CNIL.

Décision n° 2016-007 du 26 janvier 2016 mettant en demeure les sociétés FACEBOOK INC. et FACEBOOK IRELAND

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 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 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 les arrêts rendus par la Cour de justice de l'Union européenne le 13 mai 2014 dans l'affaire C-131/12 Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, le 1er octobre 2015 dans l'affaire C-230/14 Weltimmo s.r.o. contre Nemzeti Adatvédelmi és Információszabadság Hatóság et le 6 Octobre 2015 dans l'affaire C-362/14 Maximillian Schrems contre Data Protection Commissioner ;

Vu les décisions de la Présidente de la Commission nationale de l'informatique et des libertés de procéder à des missions de vérification des traitements de données à caractère personnel mis en œuvre par la société FACEBOOK Inc. (n° 2015-091C du 17 mars 2015) et portant, en tout au partie, sur des données collectées au moyen du site web FACEBOOK.COM ou au moyen des cookies relevant de ce domaine (n° 2015-401C du 14 décembre 2015) ;

Vu les procès-verbaux de contrôle sur place n° 2015-091/1 et n° 2015-091/2 des 8 et 9 avril 2015, les réponses apportées par FACEBOOK INC. au questionnaire envoyé par la CNIL le 30 juillet 2015 et le procès-verbal de constatations en ligne n° 2015-401 du 15 décembre 2015 ;

Vu les autres pièces du dossier ;

I- Constate les faits suivants

La société FACEBOOK Inc. a été fondée en 2004 et a son siège social aux États-Unis (1601 Willow Road, Menlo Park, CA 94025). Elle a pour activité la gestion du réseau social FACEBOOK (FACEBOOK.COM) (ci-après le « site ») et compte environ 1,5 milliard d'utilisateurs actifs par mois dans le monde. La société a également une activité de régie publicitaire. Elle possède 49 bureaux implantés dans une trentaine de pays et compte environ 12 000 salariés à travers le monde.

La société FACEBOOK Inc. a créé plusieurs dizaines de filiales dans le monde, dont la société FACEBOOK Ireland Limited, située 4 Grand Canal Square, Grand Canal Harbour, à Dublin, et la société FACEBOOK France Sarl, située 108 avenue de Wagram à Paris (75017).

En application de la décision n° 2015-091C du 17 mars 2015 de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après « CNIL » ou « la Commission »), une délégation de la CNIL a procédé à une mission de contrôle sur place les 8 et 9 avril 2015 et à un contrôle sur pièces le 30 juillet 2015. Puis, par décision n° 2015-401C du 14 décembre 2015, la Présidente de la CNIL a décidé de faire procéder également à des constatations en ligne le 15 décembre 2015. Ces missions ont eu pour objet de procéder à la vérification du respect par la société FACEBOOK Inc. des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée en ce qui concerne les règles de confidentialité applicables aux services à destination des internautes français et ont également porté sur les données collectées au moyen du site FACEBOOK.COM et des témoins de connexion (ci-après « cookies ») relevant de ce domaine.

Sur l'applicabilité de la loi française

Il est tout d'abord rappelé que, conformément à son article 4, la directive 95/46/CE s'applique lorsque « *le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'Etat membre* ». L'article 5 de la loi du 6 janvier 1978 modifiée prévoit quant à lui que la loi française est applicable dès lors que le responsable de traitement est établi sur le territoire français.

La loi française est en l'espèce applicable dans la mesure où FACEBOOK France est un « *établissement* » au sens de la directive 95/46/CE, telle qu'interprétée par la Cour de Justice de l'Union Européenne (CJUE) dans son arrêt *Weltimmo* du 1er octobre 2015. En outre, il apparaît que le traitement, mis en œuvre dans le cadre du réseau social FACEBOOK, est effectué « *dans le cadre des activités* » de cet établissement au sens de l'arrêt *Costeja* de la CJUE en date du 13 mai 2014.

Par ailleurs, au regard des constats effectués et des pièces fournies lors des différents contrôles, il apparaît que tant FACEBOOK Inc. que FACEBOOK Ireland participent à la détermination des finalités et des moyens du traitement (ci-après la « société »). Ces deux sociétés doivent, par conséquent, être considérées comme conjointement responsables de traitement, comme le permet la directive 95/46/CE. En effet, l'article 2(d) de ladite directive

définit le « *responsable du traitement* » comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* ».

En tout état de cause, la circonstance que l'un des responsables de traitement, en l'espèce la société FACEBOOK Ireland, soit situé sur le territoire de l'Union européenne est indifférente en matière de contrôle et de sanction. En effet, l'article 48 de la loi du 6 janvier 1978 modifiée prévoit que la CNIL peut exercer ces pouvoirs « *à l'égard des traitements dont les opérations sont mises en œuvre, en tout ou partie, sur le territoire national, y compris lorsque le responsable du traitement est établi sur le territoire d'un autre État membre de la Communauté européenne* ».

