatisée [..] et
(vi) des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées […].

En l'espèce, la délégation a constaté qu'au moment de l'installation des applications contrôlées, les personnes ne sont pas informées de la collecte de leurs données de géolocalisation *via* le SDK à des fins de profilage des utilisateurs et de ciblage publicitaire.

Lors du contrôle, la société a indiqué qu'elle procédait à la modification des contrats avec ses partenaires éditeurs d'applications mobiles pour y inclure une clause concernant leur responsabilité en matière de recueil du consentement. Elle a précisé que cette modification impliquait un accord avec la société SINGLESPOT sur le texte concernant l'autorisation à la collecte des données de géolocalisation.

Il ressort des pièces du contrôle que l'avenant apporté aux contrats avec les partenaires éditeurs mentionne la possibilité, pour la société SINGLESPOT, d'utiliser les données des utilisateurs.

La société a également indiqué qu'elle était en train de mettre en place une fenêtre pop-up qui permettrait d'afficher une information et de recueillir un consentement des utilisateurs préalablement à la collecte de leurs données de géolocalisation. Cette fenêtre serait

déclenchée par le SDK, hébergée sur les serveurs de la société, et pourrait être forcée dans les applications mobiles intégrant le SDK.

Les contrats ou avenants communiqués par la société à la délégation mentionnent une simple obligation, mise à la charge de l'éditeur d'application mobile, de fournir *aux Utilisateurs Uniques concernés par les opérations de traitement l'information relative aux traitements de données réalisés au titre du Contrat* **selon une formulation et un format à convenir avec SINGLESPOT** *aux fins d'obtenir le consentement de chaque Utilisateur Unique à la collecte et au traitement de leurs données à caractère personnel dans le cadre du Contrat* .

Cette formulation est insatisfaisante en ce qu'elle ne fixe pas les exigences concrètes et précises de la forme dans laquelle le consentement de l'utilisateur devra être recueilli, laissant le soin à des négociations ultérieures de fixer ces modalités. Faute de dispositions claires sur le format, la formulation du recueil du consentement et l'information à délivrer aux personnes concernées, la société SINGLESPOT n'est, à ce stade, pas en mesure de permettre à l'éditeur de l'application de satisfaire aux obligations qu'elle met à sa charge au titre de la protection des données, ni, à fortiori, d'en garantir le respect, ce qu'il lui appartiendra de faire.

Si la fenêtre contextuelle communiquée par la société à la Commission le 5 octobre 2018 offre à l'utilisateur une meilleure information quant au traitement des données à caractère personnel de l'utilisateur, rien ne met en mesure la société SINGLESPOT de s'assurer de son intégration effective au sein des applications de ses éditeurs partenaires.

En outre, la société a précisé imposer à ses partenaires uniquement une référence à sa société dans la politique de confidentialité des applications. Or, cette seule mention ne permet pas d'assurer une information suffisante des personnes dès lors que la finalité de la collecte de leurs données de géolocalisation – la publicité ciblée – les droits dont elles disposent ainsi que la base légale de ce traitement ne sont pas portés directement à leur connaissance.

Il apparaît, enfin, que l'information dans la politique de confidentialité des applications mobiles est tardive dès lors qu'elle n'est accessible aux personnes qu'après l'installation de l'application et du SDK, alors que leur identifiant publicitaire et leurs données de localisation sont déjà collectés par la société *via* le SDK.

Dès lors, les personnes ayant téléchargé l'application mobile avant la mise en place du SDK ne sont pas directement informées de l'intégration de celui-ci à l'application et de la finalité poursuivie par ce traitement.

Par conséquent, les personnes ne sont pas dûment informées de la collecte de leurs données de géolocalisation par la société, *via* l'installation d'un SDK, à des fins de publicité ciblée.

Dès lors, le consentement recueilli n'est pas informé en l'espèce.

En deuxième lieu, le consentement doit être spécifique.

Dans ses lignes directrices du 10 avril 2018 sur le consentement au sens du Règlement 2016/679, le G29 indique qu' *afin de se conformer au caractère spécifique du*

consentement, le responsable du traitement doit garantir :
(i) la spécification des finalités en tant que garantie contre tout détournement d'usage,
(ii) le caractère détaillé des demandes de consentement, et
(iii) la séparation claire des informations liées à l'obtention du consentement au traitement des données et des informations concernant d'autres sujets.

Le RGPD établit clairement que le consentement nécessite une déclaration de la part de la personne concernée ou un acte positif clair, ce qui signifie qu'il doit toujours être donné par une déclaration ou un geste actif. […] Le silence ou l'inactivité de la personne concernée, ainsi que le simple fait qu'elle continue à utiliser un service, ne peuvent être considérés comme une indication active de choix.

En l'espèce, la délégation a constaté à l'occasion du contrôle sur place que les personnes sont amenées à valider l'autorisation système de collecter leurs données de géolocalisation uniquement pour l'utilisation globale de l'application mobile téléchargée.

