Numéro d'ordre Chambre :
222
Répertoire :
2015 /
Date du jugement :
9 novembre 2015
Numéro de rôle :
15/57/C

( ) Ne pas présenter au destinataire

Expédition
Libre : art. 260, 2°
C. enreg.
[illisible] art. 792-1030)

TRIBUNAL DE PREMIÈRE INSTANCE NÉERLANDOPHONE DE BRUXELLES

Ordonnance

Chambre des référés
Mesures provisoires
Art. 584 du Code judiciaire

Présenté le :
Ne pas enregistrer

En cause de :

Monsieur **WILLEM DEBEUCKELAERE**, agissant conformément à l'article 32, §3 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel en sa qualité de **PRÉSIDENT DE LA COMMISSION BELGE DE LA PROTECTION DE LA VIE PRIVÉE,** immatriculée sous le numéro d'entreprise 0893.076.921, instituée par la Chambre des représentants conformément à l'article 23 de la loi précitée du 8 décembre 1992, ayant son siège Rue de la Presse 35 à 1000 Bruxelles, où il fait élection de domicile,

Partie demanderesse,
Représenté par Maître Frederic Debusseré, Maître Jos Dumortie et Maître Roex, avocats de résidence à 1000 Bruxelles, Rue du Congrès 35 ;

Contre :

1. La société de droit de l'État du Delaware (États-Unis d'Amérique) **FACEBOOK Inc.**, ayant son siège 1601 Willow Road, CA 94025 Menlo Park, États-Unis d'Amérique,

Première partie défenderesse,
Représentée par Maître Dirk Van Liedekerke, avocat de résidence à 1050 Bruxelles, Avenue Louise 326 ;

2. La **SPRL FACEBOOK BELGIUM**, dont le siège social est établi à 1040 Bruxelles, Place Robert Schuman 11, immatriculée sous le numéro d'entreprise 0836.948.464 au RPM de Bruxelles,

Deuxième partie défenderesse,
Représentée par Maître Dirk Lindemans, avocat de résidence à 1000 Bruxelles, Boulevard de l'Empereur 3, en son nom propre et loco Maître Henriette Tielemans, avocate de résidence à 1040 Bruxelles, Avenue des Arts 44 ;

3. La société de droit irlandais **FACEBOOK IRELAND LIMITED**, dont le siège social est établi à 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, 216410, Irlande, immatriculée sous le numéro d'entreprise 462932,

Troisième partie défenderesse,

Représentée par Maître Paul Lefebvre, avocat de résidence à 1050 Bruxelles, Avenue Louise 480 ;

++++++++++++++++++

En cette cause, il a été conclu et plaidé en néerlandais à l'audience publique du 21 septembre 2015.

Après délibération, le président du Tribunal de première instance néerlandophone de Bruxelles prononce l'ordonnance suivante :

Vu :

- la citation signifiée le 10 juin 2015
- les conclusions de la partie demanderesse, déposées au greffe le 17 août 2015
- les conclusions de la première défenderesse, déposées au greffe les 20 juillet et 16 septembre 2015
- les conclusions de la deuxième défenderesse, déposées au greffe le 15 juillet 2015
- les conclusions de la troisième défenderesse, déposées au greffe les 20 juillet et 16 septembre 2015

* * *

1. Faits pertinents et antécédents :

Facebook Inc. est une société de droit des États-Unis d'Amérique, dont le siège principal est établi Menlo Park, Californie, États-Unis. Facebook Inc. met le service Facebook à la disposition des internautes des États-Unis et du Canada.

Facebook Belgium SPRL est une société de droit belge qui a été constituée en 2011 afin d'assurer la gestion des relations avec les autorités et le lobbying. Au moment de sa création, on recensait déjà en Belgique plus de 4 millions de membres Facebook enregistrés.

Facebook Ireland est une société de droit irlandais. Facebook Ireland met le service Facebook à la disposition des internautes de l'U.E. par le biais du site www.facebook.com, conformément à la Déclaration des droits et responsabilités de Facebook.

Les défenderesses affirment que Facebook Inc. ne met pas le service Facebook à la disposition des internautes de l'U.E. et ne dispose d'aucun contrôle sur les données à caractère personnel des utilisateurs de l'U.E. Selon elles, Facebook Ireland est la seule personne morale à même d'exercer un contrôle sur les données à caractère personnel reçues dans le cadre de l'exploitation du service Facebook en dehors des États-Unis et du Canada.

Facebook Ireland serait dès lors seule responsable du traitement des données reçues par le biais de la plateforme Facebook, y compris les données reçues par l'intermédiaire des cookies et plug-ins concernant les navigateurs ou appareils des internautes belges. Il existerait certaines différences significatives entre le service Facebook proposé par Facebook Inc. aux États-Unis et au Canada, et celui proposé par Facebook Ireland dans l'U.E. et le reste du monde.

Lorsqu'une page web donnée est créée sur Internet, le propriétaire de ce site web publie ou montre son propre contenu à partir de ses propres serveurs (« serveur First party » ou « serveur de première partie »), mais il met souvent aussi à disposition du contenu d'autres sites web, contenu qui est enregistré sur les serveurs de ces tierces parties (« serveurs Third party » ou « serveurs tiers »).

Lorsqu'un utilisateur veut lire une page web donnée (requête http), le navigateur envoie automatiquement certaines informations à chaque serveur « First party » ou « Third party » sur lequel le contenu demandé est enregistré. Typiquement, ces informations incluent l'adresse IP du nœud de réseau (« node ») utilisé par l'ordinateur pour transmettre la requête, l'URL du site web qui a fourni le lien vers le site web de la première partie, et tous les cookies placés au préalable par le site web à destination duquel le navigateur envoie une requête de contenu (« First party » ou « Third party »).

Le serveur de première partie envoie ensuite les informations de la page web au navigateur. En marge du contenu de première partie de la page web, ces informations contiennent également les instructions dont le navigateur a besoin pour charger le contenu de tierce partie que le développeur du site web a choisi pour la page concernée.

Le navigateur de l'internaute enregistre ces informations sans aucune intervention ni demande des serveurs tiers et envoie à ces derniers une requête http en vue d'obtenir le contenu nécessaire pour poursuivre le chargement du site web. Ces requêtes http contiennent typiquement (1) une adresse IP, (2) l'URL du site web de première partie, (3) le système d'exploitation du navigateur, (4) le type de navigateur et (5) les cookies placés au préalable par le site web de tierce partie à partir duquel le navigateur demande le contenu de tierce partie.

Les sites web de tierce partie reçoivent donc automatiquement tous les cookies ayant trait au site web de tierce partie dont le contenu est demandé, ainsi que l'adresse IP liée à la requête et l'identité du site web de première partie qui est visité par l'internaute.

Un cookie est un simple fichier texte qu'un serveur web envoie à un navigateur qui demande d'accéder au serveur. Le navigateur conserve ce fichier dans un dossier en vue d'un usage ultérieur. Les navigateurs ont été conçus de telle manière qu'un cookie qui a été enregistré dans un navigateur

sera automatiquement communiqué au serveur web qui l'a initialement envoyé chaque fois que le navigateur demandera à accéder à ce serveur. De cette manière, le serveur pourra identifier le navigateur dont provient la requête et trouver les informations spécifiques au navigateur qui sont nécessaires pour la mise à disposition efficace des services et du contenu demandés.

Certains cookies peuvent contenir une séquence de caractères (alphanumériques) qui correspondent à un navigateur (l'identificateur, ou « random identifier »). Les cookies utilisent souvent un identificateur généré par une machine qui permet au serveur web de distinguer les navigateurs qui envoient des requêtes en vue de journaliser et de compter les requêtes « uniques » des navigateurs (les « server hits » (visites) qui sont journalisés à partir de navigateurs uniques et non redondants sur une certaine période, par exemple). Chaque fois que la machine envoie un nouvel appel au serveur web, le cookie sera scanné et le serveur web pourra journaliser l'identificateur qui se trouve dans le cookie, et donc se baser sur les informations qui ont déjà été communiquées précédemment dans le cadre de cette session de journalisation.

Les cookies peuvent également permettre aux sites web de proposer aux utilisateurs enregistrés une fonction « se rappeler de moi » qui permet à ces derniers de gagner du temps. Cette fonction repose sur des cookies qui permettent une connexion spontanée chaque fois qu'un utilisateur accède au site web. L'utilisateur ne devra donc plus réintroduire à chaque fois ces informations lorsqu'une page du site web est appelée par un navigateur ou appareil spécifique. Dès lors, l'utilisateur est en mesure de mieux sécuriser son compte en utilisant des mots de passe et phrases de passe plus complexes.

Plus particulièrement, les propriétaires de sites web utilisent les cookies pour garantir la sécurité des données à caractère personnel de leurs utilisateurs enregistrés, pour prévenir le piratage malveillant et pour contrer les attaques par spams. Les cookies aident notamment à avertir un site web lorsqu'une personne tente de se connecter à un compte depuis un nouvel emplacement, et aident les sites web à identifier les spams, les attaques par déni de service (« denial of service ») et autres activités malveillantes.