Sur les faits

La délégation a été informée et a constaté que la société collecte des données, relatives à la navigation sur des sites tiers, des internautes qui ne disposent pas de compte sur le site FACEBOOK.COM.

La délégation a également été informée que la société transfère des données personnelles des internautes vers les Etats-Unis sur la base du *Safe harbor*.

Elle a constaté que la société collecte des données relatives à l'orientation sexuelle, aux opinions religieuses et aux opinions politiques des inscrits. La société peut également collecter des dossiers médicaux fournis par les inscrits en tant que justificatifs d'identité.

Par ailleurs, la délégation a été informée que la société procède sans base légale à la combinaison de nombreuses données relatives aux inscrits et qu'elle a mis en place sans autorisation de la CNIL des traitements ayant pour finalité de lutter contre la fraude et visant à exclure des inscrits de son site.

Elle a également constaté que le formulaire d'inscription au site ne contient aucune mention d'information relative au traitement de données à caractère personnel et que les internautes ne sont pas informés notamment de la finalité du transfert de données vers les Etats-Unis.

En outre, la délégation a constaté que 13 cookies ont été déposés sur son terminal.

La délégation a également constaté que la société conserve toutes les adresses IP utilisées par les inscrits pour se connecter à leurs comptes.

Enfin, la délégation a constaté que les internautes qui souhaitent s'inscrire sur le site peuvent choisir un mot de passe de 6 caractères.

II- Sur les manquements constatés au regard des dispositions de la loi du 6 janvier 1978 modifiée

Un manquement à l'obligation de disposer d'une base légale pour les traitements mis en œuvre

La délégation a été informée que la société procède à la combinaison de multiples informations aux fins d'affichage de publicités ciblées sur les comptes des inscrits et de mesure d'efficacité des campagnes publicitaires. En effet, la Politique d'utilisation des données de la société prévoit que « *Nous nous servons des informations à notre disposition pour améliorer nos systèmes de publicité et de mesure, ce qui nous permet de vous présenter des publicités pertinentes, à travers nos services ou en dehors, et d'évaluer l'efficacité et la portée de nos publicités et de nos services* ».

Le lien hypertexte « *Informations à notre disposition* » renvoie vers le haut de la Politique d'utilisation des données dont la première rubrique énumère les types de données collectées par la société. En réponse au questionnaire, la société a confirmé qu'elle pouvait utiliser toutes ces données pour adresser des publicités ciblées (réponse à la question 11).

Ainsi, il apparaît que la société procède notamment à la combinaison des données suivantes :

- les données fournies par les inscrits lors de la création de leur compte sur le site ;
- les données relatives à l'activité des inscrits sur le site (contenus partagés ou consultés par exemple), quel que soit le terminal utilisé par ces derniers ;
- les données relatives aux appareils (ordinateur, téléphone et autres) utilisés par les inscrits (système d'exploitation, coordonnées GPS, type de navigateur, numéro de téléphone mobile par exemple) ;
- les données provenant de sites tiers et applications intégrant notamment des boutons « *J'aime* » ou « *Se connecter* » (sites consultés et applications utilisées par exemple) ;
- les données provenant de partenaires tiers (partenaires avec qui la société a collaboré pour offrir un service ou annonceurs avec lesquels les inscrits ont interagi) (adresse électronique par exemple) ;
- les données provenant des sociétés qui appartiennent ou qui sont exploitées par la société (Facebook Payments Inc., Instagram LLC, WhatsApp Inc. par exemple).

Or, une telle combinaison à des fins publicitaires des données personnelles des inscrits ne peut intervenir que si la société peut se prévaloir d'une des conditions prévues à l'article 7 de la loi n° 78-17 du 6 janvier 1978 modifiée, qui prévoit que : « *un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :*

1° Le respect d'une obligation légale incombant au responsable du traitement ;

2° La sauvegarde de la vie de la personne concernée ;

3° L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;

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. »

En l'espèce, faute de recueil du consentement des inscrits préalablement à la combinaison de leurs données, la mise en œuvre de ce traitement ne peut avoir pour base légale que l'une des conditions énumérées par les 1° à 5° de l'article précité.

Compte tenu de la nature des traitements en cause, les 1°, 2° et 3° de l'article 7 ne peuvent constituer la base légale de la combinaison des données par la société. Le traitement issu de cette combinaison ne peut donc être examiné qu'au regard du 4° et du 5° de l'article 7.

S'agissant du 4° de l'article 7, il n'existe pas, en l'espèce, de cadre contractuel gouvernant la combinaison de données à des fins d'affichage de publicités ciblées. Bien que mentionnée par la société dans sa Politique d'utilisation des données, la combinaison de données ne constitue pas l'objet principal du contrat auquel souscrit l'internaute lorsqu'il s'inscrit sur le site. La possibilité que se ménage la société de combiner les données doit être considérée comme accessoire audit contrat, fixé unilatéralement par la société.

