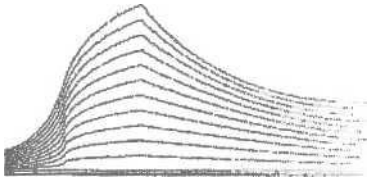

COPIE

(libre : art. 260,2°C.enreg.)

(C.pén., art 792-1090)

Numéro de la chambre 53
Numéro de répertoire 2018/
Date du prononcé Le 16 février 2018
Numéro de rôle 2016/153/A

Ne pas soumettre au receveur

Jugement définitif

TRIBUNAL DE PREMIÈRE INSTANCE NÉERLANDOPHONE DE BRUXELLES

JUGEMENT

24e CHAMBRE

Affaires civiles

Présenté le
N'est pas soumis à l'enregistrement

EN LA CAUSE DE :

1. Monsieur **WILLEM DEBEUCKELAERE, agissant en sa qualité de PRÉSIDENT DE LA COMMISSION BELGE DE LA PROTECTION DE LA VIE PRIVÉE**, numéro d'entreprise 0893.076.921, sise à 1000 Bruxelles, Rue de la Presse 35, où il fait élection de domicile,

Partie demanderesse,

Représentée par maître Frederic Debusseré et maître Ruben Roex, agissant tous deux en leur nom propre et loco Maître Jos Dumortier, avocats ayant leur cabinet à 1000 Bruxelles, Rue Joseph Stevens 7,

CONTRE :

1. **FACEBOOK IRELAND LIMITED**, société étrangère de droit irlandais, ayant son siège social à Dublin 2,216410 (Irlande), Grand Canal Square 4, Grand Canal Harbour, numéro d'entreprise 462932,

Première défenderesse,

Dénommée ci-après « Facebook Ireland » ou « première défenderesse »,

Représentée par maître Paul Lefebvre, avocat ayant son cabinet à 1050 Bruxelles, Avenue Louise 480,

2. **FACEBOOK, INC**., société étrangère de droit de l'État du Delaware (États-Unis d'Amérique), dont le siège est établi à CA 94025 Menlo Park (États-Unis d'Amérique), Willow Road 1601,

Deuxième défenderesse,

Dénommée ci-après « Facebook Inc. » ou « deuxième défenderesse »,

Représentée par maître Dirk Van Liedekerke, avocat ayant son cabinet à 1170 Bruxelles, Chaussée de la Hulpe 178,

3. **FACEBOOK BELGIUM SPRL**, société de droit belge dont le siège est établi à 1040 Bruxelles, Rond-point Robert Schuman 11, numéro d'entreprise 0836.948.464,

Troisième défenderesse,

Dénommée ci-après « Facebook Belgium » ou « troisième défenderesse »,

Représentée par maître Dirk Lindemans, agissant en son nom propre et loco maître Henriette Tielemans, avocats ayant respectivement leur cabinet à 1000 Bruxelles, Boulevard de l'Empereur 3 et 1040 Bruxelles, Avenue des Arts 44,

Les trois défenderesses étant également dénommées conjointement ci-après les « défenderesses »

EN LA PRÉSENCE DE :

La **COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE**, établie à 1000 Bruxelles, Rue de la Presse 35, numéro d'entreprise 0893.076.921, représentée par son président, monsieur Willem DEBEUCKELAERE,

Partie en intervention volontaire,

Représentée par maîtres Frederic Debusseré et Ruben Roex, tous deux intervenant en leur nom propre et loco Maître Jos Dumortier, avocats ayant leur cabinet à 1000 Bruxelles, Rue Joseph Stevens 7,

* * *

I. PROCÉDURE

1.

Le tribunal a pris connaissance du jugement interlocutoire du tribunal de céans du 02.11.2017 et des pièces de procédure qui y sont mentionnées.

Dans ledit jugement interlocutoire, le tribunal a ordonné la réouverture de plein droit des débats à l'audience du 01.12.2017, pour permettre à la partie la plus diligente de déposer le texte complet de l'arrêt de la Cour d'appel de Bruxelles, 18e chambre néerlandophone, affaires civiles, rendu le 29.06.2016, en la cause portant le numéro de rôle 2016/KR/2, numéro de répertoire 2016/5747.

Les parties ont déposé les pièces demandées à l'audience du 01.12.2017. La cause a ensuite été reprise en délibération.

La procédure s'est déroulée dans le respect des dispositions applicables de la loi du 15 juin 1935 relative à l'emploi des langues en matière judiciaire et des lois modifiant et complétant ladite loi.

II. FAITS ET RÉTROACTES

2.