Un plug-in est une fraction de contenu (« content ») ou de logiciel que le propriétaire d'un site web peut intégrer à sa page web afin d'offrir à ses visiteurs une fonctionnalité ou un contenu mis à disposition par un site web d'une tierce partie. Ce sont les propriétaires des sites web qui décident quels plug-ins ils intègrent à leurs sites, et dans quelle mesure.

Un propriétaire de site web ajoute un plug-in sur un site web en ancrant dans ce dernier une instruction qui ordonne au navigateur du visiteur d'envoyer une requête http aux serveurs de l'entreprise qui propose la fonctionnalité du plug-in. Cette fonctionnalité se charge alors directement dans le navigateur de l'utilisateur, depuis le serveur de cette entreprise. Les plug-ins permettent ainsi aux propriétaires des sites web d'étendre considérablement l'éventail de fonctionnalités avancées et de contenu qu'ils proposent sur leur site.

Les plug-ins sociaux sont une catégorie de plug-ins permettant aux sites web d'offrir, notamment, à leurs visiteurs la possibilité de partager du contenu avec leur réseau social. Par exemple pour un article, en postant une réaction ou un commentaire par le biais d'un plug-in Facebook afin d'alimenter un débat, ou en « aimant » un article et en le partageant avec leurs contacts sur les médias sociaux. De cette manière, les propriétaires des sites web parviennent grâce aux plug-ins à exploiter les communautés d'utilisateurs existantes sans devoir développer de fonctionnalités propres.

Comme nombre d'autres entreprises actives sur Internet, le service Facebook propose toute une gamme de plug-ins sociaux parmi lesquels les propriétaires de sites web peuvent choisir ceux qu'ils veulent intégrer à leurs propres sites. Ces fonctionnalités offrent aux titulaires d'un compte Facebook un moyen simple de partager des informations et de communiquer à ce sujet avec d'autres utilisateurs du service Facebook avec qui ils ont choisi de partager du contenu (leurs « amis Facebook ») pendant qu'ils surfent sur des sites autres que Facebook.

Un propriétaire de site web peut par exemple placer sur son site web le bouton « J'aime » afin de permettre à ses visiteurs de faire savoir à leurs amis Facebook et aux autres visiteurs du site web en question qu'ils approuvent ce contenu (qu'ils l'« aiment »). De cette manière, tous les internautes (y compris les utilisateurs non inscrits de Facebook) peuvent voir combien de mentions « J'aime » une page web a recueillies.

D'autres plug-ins Facebook, comme le plug-in « Réagir », permettent aux propriétaires de sites web d'afficher directement sur leur page les commentaires et réactions des titulaires d'un compte Facebook, ce qui simplifie bien entendu considérablement la communication et l'interaction.

Facebook Ireland conserve par ailleurs un journal des accès qui journalise des informations au sujet des appareils ou navigateurs chaque fois qu'une requête est envoyée aux serveurs de la plateforme Facebook en vue du chargement d'une page web facebook.com ou d'un plug-in social d'un service Facebook. Elle affirme conserver ces données dans le but de garantir la sécurité du service Facebook et d'améliorer la qualité de ses services.

Ces informations précisent également la présence ou non dans le navigateur du cookie « Datr ». Selon Facebook Ireland, ces journaux des accès servent des objectifs essentiels en termes d'intégrité du site web, d'efficacité et – surtout – de sécurité.

L'entreprise affirme également ne conserver ces données que pendant une période suffisamment longue que pour garantir une sécurité effective, et ne conserver les données de journalisation ayant trait aux navigateurs des internautes ne disposant pas d'un compte Facebook que pendant une période de dix jours à compter de leur création.

Les données enregistrées dans les journaux des accès des serveurs web de Facebook Ireland contiennent des données d'adresses IP anonymes et des identificateurs de cookie de navigateur « Datr » anonymes (appelés « browser identifiers »). Selon Facebook Ireland, un opérateur de site web ne serait pas en mesure d'identifier ou de sélectionner sur la base de ces seules informations un utilisateur individuel non inscrit.

Facebook Ireland affirme ne placer le cookie « Datr » sur un navigateur que lorsqu'un internaute disposant d'un compte Facebook ou un utilisateur non inscrit de Facebook (c'est-à-dire une personne qui choisit de visiter un site web du domaine facebook.com ou d'interagir au moyen d'un plug-in Facebook sur un site web de tiers) interagit explicitement avec le service Facebook.

Elle déclare ne pas appliquer le cookie « Datr » en qualité de tierce partie. Cela signifie qu'un navigateur Internet ne reçoit le cookie « Datr » que si un internaute interagit directement avec le service Facebook, par exemple (i) en visitant une page sur facebook.com ou (ii) en interagissant activement avec du contenu Facebook, notamment par le biais d'un plug-in social.

Il est apparu pendant les débats que Facebook, depuis la citation dans le cadre de la présente procédure, déploie dans toute l'U.E., y compris en Belgique, une bannière relative aux cookies lorsque l'utilisateur n'est pas inscrit sur Facebook, afin d'aller au-devant des éventuelles inquiétudes à l'égard du caractère adéquat du consentement. La bannière relative aux cookies s'est inspirée des discussions qui ont été entamées l'année dernière avec la Commission de protection des données irlandaise (DPC). Selon Facebook Ireland, cette bannière est déployée au sein de l'U.E. afin de consolider le consentement que les internautes européens donnent lorsqu'ils interagissent avec un service Facebook.

Lors d'une première visite sur un site facebook.com, Facebook fait apparaître une bannière qui explique que Facebook recourt à des cookies lorsqu'un visiteur de la plateforme Facebook est un utilisateur non inscrit. Facebook Ireland prévoit aussi un lien vers des informations additionnelles sur la manière dont la plateforme Facebook utilise les cookies.

Les défenderesses affirment à présent que si l'utilisateur quitte la page ou suit le lien vers les informations additionnelles, aucun cookie n'est enregistré.

La Commission de la protection de la vie privée prétend le contraire.

De plus, il y aurait un lien « cookie » sur virtuellement chaque page facebook.com, et les informations communiquées par Facebook Ireland dans sa politique d'utilisation des cookies précisent que les cookies sont dans ces situations utilisés pour garantir la sécurité du site et de l'utilisateur.

Selon Facebook Ireland, cette bannière lui procure le consentement de l'utilisateur avant l'enregistrement du cookie « Datr ».

Facebook Ireland affirme que le cookie de sécurisation « Datr » joue un rôle essentiel dans la protection du service Facebook, tant au profit des utilisateurs disposant d'un compte Facebook que des utilisateurs non inscrits de Facebook, contre toute une série de menaces de sécurité dont elle cite une dizaine d'exemples dans ces conclusions.

Facebook Ireland explique aussi que ses pratiques à l'égard du cookie « Datr » et des plug-ins sociaux dans le cas des utilisateurs non inscrits de Facebook n'ont pas changé depuis l'audit détaillé et l'enquête réalisée par la DPC en 2011, 2012 et 2014, ni depuis l'entrée en vigueur de la Nouvelle politique d'utilisation des données (« nouvelles conditions et règles de la politique d'utilisation des données ») du 30 janvier 2015. Pour la réalisation de cet audit, la DPC avait travaillé en collaboration et en concertation avec d'autres instances de surveillance européennes compétentes pour la protection des données, y compris le Groupe de travail Article 29, lequel organise la concertation entre les instances de surveillance européennes, dont fait partie la Commission belge de la protection de la vie privée.

À la suite de l'annonce, en novembre 2014, de la modification des conditions d'utilisation et des questions à ce sujet émanant d'utilisateurs inquiets de Facebook, des médias, du parlement fédéral et du Secrétaire d'État à la Protection de la vie privée, la Commission de la protection de la vie privée a ouvert une enquête technique et juridique en vue de confronter ces nouvelles conditions d'utilisation et les modifications apportées à la législation belge en matière de protection de la vie privée.
Elle a également fait appel dans ce contexte à l'expertise technique de chercheurs scientifiques de la Katholieke Universiteit Leuven et de la Vrije Universiteit Brussel ayant, dans le cadre de leurs projets de recherche en cours, déjà mené des enquêtes approfondies au sujet de Facebook.

Le 31 mars 2015, la dernière version du rapport d'enquête intitulé « From social media service to advertising network. A critical analysis of Facebook Revised Policies and Terms » (traduction libre : « D'un média social à un réseau publicitaire. Analyse critique de la nouvelle politique d'utilisation de Facebook ») a été publiée sur le site web de l'Interdisciplinair Centrum voor Rechten ICT (ICRI) de la KU Leuven.

L'une des conclusions de ce rapport est que Facebook traite également, par le biais de plug-ins sociaux et de cookies, des données à caractère personnel d'internautes qui ne disposent pas d'un compte Facebook. Ce faisant, Facebook suit le parcours de navigation de personnes ne disposant pas d'un compte Facebook.