A cet égard, il convient de noter que les inscrits ont la possibilité de s'opposer à l'affichage de publicités ciblées dans les paramètres de leur compte (rubrique « *Publicités* »), cet affichage étant directement issu de la combinaison de données. Les inscrits peuvent donc demander à ce que cette fonctionnalité ne leur soit pas appliquée, ce qui confirme que la combinaison de données n'est ni l'objet, ni une clause substantielle du contrat.

En conséquence, la société ne peut fonder la combinaison de données à des fins publicitaires sur l'exécution de la seule Politique d'utilisation des données, de sorte que le 4° de l'article 7 précité ne peut trouver à s'appliquer en l'espèce.

En ce qui concerne le 5° de l'article 7, l'intérêt légitime du responsable de traitement doit être apprécié d'une part, en tant que tel, et d'autre part, au regard de l'intérêt de la personne concernée et de ses droits et libertés fondamentaux, auquel l'intérêt légitime du responsable de traitement ne saurait porter atteinte.

D'une part, pour apprécier la légitimité de l'intérêt du responsable de traitement, il convient notamment de tenir compte de la proportionnalité du traitement de données au regard de ses finalités. En l'espèce, la société affirme que la combinaison de l'ensemble des données lui permet d' « *améliorer [ses] systèmes de publicité et de mesure* ».

D'autre part, force est de constater qu'une telle combinaison de données est, par sa nature même, son ampleur et son caractère massif, susceptible de méconnaître l'intérêt des utilisateurs inscrits et leur droit fondamental au respect de leur vie privée.

Dès lors, l'intérêt économique et commercial de la société ne peut être regardé comme légitime que si le responsable de traitement met à disposition des utilisateurs inscrits des moyens adéquats leur permettant de contrôler la combinaison de leurs données et d'exercer effectivement le droit qui leur est reconnu par l'article 38 de la loi du 6 janvier 1978 modifiée.

En l'état, la société n'offre pas d'outils permettant aux inscrits de faire obstacle à la combinaison de leurs données personnelles, et, par suite, d'opposer leur intérêt privé ou le respect de leurs droits et libertés à l'intérêt du responsable de traitement. En effet, dans les paramètres de compte, rubrique « *Publicités* », la société propose uniquement aux inscrits des outils leur permettant de s'opposer à l'affichage de publicités ciblées :

- pour les publicités basées sur les préférences des inscrits : la société précise que « *Nous voulons vous montrer des publicités que vous jugez intéressantes. C'est pourquoi nous avons créé les préférences publicitaires, un outil dans lequel vous pouvez voir, ajouter et supprimer les préférences que nous avons créées pour vous en fonction des informations de votre profil, de votre activité sur Facebook et des sites web et apps que vous utilisez en dehors de Facebook (...) Si vous supprimez toutes vos préférences, vous verrez toujours des publicités mais elles seront peut-être moins intéressantes pour vous* ». Si les inscrits peuvent effectivement supprimer les préférences identifiées par la société, cet outil ne leur permet pas de s'opposer à la collecte et à la combinaison de ces données à des fins publicitaires ;
- pour les publicités affichées en fonction de la navigation des inscrits sur les sites web et applications : la société indique qu' « *une des façons de vous présenter des publicités repose sur votre utilisation des sites webs et applications qui utilisent les technologies Facebook. Par exemple, si vous consultez des sites de voyage, il se peut que vous voyiez ensuite des publicités pour des hôtels sur Facebook (...) Si vous désactivez les publicités en ligne basées sur les intérêts, vous verrez toujours le même nombre de publicités, mais elles seront peut-être moins pertinentes pour vous* ». Cet outil ne permet donc pas aux inscrits d'exercer leur droit d'opposition à la collecte et à la combinaison de leurs données à des fins publicitaires.

Il résulte de ce qui précède que la combinaison de l'ensemble des données des inscrits est dépourvue de base légale faute, soit de faire l'objet d'un encadrement contractuel adéquat, soit de respecter, dans la recherche de son intérêt légitime en tant que responsable de traitement, l'intérêt et les droits et libertés des personnes, en mettant à leur disposition des moyens leur permettant de maîtriser la combinaison des données les concernant et d'exercer leurs droits de manière effective.

Ces faits sont de nature à constituer un manquement aux dispositions de l'article 7 de la loi du 6 janvier 1978 modifiée.

Un manquement à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données

La délégation a constaté que la société peut être amenée à demander aux internautes qui se sont inscrits sur le site (ci-après « les inscrits ») de fournir des justificatifs d'identité, tels qu'un dossier médical, par exemple lorsqu'ils tentent de remplacer leur nom de famille par celui d'une célébrité. Dans les Pages d'aide du site, la société invite les internautes, lorsqu'ils envoient de tels documents, à *« masquer les informations personnelles qui ne sont pas nécessaires à la confirmation de votre identité (par exemple, votre numéro de carte de crédit ou de sécurité sociale)* ».