Le service en ligne Facebook est un site de réseau social mondial gratuit, qui tire une grande partie de ses revenus de la réclame / publicité, plus spécifiquement de la publicité ciblée en ligne, c'est-à-dire ciblée sur les caractéristiques personnelles, les intérêts et les comportements des utilisateurs individuels d'Internet.

Le demandeur est monsieur Willem Debeuckelaere, en sa qualité de président de la Commission belge de la protection de la vie privée (ci-après la « Commission vie privée »). La Commission vie privée est intervenue volontairement en la présente procédure. À des

fins de facilité, le tribunal dénommera ci-après conjointement ces deux parties au procès « la Commission vie privée », sauf s'il s'avérait nécessaire de les nommer séparément.

Par la présente procédure, la Commission vie privée veut mettre un terme à ce qu'elle décrit notamment comme une violation grave et à grande échelle, par Facebook, de la législation sur le respect de la vie privée, notamment en collectant et en utilisant quotidiennement et illégalement des informations relatives au comportement de navigation privé de millions d'utilisateurs d'Internet en Belgique par le biais de technologies telles que les « cookies », « social plug-ins » (« modules sociaux ») et « pixels ».

Les demandes ciblent les trois défenderesses conjointement : Facebook Ireland Limited, Facebook, Inc. et la sprl Facebook Belgium.

Facebook Ireland Limited, constituée en 2008, se décrit comme une société irlandaise qui propose le service Facebook dans l'Union européenne et ailleurs (hors Amérique du Nord) conformément aux dispositions de la Déclaration des droits et responsabilités de Facebook (la « DDR »). Elle se décrit également comme étant la seule partie contractuelle des utilisateurs belges et comme la seule responsable du traitement de toutes les données reçues de ressortissants de l'UE, notamment les données visées par la présente procédure.

Facebook, Inc. se décrit comme une société américaine qui propose le service Facebook à des utilisateurs d'Internet aux États-Unis et au Canada.

Facebook Belgium se décrit comme une sprl de droit belge qui ne compte que huit travailleurs et dont la société mère directe est « Facebook Global Holdings LLC », constituée pour apporter de l'aide en matière de politique publique (« public policy ») dans le cadre du service Facebook.

3.

Préalablement à la présente procédure, la Commission vie privée a déjà intenté à l'encontre des défenderesses une procédure en référé devant le tribunal de céans, introduite par la citation signifiée le 10.06.2015.

La Commission vie privée affirme qu'à la suite de l'introduction de la nouvelle politique d'utilisation des données et des cookies de Facebook, le 30.01.2015, elle a été interpellée à plusieurs reprises, tant par des utilisateurs de Facebook inquiets que par les médias, le parlement fédéral et le Secrétaire d'État à la vie privée, raison pour laquelle elle a décidé d'examiner ces nouvelles conditions d'utilisation et d'en examiner les modifications au regard de la législation belge en matière de respect de la vie privée.

Pour ce faire, elle a également fait appel à l'expertise technique des chercheurs de la Katholieke Universiteit Leuven et de la Vrije Universiteit Brussel (respectivement l'Université catholique flamande de Louvain et l'Université libre flamande de Bruxelles) qui, dans le cadre de leur travail, avaient déjà mené des recherches approfondies sur Facebook. Le 31.03.2015, ils ont publié la version la plus récente de leur rapport d'étude : « From social media service to advertising network. A critical analysis of Facebooks Revised Policies and Terms » (traduction libre : « D'un service de média social à un réseau publicitaire. Une analyse critique de la nouvelle politique et des nouvelles conditions d'utilisation de Facebook ») sur le site Internet de l'Interdisciplinair Centrum voor Rechten ICT (ICRI) de la KU Leuven.

La Commission vie privée invoque notamment le chapitre 8 du rapport de recherche et l'annexe I audit rapport (à savoir les pièces A.I et A.2), qui décrivent comment Facebook enregistrait à l'époque, par une combinaison de social plug-in et de cookies, les sites web consultés par les internautes et comment Facebook enregistrait également le comportement de recherche des utilisateurs de Facebook[1], mais aussi des personnes qui ne l'utilisent pas, notamment à l'aide des cookies « datr » (un « tracking-cookie » ou cookie de traçage, voir également infra).

Le 13.05.2015, la Commission vie privée a émis la recommandation n° 04/2015 concernant le traitement des données à caractère personnel par le biais des social plug-ins Facebook, visant « 1) Facebook, 2) les utilisateurs d'Internet et/ou Facebook) et 3) les utilisateurs et les fournisseurs de services Facebook, notamment les social plug-ins » (pièce D.2 du demandeur).