Les plug-ins sociaux sont particulièrement populaires auprès des propriétaires de sites web étant donné le succès croissant de leur site à mesure que les visiteurs utilisent le plug-in social pour faire savoir à leurs « amis » qu'ils « aiment » ce site. Le bouton « J'aime » (le plug-in le plus populaire de Facebook) est présent sur pas moins de 32 % des 10.000 sites web les plus visités, toutes catégories confondues.

Le rapport d'enquête démontre que chaque fois qu'une personne n'étant pas un utilisateur de Facebook visite un site web du domaine facebook.com, dont notamment les pages Facebook personnelles d'individus, firmes et autres organisations, Facebook enregistre automatiquement un cookie sur le disque dur de ce visiteur. De telles pages web, toutes accessibles en Belgique, sont également fréquentées par des non-utilisateurs belges.

Le cookie en question, qui est appelé « Datr » par Facebook et que nous évoquions déjà plus haut, contient des informations qui identifient de manière unique le navigateur d'un internaute. Ce cookie est conservé sur son disque dur pendant deux ans.

Lorsque cet internaute visite ensuite un site web sur lequel se trouve un plug-in de Facebook, son navigateur établira en règle générale une connexion automatique avec le serveur de Facebook afin de charger le plug-in. Du fait de cette connexion, des informations du cookie « Datr » de Facebook ayant été enregistrées sur le disque dur de l'utilisateur sont envoyées aux serveurs de Facebook.

Dans le sillage de cette enquête, la Commission de la protection de la vie privée a mené une correspondance abondante avec Facebook.

Dans cette correspondance, Facebook affirmait notamment que la société Facebook Ireland Limited devrait être considérée comme responsable du traitement et qu'elle était disposée à fournir des explications verbales au sujet de ses services, mais rejetait néanmoins l'applicabilité du droit belge en matière de protection de la vie privée ainsi que la compétence de la Commission belge de la protection de la vie privée. Elle ajoutait dans la foulée que, si la Commission belge de la protection de la vie privée nourrissait des inquiétudes au sujet du traitement des données à caractère personnel assuré en Belgique par Facebook, elle devait se mettre en rapport avec la Commission irlandaise de protection des données, laquelle est selon Facebook seule compétente pour les activités de Facebook au sein de l'Union européenne.

Dans son courrier du 6 mars 2015, Facebook confirmait également ne pas utiliser d'informations sensibles à des fins de ciblage publicitaire personnalisé.

Après une première réunion le 15 avril 2015, la Commission de la protection de la vie privée a entendu les représentants de Facebook à l'occasion d'une audience qui s'est tenue le 29 avril 2015 dans le cadre d'une procédure de recommandation.

Le 13 mai 2015, la Commission de la protection de la vie privée a émis en application de l'article 30, §1er de la loi relative à la protection de la vie privée une recommandation qui contenait une analyse juridique des constatations techniques figurant dans le rapport d'enquête portant sur les plug-ins sociaux et cookies de Facebook.

Dans sa recommandation, la Commission de la protection de la vie privée confirme notamment que la législation belge en matière de protection de la vie privée est applicable et que la Commission belge de la protection de la vie privée est dès lors compétente pour s'opposer dans l'intérêt de l'ordre public à l'enregistrement par Facebook du comportement de navigation des internautes belges. Elle affirme également que le traitement par Facebook, par le biais de plug-ins sociaux et de cookies, de données à caractère personnel d'internautes ne disposant pas d'un compte Facebook – dont la collecte de données concernant les sites web visités par les internautes belges ne disposant pas d'un compte Facebook – constitue une violation de la loi relative à la protection de la vie privée et de l'article 129 de la loi relative aux communications électroniques.

Concernant les non-utilisateurs de Facebook, la Commission de la protection de la vie privée a ordonné que Facebook renonce à l'enregistrement systématique, sur les systèmes des non-utilisateurs de Facebook, de cookies durables permettant une identification unique.

Par courrier recommandé et e-mail du 18 mai 2015, la Commission de la protection de la vie privée a mis en demeure Facebook Inc. et la SPRL Facebook Belgium du chef de leurs violations de la loi relative à la protection de la vie privée ainsi que de l'article 129 de la loi relative aux communications électroniques, sommant les deux sociétés de lui faire savoir pour le 27 mai 2015 au plus tard si elles étaient disposées à mettre un terme à ces violations.

Par courrier recommandé et e-mail de leur conseil en date du 26 mai 2015, Facebook Inc. et Facebook Belgium ont fait connaître leur désir d'initier avec la Commission de la protection de la vie privée une concertation au sujet de la recommandation, et ont demandé à ce qu'un rendez-vous soit pris en vue d'un entretien.

La correspondance par courrier et par e-mail qui s'en est suivie n'a cependant pas rapproché les parties. La Commission de la protection de la vie privée est en effet restée sur ses positions concernant son propre pouvoir de juridiction et l'applicabilité de la législation belge en matière de protection de la vie privée, maintenant que Facebook devait renoncer immédiatement au traitement de données à caractère personnel d'internautes ne disposant pas d'un compte Facebook. De leur côté, les défenderesses continuent d'affirmer en substance qu'elles disposent du consentement au moins implicite, si pas explicite, des utilisateurs en vue de ce traitement, et que seule la Commission irlandaise de protection des données est compétente pour ses activités au sein de l'Union européenne. Par essence, Facebook affirme même que le fait, pour la Commission de la protection de la vie privée, d'exiger que Facebook reconnaisse son pouvoir de juridiction et l'applicabilité de la loi belge, équivaut à un refus de tout dialogue constructif.

Vu que la Commission de la protection de la vie privée part du principe que Facebook ne mettra pas volontairement un terme à ce traitement litigieux, elle a initié par le truchement de son président une procédure en référé.

2. Demandes des parties :

Monsieur WILLEM DEBEUCKELAERE, agissant en sa qualité de PRÉSIDENT DE LA COMMISSION BELGE DE LA PROTECTION DE LA VIE PRIVÉE**,** demande à présent au Président du Tribunal de première instance néerlandophone de Bruxelles, siégeant en référé, de déclarer la demande recevable et fondée ;

De condamner en conséquence à titre de mesure provisoire Facebook Inc, la SPRL Facebook Belgium et – pour autant que le Tribunal estime que Facebook Ireland Limited est responsable des traitements de données à caractère personnel en Belgique (quod non) ou est impliquée de quelque autre manière – Facebook Ireland Limited, à renoncer, à l'égard de tout internaute se trouvant sur le territoire belge et ne s'étant pas inscrit en tant que membre du réseau social en ligne de Facebook :

- à l'enregistrement d'un cookie « Datr » lorsque lesdits internautes visitent une page web du domaine facebook.com, sans les informer suffisamment et adéquatement au préalable du fait que Facebook enregistre le cookie « Datr » sur leurs systèmes ainsi que de l'usage que Facebook fait de ce cookie « Datr » par le biais des plug-ins sociaux ;
- à la collecte des cookies « Datr » par le biais de plug-ins sociaux placés sur des sites web de tiers ;

Le tout sous peine d'une astreinte, in solidum et au moins l'une à défaut de l'autre, de 250.000 EUR par jour faisant l'objet d'une infraction, et ce à compter de la date de l'ordonnance à intervenir ;

De condamner les défenderesses aux dépens de la procédure, y compris les frais de citation et l'indemnité de procédure, laquelle est actuellement estimée à 1.320 EUR par défenderesse ;

De déclarer l'ordonnance à intervenir exécutoire par provision, nonobstant tout recours et sans caution ni offre de cantonnement.

Pour sa part, la société de droit de l'État du Delaware FACEBOOK INC. demande au Président du Tribunal :

- de se déclarer incompétent ;
- à titre subsidiaire, de déclarer la demande inadmissible et à tout le moins irrecevable ;
- à titre encore plus subsidiaire, de rejeter la demande comme non fondée ; et

- dans tous les cas, de condamner la demanderesse aux dépens, estimés dans le chef de la première défenderesse à 1.320 EUR au titre d'indemnité de procédure.

Par ailleurs, la SPRL FACEBOOK BELGIUM demande au Président :
- de se déclarer incompétent ;
- à titre subsidiaire, de déclarer la demande inadmissible et à tout le moins irrecevable ;
- à titre encore plus subsidiaire, de rejeter la demande comme non fondée ;
- à titre tout à fait subsidiaire, de ne pas prononcer l'interdiction à l'encontre de la deuxième défenderesse Facebook Belgium ; et
- dans tous les cas, de condamner la demanderesse aux dépens, estimés dans le chef de la SPRL FACEBOOK BELGIUM à 1.320 EUR au titre d'indemnité de procédure.

Enfin, la société de droit irlandais FACEBOOK IRELAND LIMITED demande au Président du Tribunal :
- de se déclarer incompétent ;
- à titre subsidiaire, de déclarer la demande inadmissible et à tout le moins irrecevable ;
- à titre encore plus subsidiaire, de rejeter la demande comme non fondée ; et
- dans tous les cas, de condamner la demanderesse aux dépens, estimés dans le chef de la troisième défenderesse à 1.320 EUR au titre d'indemnité de procédure.