Bien que la société attire l'attention des inscrits sur la nécessité de procéder à ce masquage, il n'apparaît pas pertinent de demander le dossier médical des inscrits pour justifier de leur identité. En effet, un tel document comporte de nombreuses données pouvant porter atteinte à la vie privée des personnes concernées et de nombreux autres documents pourraient permettre aux inscrits de justifier de leur identité.

Ces faits constituent un manquement à l'article 6-3° de la loi du 6 janvier 1978 modifiée, qui dispose que les données collectées doivent être *« adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ».

Un manquement à l'obligation de recueillir le consentement des personnes concernées pour le traitement de données sensibles relatives aux opinions politiques ou religieuses, et à la vie sexuelle

La délégation a constaté qu'une fois inscrits sur le site, les internautes peuvent compléter leur profil sur la page « *A propos* », rubrique « *Informations générales et coordonnées* ». Ils peuvent notamment préciser leur orientation sexuelle (rubrique « *Ajoutez qui vous intéresse* » : « *Intéressé(e) par* □ *Femmes* □ *Hommes* »), leurs opinions religieuses (rubrique « *Ajoutez vos croyances religieuses* ») et leurs opinions politiques (rubrique « *Ajoutez vos opinions politiques* »).

Or, la délégation a relevé que la société n'a pas prévu de case à cocher pour recueillir le consentement des personnes à la collecte de ces données.

L'article 8 de la loi du 6 janvier 1978 modifiée prévoit notamment qu'il est interdit de collecter ou de traiter des données à caractère personnel qui sont relatives aux opinions politiques ou religieuses et à la vie sexuelle des personnes, sauf dans les cas prévus au II de cet article, notamment en cas de consentement exprès des personnes concernées.

Or, le consentement ne peut être exprès que s'il est donné en toute connaissance de cause, c'est-à-dire après la délivrance d'une information adéquate sur l'usage qui sera fait des données personnelles.

En l'espèce, aucun moyen technique n'est mis à la disposition des personnes lorsque les données « sensibles » sont collectées et traitées afin de s'assurer qu'elles y consentent de manière expresse sur la base d'une information spécifique.

La Commission considère que le fait, pour les personnes concernées, de renseigner leurs données sensibles, ne saurait être considéré comme un consentement exprès. Les utilisateurs doivent pouvoir marquer leur assentiment en cochant une case dédiée à l'approbation de l'usage de leurs données personnelles sensibles, ce qui n'est pas le cas en l'espèce.

Ces faits constituent un manquement à l'article 8 de la loi du 6 janvier 1978 modifiée susmentionné.

Il est rappelé enfin qu'en application des articles 226-19 et 226-24 du code pénal combinés, le fait pour une personne morale, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni d'une peine d'amende pouvant atteindre 1.500.000 €.

Un manquement à l'obligation d'informer les personnes

La délégation a constaté que le formulaire d'inscription au site ne contient aucune mention d'information relative au traitement de données à caractère personnel.

Or, l'article 32 de la loi du 6 janvier 1978 modifiée impose de fournir aux personnes concernées, sur le formulaire de collecte des données, des informations sur l'identité du responsable du traitement, la finalité de ce traitement, le caractère obligatoire ou facultatif des réponses, leurs droits d'accès, de rectification et, le cas échéant, d'opposition aux données les concernant.

En outre, la délégation a constaté que la Politique d'utilisation des données de la société prévoit que « *Les informations recueillies au sein de l'Espace Economique Européen (« EEE ») peuvent, par exemple, être transmises à d'autres pays en dehors de l'EEE aux fins décrites dans les présentes* ». Pour les internautes se trouvant en dehors des États-Unis, l'article 16 de la Déclaration des droits et des responsabilités précise : « *Vous acceptez que vos données personnelles soient transférées et traitées aux États-Unis* ».

Or, la délégation a constaté que les internautes ne sont pas informés de la nature des données transférées, de la finalité du transfert, des catégories de destinataires des données, et du niveau de protection offert par les pays destinataires, ce qui n'est pas conforme à l'article 91 du décret du 20 octobre 2005 modifié pris en application de la loi du 6 janvier 1978 modifiée.

En effet, cet article précise que : « *Les informations figurant au 7° du I de l'article 32 de la loi du 6 janvier 1978 susvisée que le responsable du traitement communique, dans les conditions prévues à l'article 90, à la personne auprès de laquelle des données à caractère personnel sont recueillies, sont les suivantes :*

1° Le ou les pays d'établissement du destinataire des données dans les cas où ce ou ces pays sont déterminés lors de la collecte des données ;

2° La nature des données transférées ;

3° La finalité du transfert envisagé ;

4° La ou les catégories de destinataires des données ;

5° Le niveau de protection offert par le ou les pays tiers :

a) Si le ou les pays tiers figurent dans la liste prévue à l'article 108, il est fait mention de la décision de la Commission européenne autorisant ce transfert ;

b) Si le ou les pays tiers ne satisfont pas aux conditions prévues à l'article 68 de la même loi, il est fait mention de l'exception prévue à l'article 69 de cette loi qui permet ce transfert ou de la décision de la Commission nationale de l'informatique et des libertés autorisant ce transfert ».