À titre d'exemple, s'agissant de l'application mobile […] , sur le système d'exploitation iOS, une fenêtre contextuelle est présentée aux personnes au moment de l'installation de celle-ci de donner son accord à la collecte de données r*elatives à votre expérience, votre navigation et votre géolocalisation* pour *optimiser votre expérience utilisateur, analyser votre trafic et vous proposer des contenus plus pertinent* .

De la même manière, au moment où l'application demande l'autorisation de collecter les données relatives à la position du téléphone, le message d'autorisation indique que *l'application collecte des données relatives à la géolocalisation afin de vous proposer des contenus plus pertinents. Par exemple, dans le cadre de l'offre la pépite , afin qu'elle soit mieux ciblée ou lors de la recherche afin de vous proposer des recettes de votre région ou de la région que vous visitez. Ces données peuvent également être partagées avec nos partenaires (y compris nos partenaires publicitaires) pour vous proposer des contenus promotionnels moins intrusifs, plus adaptés.*

Le fait de présenter l'ensemble des finalités en offrant seulement à l'utilisateur la possibilité d'accepter en bloc ne permet pas de donner un consentement spécifique pour l'utilisation du SDK. Le consentement donné pour l'utilisation des données de géolocalisation, par exemple, afin d'accéder à l'ensemble des fonctionnalités proposées par l'application entraînera nécessairement l'acceptation de la collecte et de l'utilisation des données à des fins publicitaires.

La fenêtre contextuelle proposée par la société à ses partenaires précise notamment que les finalités du traitement sont de *optimiser votre expérience utilisateur en vous proposant notamment des contenus plus pertinents* et *de mieux adapter la publicité que vous pourriez recevoir à vos centre d'intérêt* .

Les deux finalités ne font pas l'objet d'un recueil de consentement spécifique, l'accord donné pour l'une des finalités entraînant nécessairement l'accord pour l'autre finalité.

Au regard de ces éléments, les utilisateurs des applications mobiles partenaires ne consentent donc pas spécifiquement au traitement de leurs données de géolocalisation à des fins de profilage et de ciblage publicitaire.

Il résulte de tout ce qui précède que le consentement des personnes n'est pas valablement recueilli.

Les faits précités sont donc constitutifs d'un manquement aux dispositions de l'article 6 du Règlement général sur la protection des données.

En dernier lieu, le consentement doit être univoque.

Les lignes directrices WP 259 sur le consentement adoptées le 28 novembre 2017 retiennent que *le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées* .

La fenêtre contextuelle précitée offre à l'utilisateur deux onglets cliquables : j'accepte ou plus tard . Aucune de ces options ne lui propose clairement de refuser la collecte et le traitement de ses données à caractère personnel.

Dès lors, le consentement donné n'est pas univoque.

Un manquement à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement

En premier lieu, la délégation a été informée que le SDK installé dans les applications mobiles collecte les données de géolocalisation des utilisateurs environ toutes les cinq minutes sur les applications mobiles sur le système ANDROID et tous les 200 mètres pour les applications mobiles sur le système iOS. Ces données sont conservées dans la base de données […] pendant treize mois puis purgées.

Une fois croisées avec les POIs recensés, les données de géolocalisation pertinentes sont ensuite intégrées dans la table intitulée visit de la base de donnée de la société et sont utilisées par la suite à des fins publicitaires. La délégation a constaté que les identifiants publicitaires des ordiphones sur lesquels la publicité ciblée est effectuée sont également conservés pendant treize mois dans de la table intitulée devices de la base de données.

Or, la conservation par la société de toutes les données de géolocalisation des utilisateurs au-delà du temps nécessaire à la réalisation de l'opération de correspondance entre les données collectées et les zones géographiques POIs (au sein desquelles la société effectue des campagnes marketing) est excessive au regard de la finalité de ciblage publicitaire du traitement.

Lors du contrôle, la société a justifié la durée de conservation de treize mois des données de géolocalisation par le besoin de disposer d'une saisonnalité des déplacements des personnes.

La société ne peut justifier la conservation de l'intégralité des données de géolocalisation des personnes, durant treize mois, au motif d'établir uniquement un comparatif de ces données et les lieux visités par les personnes. La conservation de telles informations constitue un risque d'atteinte à la vie privée des personnes concernées.

En effet, la Commission considère que l'utilisation des dispositifs de géolocalisation est particulièrement intrusive au regard des libertés individuelles, dans la mesure où ils permettent de suivre de manière permanente et en temps réel des personnes, aussi bien dans l'espace public que dans des lieux privés. Ainsi, la CNIL estime que les données de

géolocalisation ne peuvent être conservées que pour une durée strictement proportionnée à la finalité du traitement qui a justifié cette géolocalisation.
Dès lors, quand bien même les conditions seraient réunies pour considérer que le traitement mis en œuvre dispose d'une base légale, la durée de conservation de treize mois de telles données est excessive au regard de sa finalité de profilage et de ciblage publicitaire.
En second lieu, la délégation a été informée que la table dénommée idfa_identified présente dans la base de données de la société, contient les données relatives aux profils de personnes. Ce profil est constitué à partir des données collectées précédemment et des déplacements et visites effectuées par les individus.