3. Appréciation :

3.1 Pouvoir de juridiction international et loi applicable :

L'article 4 de 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, dispose :
« Article 4

Droit national applicable

1. Chaque État membre applique les dispositions nationales qu'il arrête en vertu de la présente directive aux traitements de données à caractère personnel lorsque :

a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre ; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable ;

b) le responsable du traitement n'est pas établi sur le territoire de l'État membre mais en un lieu où sa loi nationale s'applique en vertu du droit international public ;

c) le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

2. Dans le cas visé au paragraphe 1 point c), le responsable du traitement doit désigner un représentant établi sur le territoire dudit État membre, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même. »

Dans ce dossier, la Commission de la protection de la vie privée, par le truchement de son président, a également cité la SPRL FACEBOOK BELGIUM. Les défenderesses ne contestent pas que FACEBOOK BELGIUM, en sa qualité de filiale de FACEBOOK GLOBAL HOLDINGS I LLC et FACEBOOK GLOBAL HOLDINGS II LLC, fasse partie du groupe FACEBOOK dont la première défenderesse FACEBOOK INC. est la société mère et a le plus voix au chapitre.

La SPRL FACEBOOK BELGIUM, établie à Bruxelles, est un établissement belge du responsable du traitement des données sur le réseau Facebook. Le siège adhère au point de vue de la Commission de la protection de la vie privée lorsque cette dernière affirme qu'il n'est somme toute pas pertinent dans ce dossier de déterminer, pour l'application de l'article 4.1.a) de la directive 95/46/CE, si le responsable du traitement est FACEBOOK INC. ou FACEBOOK IRELAND LIMITED : FACEBOOK IRELAND LIMITED fait en effet elle aussi partie, incontestablement, du groupe FACEBOOK par le truchement de FACEBOOK CAYMAN HOLDINGS UNLIMITED IV et FACEBOOK IRELAND HOLDINGS.

De plus, il n'est pas pertinent que le traitement ait lieu sur le territoire d'un État membre de l'U.E. ou en dehors de l'U.E. L'application de l'article 4.1.a) de la directive 95/46/CE n'en est pas tributaire. À cet égard, il convient de faire remarquer avant tout que le point 19 des considérants de la directive 95/46/CE précise que *« l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable »* et que *« la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard »*.

Les défenderesses disent elles-mêmes que la SPRL Facebook Belgium est une société de droit belge qui a été constituée en 2011 afin d'assurer la gestion des relations avec les autorités et le lobbying.

Il ressort par ailleurs des conclusions du 15 juillet 2015 de la SPRL Facebook Belgium et des conclusions du 20 juillet 2015 de Facebook Inc. que deux membres du personnel de Facebook Belgium entretiennent des contacts avec des entreprises belges à des fins de support dans le domaine du marketing et de la vente d'espace publicitaire par Facebook Ireland, et que deux de ses travailleurs offre à Facebook Ireland un support dans le cadre des activités publicitaires.

La Commission de la protection de la vie privée démontre de manière convaincante, sur la base de citations issues des derniers comptes annuels de Facebook Belgium et de l'audience du 29 avril 2015, que l'activité principale de la société consistait en 2014 à soutenir la politique à l'égard du public, à soutenir les ventes et à fournir au Groupe Facebook des services de marketing.

Cela signifie que les activités du responsable du traitement et celles de la SPRL Facebook Belgium sont indissociablement liées au sens visé par la Cour de Justice de l'U.E. dans son arrêt C-131/12 (Grande chambre) du 13 mai 2014 (demande de décision préjudicielle introduite par l'Audiencia Nacional – Espagne) – Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González (http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:62012CJ0131&rid=4) :
« 52 Cependant, ainsi que l'ont souligné notamment le gouvernement espagnol et la Commission, l'article 4, paragraphe 1, sous a), de la directive 95/46 exige non pas que le traitement de données à caractère personnel en question soit effectué « par » l'établissement concerné lui-même, mais uniquement qu'il le soit « dans le cadre des activités » de celui-ci.

53 En outre, au vu de l'objectif de la directive 95/46 d'assurer une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée, à l'égard du traitement des données à caractère personnel, cette dernière expression ne saurait recevoir une interprétation restrictive (voir, par analogie, arrêt L'Oréal e.a., C-324/09, EU:C:2011:474, points 62 et 63).

54 Il convient de relever dans ce contexte qu'il ressort notamment des considérants 18 à 20 et de l'article 4 de la directive 95/46 que le législateur de l'Union a entendu éviter qu'une personne soit exclue de la protection garantie par celle-ci et que cette protection soit contournée, en prévoyant un champ d'application territorial particulièrement large.

55 Compte tenu de cet objectif de la directive 95/46 et du libellé de son article 4, paragraphe 1, sous a), il y a lieu de considérer que le traitement de données à caractère personnel qui est fait pour les besoins du service d'un moteur de recherche tel que Google Search, lequel est exploité par une entreprise ayant son siège dans un État tiers mais disposant d'un établissement dans un État membre, est effectué « dans le cadre des activités » de cet établissement si celui-ci est destiné à assurer, dans cet État membre, la promotion et la vente des espaces publicitaires proposés par ce moteur de recherche, qui servent à rentabiliser le service offert par ce moteur.

56 En effet, dans de telles circonstances, les activités de l'exploitant du moteur de recherche et celles de son établissement situé dans l'État membre concerné sont indissociablement liées dès lors que les activités relatives aux espaces publicitaires constituent le moyen pour rendre le moteur de recherche en cause économiquement rentable et que ce moteur est, en même temps, le moyen permettant l'accomplissement de ces activités.

57 À cet égard, il convient de rappeler que, ainsi qu'il a été précisé aux points 26 à 28 du présent arrêt, l'affichage même de données à caractère personnel sur une page de résultats d'une recherche constitue un traitement de telles données. Or, ledit affichage de résultats étant accompagné, sur la même page, de celui de publicités liées aux termes de recherche, force est de constater que le traitement de données à caractère personnel en question est effectué dans le cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire espagnol. »

Vu cet objectif de la directive 95/46 et les termes de son article 4, alinéa 1, point a), il y a lieu de considérer que le traitement de données à caractère personnel aux fins d'un service d'un réseau social comme Facebook, lequel est exploité par une entreprise ayant son siège social dans un pays tiers, mais dispose d'un établissement d'un État membre, est effectué *« dans le cadre des activités »* de cet établissement si celui-ci est destiné à assurer, dans cet État membre, la promotion et la vente des espaces publicitaires proposés par ce réseau social, qui servent à rentabiliser le service offert par ce réseau social.

À cet égard, il convient de rappeler que l'affichage lui-même de données à caractère personnel sur une page Facebook constitue un traitement de telles données. Étant donné que l'affichage de cette page Facebook va de pair avec l'affichage, sur la même page web, de publicités ayant trait aux activités de l'utilisateur, il y a lieu de constater que le traitement de données à caractère personnel en question est effectué dans le cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire belge.

Par ailleurs, de l'avis du siège, la gestion des relations avec les autorités et le lobbying assurés par cet établissement constituent également une activité servant à rentabiliser le service offert par ce réseau social, de sorte que les activités de Facebook Belgium sont pour cette raison indissociablement liées aux activités de l'exploitant du réseau social.

Le fait que Facebook Belgium ne traite pas elle-même les données à caractère personnel et ne conclurait pas elle-même les contrats avec les annonceurs n'est pas pertinent. L'élément déterminant pour l'application de l'article 4.1.a) de la directive 95/46/CE ne repose pas sur cet aspect, mais bien sur la constatation que les activités de Facebook Belgium sont pour cette raison indissociablement liées aux activités de l'exploitant du réseau social.

Il en découle que la Belgique peut, en vertu de l'article 4.1.a) de la directive 95/46/CE, appliquer dans ce dossier ses dispositions nationales adoptées en exécution de ladite directive au traitement de données à caractère personnel étant donné que celui-ci est effectué dans le cadre des activités d'un établissement du responsable du traitement se trouvant sur le territoire belge. Étant donné que ce même responsable a un établissement sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour veiller à ce que chacun de ces établissements, dont l'établissement belge, respecte les obligations qui lui sont imposées par la législation locale applicable, en l'occurrence donc la législation belge.

La Commission de la protection de la vie privée n'a par conséquent pas utilisé artificiellement la présence de Facebook Belgium dans le cadre de la présente procédure, et la citation multiple n'est pas comparable à la « Belgian Torpedo » – entretemps morte et enterrée – par laquelle d'aucuns ont par le passé tenté de saboter la compétence de juridictions étrangères : dans le dossier qui nous occupe, il est question de l'application de la législation belge sur le territoire belge, et Facebook Belgium est bel et bien un établissement belge du responsable du traitement au sens de l'article 4.1.a) de la directive 95/46/CE.

Le juge belge dispose ainsi d'un pouvoir de juridiction international pour statuer sur la présente demande, et applique de surcroît la législation belge.