Ces faits constituent un manquement à l'article 32 de la loi n° 78-17 du 6 janvier 1978 modifiée quant à l'obligation pour le responsable du traitement de fournir à la personne concernée, directement sur le formulaire de collecte des données, des informations sur l'identité du responsable du traitement, la finalité de ce traitement, le caractère obligatoire ou facultatif des réponses, leurs droits d'accès, de rectification et, le cas échéant, d'opposition aux données les concernant.

Il est rappelé qu'en application des articles 131-41 et R. 625-10 du code pénal combinés, le fait pour la personne morale responsable d'un traitement de ne pas informer, dans les conditions prévues à l'article 32 de la loi du 6 janvier 1978 modifiée, la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est puni d'une peine d'amende pouvant atteindre 7.500 €.

Un manquement à l'obligation de procéder à une collecte et à un traitement loyal des données

A l'occasion de la navigation sur la page d'un site tiers sur lequel figure un module social FACEBOOK (bouton « J'aime » par exemple), la délégation a constaté que la société collecte des données relatives à la navigation des internautes qui ne sont pas inscrits sur le site FACEBOOK.COM.

Pour ce faire, la société « *dépose un cookie (le cookie datr) sur le navigateur d'un internaute lorsque cette personne interagit directement avec le site web Facebook en première partie (en se rendant sur une page de facebook.com ou en interagissant avec le domaine facebook.com)* » (réponse à la question 18). En effet, la délégation a constaté que la société dépose le cookie « *datr* » sur le terminal de tout internaute qui visite une page du site FACEBOOK.COM, et ce, alors même qu'il ne dispose pas d'un compte sur ce site.

La délégation a constaté que la société est alors en capacité de suivre la navigation des internautes sur les sites tiers, dès lors que ces sites contiennent un module social FACEBOOK. En effet, lorsqu'un internaute non inscrit sur le site FACEBOOK.COM se rend sur une page de ce site, puis visite un site tiers contenant un module FACEBOOK, l'information du site consulté est remontée à la société en même temps que le cookie « *datr* ». La délégation a été informée que : « *en ce qui concerne les non-détenteurs de comptes, les journaux d'accès relatifs aux cookies et aux modules sociaux sont supprimées dans les dix jours* » (réponse à la question 27).

A cet égard, la société a précisé qu'elle « *n'utilise pas et n'a pas utilisé le cookie datr pour surveiller le comportement de navigation des non-détenteurs de compte à des fins de publicités ou autres. Ce cookie est en réalité utilisé à des fins essentielles de sécurité et d'intégrité* » et qu'il permet de « *(i) faire la distinction entre des demandes d'accès autorisé et des demandes d'accès non autorisé ; (ii) d'empêcher tout accès non autorisé et (iii) de comprendre le volume et la fréquence des demandes d'accès pour empêcher les personnes ou les machine de récupérer des données, d'exécuter des attaques par déni de service ou de créer de faux comptes en masse* » (réponse à la question 18).

Si la finalité avancée par la société peut apparaître légitime (assurer la sécurité de ses services), la collecte des données relatives à la navigation sur des sites tiers des non inscrits au site FACEBOOK.COM est réalisée sans qu'ils en soient informés. Elle permet en effet de suivre une large part de la navigation des internautes concernés, à leur insu, pendant une durée potentielle de 10 jours, alors même qu'ils n'ont visité le site FACEBOOK.COM qu'une seule fois.

Ces faits constituent un manquement au 1° de l'article 6 de la loi n° 78-17 du 6 janvier 1978 modifiée disposant que les données à caractère personnel « *sont collectées et traitées de manière loyale et licite* ».

Un manquement à l'obligation d'obtenir l'accord préalable des personnes concernées avant d'inscrire des informations (cookies) sur leur équipement terminal de communications électroniques ou d'accéder à celles-ci

L'article 32-II de la loi du 6 janvier 1978 modifiée dispose que « *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 du 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 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 ».*

Les cookies nécessitant une information et un consentement préalables de l'internaute sont notamment les cookies liés aux opérations relatives à la publicité ciblée, certains cookies de mesure d'audience et les cookies traceurs de réseaux sociaux générés par les « boutons de partage de réseaux sociaux ».

Afin de proposer aux professionnels du secteur des lignes directrices en la matière, la CNIL a adopté la délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs. Cette recommandation, qui n'a pas de valeur impérative, vise à interpréter les dispositions législatives précitées et à éclairer les acteurs sur la mise en place de mesures concrètes permettant de garantir le respect de ces dispositions, afin, soit qu'ils mettent en œuvre ces mesures, soit qu'ils mettent en œuvre des mesures d'effet équivalent.