La délégation a constaté la présence dans cette table, de données associant l'identifiant publicitaire d'une personne à des catégories permettant un profilage (par exemple beauty , fashion , deco).

Or, la délégation a été informée que cette table n'était plus utilisée depuis le mois de janvier 2018 car elle correspondait à un projet désormais terminé avec un client.

Ces faits constituent un manquement aux dispositions de l'article 5-1 e) du Règlement général sur la protection des données qui prévoit que les données sont *[…] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées .*

Il est en outre rappelé qu'en application des articles 226-20 et 226-24 du Code pénal combinés le fait, pour une personne morale, de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni d'une peine d'amende pouvant atteindre 1 500 000 €.

Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données

En premier lieu, la délégation a constaté que le compte administrateur permettant d'accéder à la base de données […] utilise un mot de passe de 16 caractères composé uniquement de trois types caractères différents (majuscules, minuscules et chiffres).

La charte d'utilisation des systèmes d'information en date du 28 mai 2018 de la société préconise également de *choisir des mots de passe quand cela est possible d'au moins 10 caractères comprenant au moins des majuscules, minuscules, chiffres et caractères spéciaux* .

En second lieu, la délégation a été informée que les équipes de développement de la société font des tests de développement en utilisant les données présentes dans la base de données de production correspondant à des données à caractère personnel réelles.

Or, utiliser des données à caractère personnel réelles pour les phases de développement et de test présente un risque pour celles-ci, notamment en cas de perte, de modification non autorisée, d'erreur ou d'accès par des personnes non autorisées. En particulier, il est rappelé que les équipes de développement et de tests n'ont pas nécessairement à connaître des données issues de la base de données de production et que, dans

l'hypothèse où des données réelles seraient néanmoins requises, celles-ci devraient être anonymisées.

Ces faits constituent un manquement aux dispositions de l'article 32-1 b) du Règlement général sur la protection des données qui dispose que *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : […] des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement.*

Il est rappelé qu'en application des articles 121-2, 131-37, 131-38 et 226-17 du Code pénal combiné le fait, pour une personne morale, de procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni d'une amende de 1 500 000 euros.

En conséquence, la société SINGLESPOT, sise 33, rue Lafayette à Paris (75009) est mise en demeure sous un délai de trois (3) mois à compter de la notification de la présente décision **et sous réserve des mesures qu'elle aurait déjà pu adopter, de :**

- **ne pas procéder sans base légale au traitement des données de géolocalisation des personnes à des fins de ciblage publicitaire, en particulier recueillir, de manière effective, le consentement préalable des utilisateurs des applications éditées par les partenaires de la société SINGLESPOT au traitement de leurs données par cette dernière** (par exemple par la mise en place d'un pop-up contenant une information et une case à cocher dédiées ou un bouton de refus) et à défaut, supprimer lesdites données collectées ;

- **sous réserve de base légale du traitement, définir et mettre en œuvre une politique de durée de conservation des données raisonnable**, en particulier :
- **supprimer les données de géolocalisation** des utilisateurs collectées en dehors des zones de POIs une fois la correspondance entre les données de géolocalisation et les zones de POIS effectuée ;
- **définir une durée de conservation des données de géolocalisation** proportionnée à la finalité du traitement et procéder à la purge ou, le cas échéant, à l'anonymisation des données anciennes ;

- **prendre toute mesure nécessaire pour garantir la sécurité des données à caractère personnel des utilisateurs**, notamment en mettant en place **une politique contraignante relative aux mots de passe utilisés** par les comptes accédant aux bases de données ou aux plateformes d'administration de ces bases, respectant l'une des modalités suivantes :
- les mots de passe sont composés d'au minimum 12 caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ;
- les mots de passe sont composés d'au moins 8 caractères, contenant 3 des 4 catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s'accompagnent d'une mesure complémentaire comme par exemple la temporisation d'accès au compte après plusieurs échecs, (suspension temporaire de

l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum 10).

- un stockage des mots de passe sous une forme hachée (par exemple, à l'aide de l'algorithme SHA256 avec l'utilisation d'un sel) ;
- **en mettant en place une politique de séparation entre les environnements de tests de développement (ou de recette) et les environnements de production ;**

- **justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.**

À l'issue de ce délai, si la société SINGLESPOT s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l'inverse, si la société SINGLESPOT ne s'est pas conformée à la présente mise en demeure, un rapporteur sera désigné qui pourra demander à la formation restreinte de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente

Isabelle FALQUE-PIERROTIN

[1]Personne qui navigue sur Internet à partir d'un appareil mobile.
[2]Kit de développement logiciel.