C'est d'autant plus vrai que le président du Tribunal de première instance siégeant en référé a le pouvoir de pleine juridiction. Même si seul un juge étranger avait juridiction pour statuer sur le fond de cette affaire, le juge des référés civil belge resterait compétent (voir notamment J. LAENENS, K. BROECKX, D. SCHEERS et P. THIRIAR, Handboek Gerechtelijk Recht, Anvers, 2012, Intersentia, p. 263, n° 596) pour prendre des mesures provisoires.

3.2 Compétence

Dans l'examen de la question de savoir si le juge des référés est compétent, il doit vérifier si l'urgence ressort de l'acte introductif d'instance, explicitement ou même implicitement.

La citation stipule que l'affaire est urgente. Le juge des référés est par conséquent compétent pour examiner le dossier sur le fond (Cass., 11 mai 1990, Pas., 1990, I, 1045).

3.3 Recevabilité de la demande

Facebook Inc. comprend que la citation ait été envoyée tant par courrier que par le biais de l'Autorité centrale. Étant donné que Facebook Inc. peut confirmer avoir reçu la citation le 20 août 2015 par le biais de l'Autorité centrale, elle n'invoque plus la question de l'absence de signification vu que celle-ci est désormais sans objet.

À son tour, le siège ne peut toutefois pas adhérer au raisonnement selon lequel la réduction du délai de citation serait illégitime, étant donné qu'un tel point de vue irait à l'encontre de l'autorité de chose jugée de l'ordonnance du 5 juin 2015 rendue par le Vice-président de ce Tribunal, désigné pour remplacer le Président, laquelle autorisait la réduction des délais de citation.
La présente procédure n'est en effet pas une tierce opposition ni un appel à ladite ordonnance, et ne peut pas être considérée comme un moyen de droit contre celle-ci. La considération stipulée dans ladite ordonnance, selon laquelle elle n'oblige pas le juge des référés à suivre son jugement au sujet de l'urgence, ne concerne que l'urgence de la procédure en référé, mais ne porte nullement préjudice au fait que la réduction des délais de citation a été autorisée par une décision judiciaire ayant autorité de chose jugée.

L'article 32, §3 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel dispose :
« Article 32. (...)
§3. Sans préjudice de la compétence des cours et tribunaux ordinaires pour l'application des principes généraux en matière de protection de la vie privée, le Président de la Commission peut soumettre au tribunal de première instance tout litige concernant l'application de la présente loi et de ses mesures d'exécution. »

Il est d'ores et déjà établi que le Président de la Commission de la protection de la vie privée est investi de l'intérêt et de la qualité requis pour intenter la présente procédure. Lorsque le siège fait référence plus loin dans la présente ordonnance à « la Commission de la protection de la vie privée », c'est en partant du principe que le président exerce bien entendu sa compétence non en son nom propre, mais bien en sa fonction de président et représentant de la Commission de la protection de la vie privée.

La loi du 13 juin 2005 relative aux communications électroniques est la transposition en droit belge de – notamment – la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques ») (JOCE 31 juillet 2002, L 201/37) (art. 1er de la loi). Cette directive dispose en son article premier :

« Article premier

Champ d'application et objectif

1. La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.
(...) »

Dès lors que la loi du 13 juin 2005 relative aux communications électroniques constitue une transposition de cette directive, elle spécifie et complète également la directive 95/46/CE, elle-même transposée par la loi relative à la protection de la vie privée.

Dans ce sens – et uniquement en ce sens – la Commission de la protection de la vie privée peut donc invoquer l'article 129 de la loi relative aux communications électroniques. L'article 129 de la loi relative aux communications électroniques, qui est invoqué par la Commission de la protection de la vie privée, renvoie lui-même à deux reprises à la loi relative à la protection de la vie privée, lorsqu'il stipule que l'abonné ou l'utilisateur concerné doit recevoir conformément aux conditions fixées dans la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, des informations claires et précises concernant les objectifs du traitement et ses droits sur la base de la loi du 8 décembre 1992, et que son consentement n'exempte pas le responsable du traitement des obligations de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui ne sont pas imposées par ledit article.

3.4 Urgence

Il est question d'urgence au sens de l'article 584, alinéa premier du Code judiciaire dès que la crainte d'un préjudice d'une certaine gravité, voire d'inconvénients sérieux, rend une décision immédiate souhaitable (Cass., 21 mai 1987, Pas., 1987, I, 1160).

La partie demanderesse rend l'urgence de la demande plausible étant donné qu'une demande qui a trait à des droits et libertés fondamentaux (droits fondamentaux) ayant été violés par un acte de la partie défenderesse est toujours urgente. Il ressort de plusieurs considérants, dont en particulier le considérant 10 de la directive 95/46/CE, que ladite directive vise explicitement la protection des droits fondamentaux :

« (10) Considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté ; »

De plus, la Commission de la protection de la vie privée souligne à juste titre que la violation alléguée a trait non aux droits fondamentaux d'un seul individu, mais bien d'un énorme groupe d'individus. Il existe en effet en Belgique un nombre incalculable d'internautes qui n'ont pas de compte Facebook mais qui ont un jour ou l'autre visité une page web du domaine facebook.com, et dont l'ordinateur aurait par conséquent enregistré à leur insu le cookie « Datr » de Facebook. Vu les millions de sites web dotés des plug-ins sociaux de Facebook, il est pour ainsi dire impossible d'y échapper. Il s'agit également d'informations très sensibles concernant notamment la santé ou les préférences religieuses, sexuelles ou politiques (par exemple lorsque des personnes consultent de nombreux sites web consacrés à un certain problème de santé ou à une préférence religieuse, sexuelle ou politique).

Une décision immédiate visant à prévenir ce nombre colossal de violations potentielles serait donc souhaitable. La demande est par conséquent urgente.

La Commission belge de la protection de la vie privée ne s'est pas non plus rendue coupable de négligence, puisqu'elle est entrée en action immédiatement après l'arrêt « Google Spain », lequel a fondamentalement modifié la jurisprudence relative à la compétence des États membres de l'U.E. à l'égard des entreprises actives sur Internet qui opèrent sur leur territoire sans y traiter localement de données à caractère personnel, mais qui y possèdent un établissement.
L'enquête que la Commission de la protection de la vie privée a réalisée et a fait réaliser concernant les violations alléguées et les discussions qui s'en sont suivies avec Facebook ont naturellement pris beaucoup de temps, de sorte qu'il ne peut être reproché à la Commission de la protection de la vie privée d'avoir tardé à procéder à la citation et d'avoir ainsi créé elle-même l'urgence.

3.5 Évaluation de la modalité de référé

Facebook enregistre manifestement le cookie « Datr » lorsqu'un internaute visite une page web du domaine facebook.com, indépendamment du fait qu'il soit ou non un utilisateur de Facebook. Ce cookie a une durée de validité de deux ans. Pendant ces deux années, le cookie reste sur l'ordinateur de l'internaute, à moins que ce dernier ne le supprime lui-même.

Lorsque cet internaute visite par la suite un site web sur lequel se trouve un plug-in social de Facebook, le serveur de Facebook demandera au navigateur de l'intéressé, lors du chargement du contenu du plug-in social, d'envoyer le cookie « Datr ». Le cookie « Datr » n'est cependant pas le seul composant de la communication entre le navigateur et le serveur de Facebook : l'adresse IP de l'internaute et l'URL du site web sur lequel se trouve le plug-in sont également transmises. L'envoi de l'adresse IP, en particulier, est en effet une propriété essentielle du TCP/IP, le protocole qui permet la communication par Internet et sur lequel repose le protocole HTTP.

La combinaison des cookies « Datr », de l'adresse IP et du site web que l'internaute visite permet à Facebook de suivre le comportement de navigation de l'internaute individuel.

La présente requête de la Commission de la protection de la vie privée vise à entendre dire que Facebook, en (a) enregistrant le cookie « Datr » sur les ordinateurs de non-utilisateurs belges et en (b) interrogeant ensuite les informations contenues dans ce cookie chaque fois que des non-utilisateurs belges visitent un site web sur lequel un plug-in social de Facebook a été intégré, enfreint la loi relative à la protection de la vie privée et l'article 129 de la loi relative aux communications électroniques.

Selon la Commission de la protection de la vie privée, Facebook viole ainsi les articles 4 et 5 de la loi relative à la protection de la vie privée :
« Article 4. §1er. Les données à caractère personnel doivent être :
1° traitées loyalement et licitement ;
2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par le Roi, après avis de la Commission de la protection de la vie privée ;
3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ;
4° exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;
5° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Le Roi prévoit, après avis de la Commission de la protection de la vie privée, des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

§2. Il incombe au responsable du traitement d'assurer le respect du §1er.

Article 5. Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :
a) lorsque la personne concernée a indubitablement donné son consentement ;
b) lorsqu'il 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) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;
d) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
e) lorsqu'il 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 ou le tiers auquel les données sont communiquées ;
f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi.
Le Roi peut, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, préciser les cas où la condition mentionnée sous f) est considérée ne pas être remplie. »

De l'avis de la Commission de la protection de la vie privée, Facebook viole par ailleurs les droits des intéressés en ne leur fournissant pas au préalable les informations pourtant prescrites par l'article 9 de la loi relative à la protection de la vie privée.