Cette recommandation rappelle que « *la validité du consentement est liée à la qualité de l'information reçue* ». La Commission recommande donc que ce consentement soit recueilli en deux étapes :

- première étape : « *l'internaute qui se rend sur le site d'un éditeur (page d'accueil ou page secondaire du site) doit être informé, par l'apparition d'un bandeau : des finalités précises des Cookies utilisés ; de la possibilité de s'opposer à ces Cookies et de changer les paramètres en cliquant sur un lien présent dans le bandeau ; du fait que la poursuite de sa navigation vaut accord au dépôt de Cookies sur son terminal* » ;
- seconde étape : « *les personnes doivent être informées de manière simple et intelligible des solutions mises à leur disposition pour accepter ou refuser tout ou partie des Cookies nécessitant un recueil du consentement : pour l'ensemble des technologies visées par l'article 32-II précité ; par catégories de finalités : notamment la publicité, les boutons des réseaux sociaux et la mesure d'audience* ».

En outre, la recommandation indique que le consentement « *doit se manifester par le biais d'une action positive de la personne préalablement informée des conséquences de son choix et disposant des moyens de l'exercer* » et qu'il « *ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et n'est pas exposée à des conséquences négatives importantes si elle refuse de donner son consentement* ».

En l'espèce, la délégation a constaté que 13 cookies ont été déposés sur son équipement terminal lors de sa connexion à FACEBOOK.COM. Interrogée sur les finalités de ces cookies, la société a renvoyé la CNIL à la lecture de sa Politique d'utilisation des cookies et

aux rapports d'audit menés par le Commissaire Irlandais à la Protection des Données en 2011 et 2012.

La Politique d'utilisation des cookies du site (page « *Cookies, pixels et technologies similaires* ») précise que « *des outils tels que les cookies (...) sont utilisés pour comprendre et diffuser des publicités, les rendre plus pertinentes et analyser les produits et services ainsi que leur utilisation* ». De la même manière, le rapport d'audit mené par le Commissaire Irlandais à la Protection des Données en 2012 fait apparaître que certains cookies ont une finalité publicitaire (notamment le cookie « *fr* » déposé par le domaine « *.facebook.com* »).

Or, le dépôt de cookies ayant une finalité publicitaire ne peut intervenir sans une information et un accord préalables des personnes concernées.

A cet égard, la délégation a constaté que les internautes sont informés du dépôt des cookies par un bandeau indiquant « *Les cookies nous permettent de fournir, protéger et améliorer les services de Facebook. En continuant à utiliser notre site, vous acceptez notre Politique d'utilisation des cookies* ».

Dès lors, l'internaute n'est pas informé :

- de la finalité de tous les cookies déposés soumis au consentement (notamment publicitaire) ;
- de la possibilité de changer les paramètres des cookies en cliquant sur un lien présent dans le bandeau.

En outre, la délégation a constaté que la Politique d'utilisation des cookies vers laquelle renvoie le bandeau précise que « *Votre navigateur ou votre appareil sont susceptibles de vous proposer des paramètres relatifs à ces technologies. Pour en savoir plus sur la disponibilité de ces paramètres, leur fonction et leur fonctionnement, consultez l'aide de votre navigateur ou de votre appareil* ».

Or, le paramétrage du navigateur ne peut être considéré comme un mécanisme valable d'opposition au dépôt des cookies que dans deux cas :

- le site ne dépose pas de cookies techniques essentiels à son fonctionnement : dans ce cas, la personne concernée peut paramétrer son navigateur de manière à bloquer le dépôt de tous les cookies, qu'ils proviennent du domaine du site (cookies « *first party* ») ou du domaine d'un tiers (cookies « *third party* »), dont ceux nécessitant son consentement, et ce sans l'exposer à des conséquences négatives importantes ;
- le site ne dépose pas de cookies *first party* nécessitant le recueil du consentement de la personne concernée : dans ce cas, cette dernière peut paramétrer son navigateur de manière à bloquer le dépôt de cookies *third party* sans empêcher le site de fonctionner ni risquer que des cookies *first party* soumis au consentement ne soient déposés.

En l'espèce, le site dépose des cookies techniques essentiels à son fonctionnement et des cookies *first party*. En effet, la Politique d'utilisation des cookies précise que la société dépose des cookies d'authentification qui permettent de savoir à quel moment l'internaute est

connecté au site (cookies techniques). Elle dépose également des cookies issus du domaine « *.facebook.com* » qui ont, pour certains, une finalité publicitaire, comme le cookie « *fr* » (cookies first party soumis au consentement).

Par conséquent, le paramétrage du navigateur ne peut, en l'espèce, être considéré comme un mécanisme valable d'opposition au dépôt de cookies.

Au regard de ce qui précède, il apparaît que le site internet n'a pas correctement informé les personnes concernées et n'a pas recueilli valablement leur consentement avant de procéder au dépôt des cookies.