Il apparaît, au vu de cette recommandation, qu'une correspondance étendue avait déjà été échangée entre Facebook et la Commission vie privée et que cette dernière avait également entendu Facebook durant une audience du 29.04.2015. Facebook reconnaît exclusivement la compétence de la Commission vie privée irlandaise et elle estime que seul le droit de protection des données national irlandais s'applique à l'ensemble des utilisateurs européens de son réseau social. Facebook argumente en outre que ce n'est pas Facebook, Inc., mais Facebook Ireland Limited qui doit être considérée comme responsable du traitement des données à caractère personnel des utilisateurs européens.

La Commission vie privée a marqué son désaccord sur la position de Facebook auquel elle a notamment ordonné :

- d'appliquer une transparence totale en matière d'utilisation de cookies ;
- de renoncer à l'installation systématique de cookies de longue durée et d'identification unique chez les non-utilisateurs de Facebook, ainsi que de toute collecte et utilisation de données au moyen de cookies et de social plug-ins, sauf si elle reçoit pour ce faire le consentement spécifique et indubitable, par opt-in[2], de la personne concernée et dans la mesure où cela s'avère strictement nécessaire à des finalités légitimes ;
- de renoncer à la collecte et l'utilisation des données des utilisateurs au moyen de cookies et de social plug-ins, sauf si (et uniquement dans la mesure où) c'est strictement nécessaire pour fournir un service expressément demandé par l'utilisateur, ou s'il obtient pour ce faire le consentement indubitable et spécifique, par voie d'opt-in, de la personne concernée ;
- de limiter son offre de possibilités d'intégration de social plug-ins à des variantes respectueuses de la vie privée, conformes aux exigences en matière de protection des données ;
- adapter son interface utilisateur de façon à obtenir le consentement indubitable et spécifique de ses utilisateurs, au moyen d'un opt-in, pour toute collecte et

[1] Les utilisateurs de Facebook peuvent en outre être répartis en (i) les détenteurs de compte Facebook et (ii) les utilisateurs des services Facebook non-inscrits ; voir également infra.

[2] L'opt-in est un système par lequel la personne concernée doit faire quelque chose pour prendre part au règlement, à défaut, un autre règlement est applicable d'office ou il ne se passe rien.

utilisation d'informations obtenues au moyen de cookies, notamment à des fins publicitaires.

La Commission vie privée a remis cette Recommandation à Facebook, Inc. et à la sprl Facebook Belgium. Elle a également mis Facebook en demeure, par un courrier du 18.05.2015, de mettre fin à la violation de la législation belge sur la vie privée pour ce qui est des social plug-ins et des cookies (pièce E.2 demandeur). Le 26.05.2015, l'avocat de Facebook, Inc. et de la sprl Facebook a répondu que les deux sociétés souhaitaient entamer une concertation avec la Commission vie privée.

Sur le principe, la Commission vie privée était disposée à le faire, mais dans la mesure où les parties poursuivaient la discussion sur certains points et que la Commission ne souhaitait pas que les choses traînent en longueur, le 10.06.2015, le demandeur a cité les défenderesses à comparaître devant le président du présent tribunal, siégeant en référé.

4.

Par une ordonnance rendue le 09.11.2015 (pièce C5 du demandeur), le président du présent tribunal, siégeant en référé, a estimé qu'il était compétent (au niveau international) pour connaître du litige, que l'action du demandeur était recevable et il a déclaré l'action en cessation intentée fondée à l'égard de toutes les défenderesses, en ce sens qu'elles ont été obligées :

(traduction libre) « dans les 48 heures qui suivent la signification de la présente ordonnance, envers tous les utilisateurs de l'Internet sur le territoire belge qui ne sont pas inscrits dans le réseau social en ligne de Facebook, cesser :

- *de placer un cookie datr lorsqu'ils aboutissent sur une page du domaine facebook.com, sans les informer préalablement de façon suffisante et adéquate, du fait que Facebook place chez eux le cookie datr et de l'usage que Facebook fait de ce cookie datr au moyen de plug-ins sociaux ;*
- *la collecte du cookie datr par le biais de plug-ins sociaux placés sur les sites web de tiers. »*

Par un arrêt du 29.06.2016 (pièce C.8 demandeur), la Cour d'appel de Bruxelles, 18e chambre néerlandaise, a réformé l'ordonnance susmentionnée. La Cour a estimé ne pas être compétente à l'égard des actions intentées à l'encontre de Facebook Ireland Limited et de Facebook Inc., mais qu'elle était toutefois compétente pour connaître de l'action intentée par la Commission vie privée à l'encontre de la sprl Facebook Belgium, mais que cette action était non fondée dans la mesure où elle reposait sur l'art. 584 C. jud., puisqu'il n'y avait pas d'urgence.