Enfin, la Commission de la protection de la vie privée est d'avis que Facebook enfreint l'article 129 de la loi relative aux communications électroniques en collectant le cookie « Datr » chaque fois qu'un non-utilisateur visite un site web d'un tiers sur lequel un plug-in social de Facebook a été intégré, sans avoir obtenu à cette fin le consentement préalable, libre, spécifique, éclairé et indubitable des non-utilisateurs.

Le siège ne peut adhérer au point de vue de Facebook lorsque cette dernière affirme que les informations qu'elle collecte permettraient uniquement d'identifier un ordinateur et ne constitueraient pas des données à caractère personnel.

Les articles 2 de la directive 95/46/CE et 1er, §§1er et 2 de la loi relative à la protection de la vie privée définissent comme suit les concepts « données à caractère personnel » et « traitement des données à caractère personnel » :
« Article 2

Définitions

Aux fins de la présente directive, on entend par :
a) « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;
b) « traitement de données à caractère personnel » (traitement) : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ; »

Le cookie « Datr » que Facebook enregistre sur l'ordinateur d'un internaute et par le biais duquel elle obtient des informations identifie de manière unique le navigateur Internet de l'internaute en question. Le cookie contient en effet un *« unique identifier »*. Facebook reçoit également des informations additionnelles qui lui permettent, directement ou indirectement, d'identifier des individus, par exemple l'adresse IP de l'ordinateur de l'internaute.

Tant la Cour de Justice de l'U.E. que le Groupe de travail Article 29 ont déjà explicitement confirmé que les adresses IP constituent des « données à caractère personnel » (voir notamment l'arrêt de la Cour de Justice, Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) du 24 novembre 2011, C-70/10, point 51 i.f. : *« (...), ces adresses étant des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs »*).

Étant donné que les défenderesses affirment elles-mêmes que le cookie « Datr » est notamment utilisé pour exercer une certaine forme de contrôle d'accès, et donc pour entre autres pour déterminer à qui l'accès à un service Facebook sera le cas échéant refusé, le cookie « Datr » doit à ce titre être lui aussi considéré comme une donnée à caractère personnel.

Le traitement automatisé des adresses IP et des cookies de navigateur permettant une identification unique, comme le cookie « Datr », constitue par conséquent un traitement de données à caractère personnel étant donné qu'il correspond parfaitement à la définition visée à l'article 2, b de la directive 95/46/CE et à l'article 1er, §2 de la loi relative à la protection de la vie privée.

Ce traitement, qui inclut le simple enregistrement ou la simple réception automatisée de ces données du navigateur d'un utilisateur qui visite une page web dotée d'un plug-in social, doit par conséquent satisfaire aux conditions stipulées aux articles 4 et 5 de la loi relative à la protection de la vie privée. Pour cette raison, le fait que Facebook enregistre ces données durablement ou seulement pour une courte durée n'est pas pertinent.

Dans le cas d'un utilisateur qui se trouve sur le territoire belge mais qui ne s'est jamais inscrit sur Facebook, ni n'a valablement consenti, de quelque manière que ce soit, aux conditions d'utilisation de Facebook, mais qui a accédé au domaine facebook.com et a donc fait l'objet d'un enregistrement d'un cookie « Datr », les défenderesses ne prouvent pas qu'elles étaient autorisées en vertu d'un quelconque consentement indubitable de l'utilisateur (art. 5, a de la loi relative à la protection de la vie privée) à enregistrer ce cookie « Datr » et à ensuite le recevoir à nouveau.

En ce qui concerne le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un utilisateur – définition à laquelle l'enregistrement et la lecture ultérieure de cookies répondent manifestement –, l'article 129 de la loi relative aux communications électroniques est des plus explicites :
« Article 129. Le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur est autorisée uniquement à condition que :
1° l'abonné ou l'utilisateur concerné reçoive conformément aux conditions fixées dans la loi du 8 décembre 1992 relative à la protection de la vie privée et à l'égard des traitements de données à caractère personnel, des informations claires et précises concernant les objectifs du traitement et ses droits sur la base de la loi du 8 décembre 1992 ;
2° l'abonné ou l'utilisateur final ait donné son consentement après avoir été informé conformément aux dispositions visées au point 1°.
L'alinéa 1er n'est pas d'application pour l'enregistrement technique des informations ou de l'accès aux informations stockées dans les équipements terminaux d'un abonné ou d'un utilisateur final ayant pour seul but de réaliser l'envoi d'une communication via un réseau de communications électroniques ou de fournir un service demandé expressément par l'abonné ou l'utilisateur final lorsque c'est strictement nécessaire à cet effet.
Le consentement au sens de l'alinéa 1er ou l'application de l'alinéa 2, n'exempte pas le responsable du traitement des obligations de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui ne sont pas imposées par le présent article.
Le responsable du traitement donne gratuitement la possibilité aux abonnés ou utilisateurs finals de retirer le consentement de manière simple. »

La Commission irlandaise de protection des données a déclaré à ce sujet :

« Les cookies ne nécessitent pas tous un consentement pour pouvoir être utilisés. Il s'agit de cookies qui sont essentiels à la fourniture d'un service demandé par l'utilisateur – cookies de session, cookies d'authentification (pendant la durée de la session) et cookies servant à protéger l'utilisateur. Par exemple, le stockage d'articles dans un panier sur un site de vente en ligne ne requerra pas de consentement préalable. En général, ce sera le cas lorsque le cookie n'est enregistré que pour la durée de la session et est supprimé en fin de session. »

Le cookie « Datr » incriminé, qui ne disparaît pas à la fin de la session mais reste stocké pendant encore 2 ans dans les dossiers utilisés par le navigateur, ne répond pas à cette définition et est manifestement soumis aux règles des articles 4 et 5 de la loi relative à la protection de la vie privée ainsi que de l'article 129 de la loi relative aux communications électroniques.

À l'audience consacrée aux plaidoyers, il a été abondamment question de la bannière que Facebook fait depuis peu apparaître sur sa page d'accueil et qui apparaît manifestement toujours lorsqu'un utilisateur n'a encore jamais visité une page du domaine facebook.com. Cette bannière se compose du texte : « 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. ».

En cliquant sur le lien hypertexte associé aux mots « Politique d'utilisation des cookies », on accède à une page intitulée « Cookies, pixels et technologies similaires », laquelle fournit des explications relativement détaillées concernant les cookies. Toutefois, le cookie « Datr » n'y est pas explicitement nommé.

Apparemment, le cookie « Datr » n'est pas encore enregistré à ce moment, mais l'est au moment où l'utilisateur non inscrit clique sur un autre élément de cette page, par exemple sur les liens hypertextes « Services Facebook » ou « Déclaration des droits et responsabilités ».

De même, le cookie « Datr » ne serait pas enregistré lorsqu'un utilisateur non inscrit clique, consciemment ou non, sur un plug-in social de Facebook se trouvant sur une page web extérieure au domaine Facebook. En revanche, lorsque l'utilisateur clique sur « Annuler » pour quitter le plug-in social, le cookie « Datr » est apparemment enregistré.

De l'avis du siège, Facebook ne peut pas assimiler ces actes avec le fait de donner un consentement éclairé. Dans le premier cas, l'utilisateur est en effet encore en train de s'informer et le fait d'approfondir les informations proposées ne peut pas être assimilé à une utilisation des services Facebook. Dans le deuxième cas, ce même utilisateur non inscrit indique en quittant le plug-in qu'il ne souhaite justement pas faire usage du service proposé.

Le siège est également d'avis que Facebook ne dispose pas du consentement éclairé et indubitable de l'utilisateur lorsqu'il s'agit de consulter un cookie « Datr » enregistré précédemment dans le navigateur d'un utilisateur non inscrit. En vertu de l'article 129 de la loi relative aux communications électroniques, le responsable du traitement doit en effet avoir le consentement de l'utilisateur à la fois pour le stockage d'informations et pour l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un utilisateur.

Au surplus, on ne peut pas qualifier un non-utilisateur ayant un jour ou l'autre visité le domaine facebook.com (et sur l'ordinateur de qui le cookie « Datr » a par conséquent été enregistré) d'« utilisateur », au sens de l'article 129 de la loi relative aux communications électroniques, qui demanderait explicitement un service Facebook chaque fois qu'il visite un site web de tiers sur lequel un plug-in social a été implémenté.

De l'avis du siège, on ne peut en effet pas considérer comme des « utilisateurs » des services Facebook des personnes qui ne disposent pas d'un compte Facebook mais qui ont un jour ou l'autre visité une page du domaine Facebook, ne serait-ce que parce que l'on peut aussi accéder tout à fait involontairement à la page Facebook d'un individu ou d'une organisation, par exemple en suivant un lien se trouvant sur une page web extérieure au domaine Facebook sans savoir que ce lien réfère à une page Facebook.