Ces faits constituent un manquement au II de l'article 32 précité de la loi du 6 janvier 1978 modifiée, qui soumet à information et accord préalables de la personne concernée l'inscription d'informations sur son équipement terminal de communications électroniques et l'accès à celles-ci.

En outre, il est rappelé qu'en application des articles 131-41 et R. 625-10 du code pénal combinés, le fait pour la personne morale responsable d'un traitement de ne pas informer les personnes concernées et obtenir leur accord avant d'accéder à ou d'inscrire des informations dans leur équipement terminal de communications électroniques est puni d'une peine d'amende pouvant atteindre 7.500 €.

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

La délégation a constaté que la société propose aux inscrits une fonctionnalité « *Télécharger l'archive* », qui permet de recevoir « *une copie des données que vous avez publiées sur Facebook* ». La délégation a notamment constaté que dans l'onglet « *Sécurité* » de cette archive figure la liste des différentes adresses IP utilisées par les inscrits pour se connecter à leurs comptes, et ce depuis le 9 avril 2015, date d'ouverture d'un compte sur le site FACEBOOK.COM par la délégation.

Or, si la nécessité de lutter contre les usurpations de compte peut justifier de conserver ces données, il n'apparaît pas proportionné de les conserver pendant une durée supérieure à 6 mois.

Ces faits sont de nature à constituer un manquement aux dispositions de l'article 6-5° de la loi du 6 janvier 1978 modifiée qui prévoit 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* ».

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 des données

La délégation a constaté que l'internaute qui souhaite s'inscrire sur le site est invité à choisir un mot de passe contenant « *plus de 6 caractères* », « *unique* » et « *difficile à deviner pour les autres* ». En outre, elle a constaté que le mot de passe « *1234567a* » a été accepté.

Or, un mot de passe de 6 caractères ou ne comportant que 2 règles de complexité (chiffres et lettres) ne permet pas d'assurer la sécurité et la confidentialité des données auxquelles ils permettent d'avoir accès.

Ces faits constituent un manquement à l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée disposant que « *le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

Il est en outre rappelé qu'en application des articles 226-17 et 226-24 du code pénal combinés, le fait pour une personne morale de procéder ou de faire 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 notamment puni d'une peine d'amende pouvant atteindre 1.500.000 €.

Un manquement à l'obligation d'accomplir les formalités préalables à la mise en œuvre des traitements de lutte contre la fraude et d'exclusion

La délégation a été informée de la mise en place d'un traitement de lutte contre la fraude par la société. En effet, la Politique d'utilisation des données du site prévoit que « *Nous pourrons également accéder à des informations personnelles, les préserver et les partager lorsque nous sommes convaincus qu'il est nécessaire de : détecter, empêcher et traiter des fraudes ou toute autre activité illicite ; nous protéger nous-mêmes et protéger des tiers, notamment dans le cas d'enquêtes ; ou empêcher la mort ou tout risque imminent d'atteinte à l'intégrité physique d'une personne. Par exemple, nous pouvons partager des informations concernant la fiabilité de votre compte à nos partenaires tiers afin d'éviter toute forme de fraude et d'abus à travers comme en dehors de nos service* ».

En outre, la délégation a été informée que la société se réserve la possibilité d'exclure des inscrits en cas de non respect de la Déclaration des droits et responsabilités. En effet, l'article 14 de ce document précise que « *Si vous enfreignez la lettre ou l'esprit de cette Déclaration, ou créez autrement un risque de poursuites à notre encontre, nous pouvons arrêter de vous fournir tout ou partie de Facebook* ».

Or, la délégation a constaté que la société n'a effectué aucune demande d'autorisation pour encadrer la mise en œuvre de ces traitements.

Ces faits constituent un manquement aux dispositions du 4° de l'article 25-I de la loi du 6 janvier 1978 modifiée qui dispose que, sont mis en œuvre après autorisation de la CNIL, « *Les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire* ».

Il est rappelé qu'en application des articles 226-16 alinéa 1er et 226-24 du code pénal combinés, le fait pour une personne morale, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni d'une peine d'amende pouvant atteindre 1.500.000 €.

Un manquement relatif à l'obligation de disposer d'une base légale pour transférer des données personnelles hors de l'Union Européenne

L'article 16 de la Déclaration des droits et des responsabilités prévoit que les données relatives aux internautes se trouvant en dehors des États-Unis sont « *transférées et traitées aux États-Unis* ».

A cet égard, la Politique d'utilisation des données du site précise que « *Facebook Inc. adhère aux programmes « Safe Harbor framework » établis entre les Etats-Unis et l'Union européenne, et entre les Etats-Unis et la Suisse pour la collecte, l'utilisation et la conservation des données provenant de l'Union européenne et de la Suisse, comme défini par le ministère du Commerce américain* ». La société a ajouté que « *les clauses contractuelles type approuvées par la Commission européenne et le Safe Harbor (s'il s'agit d'importateurs basés aux Etats-Unis) sont les moyens par lesquels Facebook Irlande veille à ce que ces exportations de données soient (i) licites et (ii) protègent de façon adéquate les personnes concernées* » (réponse à la question 10).