Le siège adhère en effet au point de vue de la Commission de la protection de la vie privée lorsque celle-ci affirme que rien ne prouve que les personnes qui visitent à l'occasion une page web du domaine facebook.com aient marqué leur accord sur les conditions d'utilisation de Facebook vers lesquelles pointe un lien se trouvant sur cette page, et donc aient consenti à ce que le cookie « Datr » soit enregistré sur leur disque dur. On ne peut que faire dans ce dossier une distinction entre d'une part les internautes disposant d'un compte Facebook, et d'autre part ceux qui n'en disposent pas mais qui visitent occasionnellement une page web du domaine facebook.com. Pour les premiers, on peut supposer qu'ils aient donné, au moins implicitement mais en tout cas indubitablement, leur consentement en vue de l'enregistrement et de la consultation ultérieure du cookie « Datr », mais pour les seconds, les défenderesses doivent le prouver. Or, il a été considéré plus haut que l'obtention de ce consentement n'a pas été prouvée.

Étant donné que les données à caractère personnel des utilisateurs non inscrits, en particulier en cas d'utilisation irréfléchie de la bannière ou du plug-in social, sont déjà traitées avant même que l'utilisateur non inscrit n'ait pu s'informer de manière exhaustive – voire alors qu'il ne souhaite pas faire usage du plug-in social ou, plus généralement, des services Facebook –, ces données ne font manifestement pas l'objet d'un traitement équitable et légitime. Elles ne sont en outre pas obtenues pour des finalités déterminées, explicites et légitimes, et sont traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables.

Il s'agit là d'une violation manifeste de l'article 4, 1° et 2° de la loi relative à la protection de la vie privée.

Enfin, le rôle de première partie que Facebook remplit le cas échéant dans le cadre de l'enregistrement du cookie « Datr » n'est plus présent lorsqu'elle collecte par la suite le cookie par le biais de plug-ins sociaux intégrés sur des sites web extérieurs au domaine Facebook, puisqu'elle agit alors en qualité de tierce partie dans le cadre du parcours de navigation de l'utilisateur non inscrit. En sa qualité de tierce partie, elle est en effet à ce moment uniquement en relation avec le propriétaire ou le designer du site web visité, et non avec le visiteur de cette page, lequel ne recourt pas explicitement aux services dudit tiers.

La prétendue extension du consentement déjà bancal de l'utilisateur non inscrit engendre apparemment elle aussi un traitement inéquitable et illégitime des données à caractère personnel, ne tenant de surcroît pas compte des attentes raisonnables de l'utilisateur non inscrit, ce qui semble constituer une nouvelle violation de l'article 4, 1° et 2° de la loi relative à la protection de la vie privée.

À présent qu'il est clair que les défenderesses ne peuvent manifestement pas invoquer le consentement éclairé et indubitable des visiteurs non inscrit pour légitimer le traitement contesté des données à caractère personnel, il y a lieu d'examiner si elles peuvent invoquer les autres motifs d'admissibilité de l'article 5 de la loi relative à la protection de la vie privée.

Dès lors que les défenderesses n'ont pas de contrat avec un utilisateur se trouvant sur le territoire belge mais ne s'étant jamais inscrit sur Facebook, et n'ayant en outre aucunement marqué son accord sur les conditions d'utilisation de Facebook, elles ne peuvent en aucun cas invoquer une quelconque nécessité du traitement contesté en vue de 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.

En vertu de l'article 16, §4 de la loi relative à la protection de la vie privée, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent, afin de garantir la sécurité des données à caractère personnel, prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.
Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
Sur avis de la Commission de la protection de la vie privée, le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements.

Cela ne signifie pourtant pas que le traitement contesté des données à caractère personnel soit nécessaire pour permettre aux défenderesses de respecter une obligation dont le responsable du traitement est investi par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Il y a en effet lieu de vérifier d'abord si un motif d'admissibilité de l'article 5 peut être invoqué. Dans la négative, le traitement des données à caractère personnel n'est pas autorisé. Or, ce n'est que lorsque le traitement des données à caractère personnel est autorisé que naît l'obligation de prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Le fait de disposer d'un motif d'admissibilité est une obligation fondamentale autonome à l'égard des autres obligations découlant de la loi relative à la protection de la vie privée. Les obligations légales au sens de l'article 5, c de la loi relative à la protection de la vie privée ne désignent donc naturellement que des obligations stipulées dans d'autres lois que la loi relative à la protection de la vie privée elle-même, par exemple des obligations découlant de la législation du travail et de la sécurité sociale.

En juger autrement reviendrait à adopter un raisonnement en boucle qui impliquerait que n'importe quelles données à caractère personnel peuvent être traitées en toute circonstance, ce qui viderait entièrement de son sens la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

En effet, étant donné que l'on est toujours dans l'obligation de préserver l'intégrité des données à caractère personnel traitées, on pourrait toujours invoquer l'admissibilité du traitement, et il n'y aurait donc de cette manière jamais lieu de s'abstenir d'un traitement de données à caractère personnel.

On verrait ainsi apparaître une situation complètement absurde dans laquelle les utilisateurs de Facebook doivent indubitablement consentir au traitement de leurs données à caractère personnel, tandis que les non-utilisateurs – sans avoir donné aucun consentement – devraient tolérer que leurs données à caractère personnel soient traitées pour protéger les données à caractère personnel d'autres individus. Cette situation n'est évidemment pas acceptable : tout intéressé doit avoir la possibilité de consentir lui-même au traitement de ses données à caractère personnel.

Par ailleurs, les mesures prises elles-mêmes ne peuvent pas aller à l'encontre des exigences de qualité imposées par l'article 4 de la loi relative à la protection de la vie privée vu que cela les priverait de tout caractère approprié. Vu le caractère totalement abusif des traitements litigieux, les mesures prises n'ont aucun « caractère approprié ». Dès lors, l'article 16, §4 de la loi relative à la protection de la vie privée ne peut en aucun cas servir de motif de légitimation.

Par ailleurs, on ne voit pas en quoi le traitement contesté serait nécessaire à la préservation d'un intérêt vital des utilisateurs non inscrits.

Les défenderesses ne démontrent pas – et n'invoquent même pas – avoir été investies d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

Le sixième et dernier motif d'admissibilité est la nécessité pour la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi.
Le Roi peut, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, préciser les cas où la condition mentionnée sous f) est considérée ne pas être remplie.

Il est peu vraisemblable que la consultation du cookie « Datr », chaque fois qu'un plug-in social est chargé sur un site web visité par un non-utilisateur, soit réellement nécessaire à la sécurité des services Facebook.

Les défenderesses affirment que le cookie « Datr » aide en cas d'attaques à l'encontre de la plateforme Facebook, en particulier lorsqu'il s'agit de tentatives d'accès frauduleux. On peut supposer que c'est dans une certaine mesure le cas lorsqu'un contact est établi avec une page Facebook, mais dans la situation dont il est question ici, les non-utilisateurs ne souhaitent pas établir de connexion avec la plateforme Facebook, mais veulent seulement visiter un tout autre site web. Les défenderesses ne rendent pas plausible l'hypothèse selon laquelle une attaque pourrait être perpétrée contre la plateforme Facebook par le biais de plug-ins qui ne sont pas effectivement utilisés par les utilisateurs accédant à une page extérieure au domaine Facebook.

Même une personne totalement ignorante de la technologie numérique comprendra que la collecte systématique du cookie « Datr » est en soi insuffisante pour contrer les attaques évoquées par Facebook, étant donné que les criminels peuvent très aisément contourner l'enregistrement de ce cookie en utilisant des logiciels qui bloquent l'enregistrement des cookies. Pour un pirate potentiel disposant des connaissances IT que suppose la mise en place d'une telle attaque, il doit être un jeu d'enfant de bloquer tout simplement les cookies ou de les supprimer avant ou pendant le lancement de l'attaque. Le traitement contesté manque ainsi de l'efficacité requise pour la réalisation de la prétendue protection, vu qu'il suffit qu'un seul pirate malveillant sache comment bloquer les cookies pour que cette protection soit réduise à néant, et ce alors que ces connaissances sont étalées sur Internet et sur les pages d'aide.

De plus, il semble qu'il existe des méthodes moins invasives pour réaliser la protection visée. Il n'est par exemple pas plausible qu'une attaque DDoS, qui passe par des milliers voire des dizaines de milliers d'ordinateurs infectés à travers le monde, ayant chacun leur cookie propre contenant un *« unique identifier »* – ou en étant dépourvu parce que le code utilisé le bloque ou le supprime – pourrait être empêchée par la simple collecte des cookies « Datr » des systèmes infectés.
Un géant informatique comme Facebook dispose assurément de méthodes de sécurisation plus efficaces, de sorte que le traitement contesté échoue également au contrôle de proportionnalité.

Vu le grand nombre de sites web recourant à un plug-in social de Facebook, la collecte des données à caractère personnel de non-utilisateurs par le biais de plug-ins sociaux permet incontestablement d'exposer et d'enregistrer une partie significative du comportement de navigation des utilisateurs de Facebook. De ce fait, cette mesure a un impact substantiel sur le droit fondamental au respect de la vie privée et à la protection des données à caractère personnel, d'autant qu'un géant de l'internet comme Facebook se trouve dans une position de force par rapport à un non-utilisateur individuel.

La mise en balance provisoire de l'intérêt de Facebook contre les droits fondamentaux des non-utilisateurs concernés penche incontestablement en faveur des non-utilisateurs, dès lors que les traitements litigieux sont clairement disproportionnés vu la finalité indiquée et l'échelle à laquelle les traitements sont effectués, et dès lors qu'il ne s'agit pas de traitements équitables et légitimes.

Ce fait constitue manifestement aussi une violation de l'article 4, 2° et 3° de la loi relative à la protection de la vie privée, qui dispose que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. Les données à caractère personnel doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

3.6 La mesure demandée :

L'article 39, 1° et 2° de la loi relative à la protection de la vie privée détermine les sanctions pouvant être infligées au responsable du traitement, son représentant en Belgique, son préposé ou mandataire qui traite des données à caractère personnel en infraction aux conditions imposées par l'article 4, §1er, ainsi qu'au responsable du traitement, son représentant en Belgique, son préposé ou mandataire qui traite des données en dehors des cas prévus à l'article 5.

Les obligations imposées par les articles 4, §1er et 5 de la loi relative à la protection de la vie privée touchent par conséquent à l'ordre public belge, de sorte que la demande du Président de la Commission de la protection de la vie privée ne viole pas le principe de proportionnalité ni le principe de non-discrimination, tandis qu'il n'y a pas lieu non plus de mettre en balance les intérêts.

La demande ne vise pas à entendre prononcer une interdiction de l'établissement d'un profil à des fins publicitaires, mais bien à obliger les défenderesses à respecter les obligations qui leur incombent en leur qualité de responsable du traitement dans le cadre de la collecte du cookie « Datr » auprès de non-utilisateurs par le biais de plug-ins sociaux placés sur des sites web de tiers – y compris bien entendu l'obligation pour les défenderesses de mettre elles-mêmes un terme à la violation du principe de proportionnalité.

De plus, il s'agit de violations massives : il n'est pas question de la violation du droit fondamental d'un seul individu, mais bien d'un énorme groupe d'individus. Il existe en effet en Belgique un nombre incalculable d'internautes qui n'ont pas de compte Facebook mais qui ont un jour ou l'autre visité une page web du domaine facebook.com, et dont l'ordinateur aurait par conséquent enregistré à leur insu le cookie « Datr » de Facebook. Vu les millions de sites web dotés des plug-ins sociaux de Facebook, il est pour ainsi dire impossible d'y échapper. Il s'agit également souvent d'informations très sensibles concernant notamment la santé ou les préférences religieuses, sexuelles ou politiques.

Le fait que les défenderesses collectent des données sur le comportement de navigation de millions de résidents belges ayant décidé de ne pas devenir membres du réseau social de Facebook constitue, peu importe l'usage qu'elles font de ces données, une violation manifeste de la législation en matière de protection de la vie privée.

Vu que la violation des articles 4, §1er et 5 de la loi relative à la protection de la vie privée touche à l'ordre public belge, la mesure demandée n'est aucunement disproportionnée.

Il est totalement invraisemblable que la mesure ne pourrait pas être exécutée en Belgique. À cet égard, l'affirmation selon laquelle la structure organisationnelle interne et sociétale du groupe Facebook nécessiterait que les éventuelles implémentations techniques soient réalisées à l'étranger n'est absolument pas pertinente. Pour Facebook, il est du reste aisé de limiter la mise en œuvre des mesures provisoires au territoire belge étant donné qu'elle peut le cas échéant la limiter aux adresses IP belges.

La mesure demandée doit non seulement être imposée à FACEBOOK INC., mais aussi à FACEBOOK IRELAND LIMITED et à la SPRL FACEBOOK BELGIUM. Non seulement, il a déjà été évalué plus haut que

les activités de FACEBOOK BELGIUM étaient indissociablement liées aux activités de l'exploitant du réseau social, mais par ailleurs les sanctions visées à l'article 39, 1° et 2° de la loi relative à la protection de la vie privée s'appliquent tant au responsable du traitement qu'à son représentant en Belgique, son préposé ou mandataire qui traite des données à caractère personnel. Étant donné que les défenderesses affirment elles-mêmes que Facebook Ireland met le service à la disposition des utilisateurs de l'U.E., cette société doit également respecter la mesure à imposer.

Dans ce dossier, l'approbation de la mesure demandée ne peut que s'accompagner de l'imposition d'une astreinte afin d'exercer sur les défenderesses la pression nécessaire pour qu'elles respectent la mesure. Dans la détermination du montant de l'astreinte, le juge devra principalement tenir compte de la capacité financière de la condamnée et de la résistance à laquelle on peut s'attendre de sa part à l'encontre de l'exécution de la condamnation (voir notamment K. WAGNER, « Dwangsom 2003-2009 » dans : Vlaamse Conferentie bij de Balie te Antwerpen (éd.), Meester van het proces. Topics gerechtelijk recht, Gand, Larcier, 2010, (I) 7).

De même, le fait que le groupe Facebook se compose dans une large mesure de sociétés étrangères n'empêche aucunement d'imposer aux défenderesses une astreinte en Belgique.

Vu que le groupe Facebook a incontestablement réalisé un chiffre d'affaires de 12,4 milliards de dollars et un bénéfice de 2,9 milliards de dollars et est l'une des entreprises les plus puissantes au monde du point de vue financier, l'astreinte demandée de 250.000 EUR par jour de non-respect de la mesure à ordonner paraît adéquate pour être suffisamment dissuasive. Il peut être accordé aux défenderesses un délai raisonnable de 48 heures pour implémenter la mesure à ordonner, partant du principe qu'elles disposent d'assez de personnel juridique, lui-même suffisamment assisté par une équipe d'avocats spécialisés, pour savoir qu'elle devait prendre au moins les mesures nécessaires pour préparer ladite implémentation pendant la mise en état et les délibérations de la présente procédure.

Les mesures demandées apparaissent fondées dans la mesure déterminée dans le dispositif de la présente ordonnance et peuvent par conséquent être ordonnées comme ci-après.

3.7 Caractère exécutoire

Le siège rappelle que la présente ordonnance est exécutoire par provision, de plein droit et sans offre de cantonnement (art. 1039 du Code judiciaire).

PAR CES MOTIFS :

Monsieur W. Thiery, juge, désigné aux fins de remplacer le président du Tribunal de première instance néerlandophone séant à Bruxelles, assisté par Madame C.KINT, greffière ;

Vu la loi du 15 juin 1935 concernant l'emploi des langues en matière judiciaire ;

Disant droit provisoirement et contradictoirement ;

Rejetant toutes autres conclusions contraires ;

Déclare la demande recevable et fondée dans la mesure suivante :

Ordonne aux défenderesses, la société de droit de l'État du Delaware (États-Unis d'Amérique) FACEBOOK Inc., la SPRL FACEBOOK BELGIUM et la société de droit irlandais FACEBOOK IRELAND LIMITED, à renoncer, dans les 48 heures de la signification de la présente ordonnance, à l'égard de tout internaute se trouvant sur le territoire belge et ne s'étant pas inscrit en tant que membre du réseau social en ligne de Facebook :

- à l'enregistrement d'un cookie « Datr » lorsque lesdits internautes visitent une page web du domaine facebook.com, sans les informer suffisamment et adéquatement au préalable du fait que Facebook enregistre le cookie « Datr » sur leurs systèmes ainsi que de l'usage que Facebook fait de ce cookie « Datr » par le biais des plug-ins sociaux ;
- à la collecte des cookies « Datr » par le biais de plug-ins sociaux placés sur des sites web de tiers ;

Condamne les défenderesses, la société de droit de l'État du Delaware (États-Unis d'Amérique) FACEBOOK INC., la SPRL FACEBOOK BELGIUM et la société de droit irlandais FACEBOOK IRELAND LIMITED, à payer au demandeur, Monsieur WILLEM DEBEUCKELAERE, agissant conformément à l'article 32, §3 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel en sa qualité de PRÉSIDENT DE LA COMMISSION BELGE DE LA PROTECTION DE LA VIE PRIVÉE, une astreinte de 250.000 EUR par période entamée de 24 heures au cours de laquelle cet ordre ne serait pas respecté ;

Rejette le surplus des demandes ;

Condamne en outre les défenderesses, la société de droit de l'État du Delaware (États-Unis d'Amérique) FACEBOOK Inc., la SPRL FACEBOOK BELGIUM et la société de droit irlandais FACEBOOK IRELAND LIMITED, aux dépens de la procédure, estimés dans le chef de Monsieur WILLEM DEBEUCKELAERE, agissant en sa qualité de PRÉSIDENT DE LA COMMISSION BELGE DE LA PROTECTION DE LA VIE PRIVÉE, à 459,99 € de frais de citation et 1.320,- € d'indemnité de procédure ;

Déclare la présente ordonnance exécutoire par provision, nonobstant tout recours et sans caution ni offre de cantonnement.

Ainsi rendu et prononcé à l'audience publique en référé du 9 novembre 2015.

[signature]
C. KINT

[signature]
W. THIERY