Or, dans sa décision du 6 octobre 2015, la Cour de Justice de l'Union Européenne a invalidé la décision de la Commission européenne n° 2000-520 du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la sphère de sécurité (*Safe harbor*) publiés par le ministère du commerce des Etats-Unis, qui permettait d'encadrer les transferts de données à caractère personnel de l'Union européenne vers les Etats-Unis.

Dans la mesure où cette décision a été invalidée, il n'est désormais plus possible pour la société de procéder à un transfert de données personnelles vers les Etats-Unis sur la base du *Safe Harbor*.

Ces faits constituent un manquement à l'article 68 de la loi n° 78-17 du 6 janvier 1978 modifiée disposant que « *Le responsable d'un traitement ne peut transférer des données à*

caractère personnel vers un État n'appartenant pas à la Communauté européenne que si cet État assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet ».

En conséquence, les sociétés FACEBOOK Inc., sise 1601 Willow Road, Menlo Park, CA 94025 (Etats-Unis), et FACEBOOK Ireland Limited, sise 4 Grand Canal Square, Grand Canal Harbour, à Dublin (Irlande), sont mises en demeure, sous un délai de trois (3) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elles auraient déjà pu adopter, de :

- **ne pas procéder sans base légale à la combinaison des données des inscrits à des fins publicitaires ;**
- **ne pas traiter de données non pertinentes, excessives ou inadéquates au regard des finalités poursuivies,** en particulier cesser de demander aux inscrits de justifier de leur identité en fournissant un dossier médical ;
- **recueillir le consentement exprès des inscrits, sur la base d'une information spécifique, à la collecte et au traitement de leurs données « sensibles »** - en l'espèce des données relatives aux opinions politiques, religieuses et à l'orientation sexuelle - **par tout procédé, tel qu'une case à cocher, apposé à l'endroit de la collecte ;**
- **procéder à l'information des inscrits, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée :**
  - quant aux traitements de données à caractère personnel mis en place, et ce directement sur le formulaire d'inscription ainsi que sur les pages permettant aux inscrits de compléter leur profil ;
  - quant à la nature des données transférées hors de l'Union européenne, à la finalité du transfert, aux destinataires des données, et au niveau de protection offert par les pays destinataires ;
- **procéder à une collecte et à un traitement loyal** des données des internautes non inscrits s'agissant des données collectées via le cookie « datr » et le bouton « J'aime » ;
- **informer et obtenir l'accord préalable des internautes à l'inscription d'informations sur leur équipement terminal (cookies) et à l'accès à celles-ci.** A cet égard, il appartient à la société, sauf à mettre en place un dispositif présentant les mêmes garanties, d'indiquer aux internautes, au préalable et de manière claire et complète, sur le bandeau présent sur le site internet :
  - les finalités de tous les cookies soumis au consentement ;
  - qu'ils ont la possibilité de changer les paramètres de ces cookies en cliquant sur un lien présent dans le bandeau. Ce bandeau doit renvoyer vers une page présentant les solutions adéquates mises à leur disposition pour accepter ou refuser le dépôt des cookies ;
- **ne pas conserver de donnée à caractère personnel au-delà de la durée nécessaire aux finalités pour lesquelles elle a été collectée et traitée,** notamment en supprimant

à l'expiration d'un délai de 6 mois les adresses IP utilisées par les inscrits pour se connecter aux comptes ;

- **prendre toutes mesures nécessaires pour garantir la sécurité des données à caractère personnel des inscrits,** notamment en renforçant la robustesse des mots de passe des comptes (mots de passe composés d'au moins huit caractères de 3 types parmi les 4 suivants : chiffre, majuscule, minuscule et caractère spécial) ;
- **procéder à l'accomplissement des formalités préalables applicables aux traitements mis en œuvre,** en particulier procéder à une demande d'autorisation pour l'ensemble des traitements de données ayant pour finalité de lutter contre la fraude et susceptibles d'exclure des personnes ;
- **ne pas procéder à des transferts de données personnelles vers les Etats-Unis sur la base du *Safe Harbor* ;**
- **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 les sociétés FACEBOOK Inc. et FACEBOOK Ireland Limited se sont conformées à la présente mise en demeure, il sera considéré que la procédure est close et un courrier leur sera adressé en ce sens.

À l'inverse, si les sociétés FACEBOOK Inc. et FACEBOOK Ireland Limited ne se sont pas conformées à la présente mise en demeure, un rapporteur pourra être désigné qui pourra demander à la formation restreinte de la Commission de prononcer l'une des sanctions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente

Isabelle FALQUE-PIERROTIN