Il ressort en outre de cet arrêt que, dans l'intervalle, Facebook avait adapté (en mai 2016) sa politique des cookies et sa « cookie-banner » (bannière cookies) (voir également par exemple pièce E.II du demandeur). Le 31.08.2016, Facebook Ireland annonçait avoir l'intention de remettre sous peu en ligne l'ensemble de ses services destinés aux utilisateurs non-inscrits en Belgique, notamment l'utilisation de tous les cookies et l'accès au contenu de ses pages publiques, étant entendu que la bannière cookies avait été adaptée, mais que l'usage de cookies serait étendu (voir pièce E.12 du demandeur).

Dans son complément à la Recommandation d'initiative n° 03/2017 du 12.04.2017, émise

de sa propre initiative à la suite de la modification de la politique des cookies et aux pratiques modifiées de Facebook (voir également supra), la Commission vie privée a exposé ce qui suit au sujet de ces modifications

« 18. L'ordonnance du Président du tribunal de première instance de Bruxelles a été signifiée à Facebook le 2 décembre 2015. Suite à cette signification, Facebook a décidé de refuser l'accès aux internautes du territoire belge qui ne disposent pas d'un compte Facebook. Lorsqu'un non-utilisateur tentait de visiter une page Internet faisant partie du domaine facebook.com (à l'exception de certaines pages comme la page d'inscription de Facebook), le message suivant s'affichait à l'écran : 'Permission refusée Ce contenu n'est pas disponible pour le moment. Nous avons mis en place des fonctions de sécurité supplémentaires qui nécessitent que vous vous connectiez à Facebook pour voir cette page en Belgique. <Pourquoi ?>'

Le visiteur qui cliquait sur "Pourquoi" accédait aux informations suivantes : 'Pourquoi mon expérience sur Facebook a-t-elle changé en Belgique ? La sécurité de votre compte nous tient à cœur. Au fil des années, nous avons mis en place un certain nombre d'outils de sécurité sophistiqués qui visent à protéger votre compte sans interrompre votre navigation sur Facebook. En raison des exigences imposées par la Commission belge de la vie privée, nous avons récemment dû limiter notre utilisation d'un outil de sécurité important, le cookie « datr ». Nous vous invitons à lire ce qui suit pour comprendre le fonctionnement de cet outil et les raisons pour lesquelles nous ne présentons plus les Pages publiques Facebook et d'autres contenus en Belgique aux personnes qui ne possèdent pas de compte Facebook. Qu'est-ce que le cookie « datr » et comment permet-il d'assurer la sécurité sur Facebook ? Ce cookie est un outil de sécurité que nous utilisons depuis plus cinq ans déjà dans le monde entier pour nous aider à faire la distinction entre les visites légitimes de Facebook par de véritables personnes et les visites illégitimes (par des spammeurs, des hackers qui tentent d'accéder au compte d'autres personnes ou par d'autres personnes malintentionnées). Ce cookie peut nous aider à sécuriser Facebook en communiquant des informations statistiques sur les activités d'un navigateur Internet, telles que le volume et la fréquence de requêtes. Nos systèmes de sécurisation analysent ces données de navigateur pour nous aider à faire la distinction entre les personnes qui se connectent simplement à leur compte et les attaques potentielles. Si le cookie « datr » indique par exemple qu'un navigateur a visité plusieurs pages sur Facebook en très peu de temps, cela signifie que le navigateur est probablement utilisé par un logiciel automatisé, un "bot" pour effectuer une opération illégitime, comme le vol du contenu de pages. Si le cookie « datr » indique des schémas de visite normaux pendant plusieurs jours, nos systèmes en déduisent que le navigateur est utilisé par une personne normale qui doit simplement accéder à Facebook. Le cookie nous aide à préserver la sécurité du site de différentes manières. Nous utilisons par exemple ce cookie pour :

- *éviter que des hackers créent de faux comptes afin d'envoyer du spam avec ceux-ci ;*
- *limiter le risque que quelqu'un d'autre prenne possession de votre compte ;*
- *protéger du vol vos photos, messages et d'autres contenus ;*
- *empêcher des attaques techniques qui peuvent rendre votre site Internet inaccessible pour vous et pour des tiers et pour éviter de futures attaques ;*
- *vous aider à vous connecter plus rapidement, afin que vous puissiez atteindre les personnes, photos et messages auxquels vous tenez, sans courir de risque au niveau des informations.*

Pour les personnes qui ne disposent pas d'un compte, nous enregistrons et ne conservons que pendant dix jours les informations du cookie datr » que nous recevons d'autres sites. Ces dix jours donnent à nos systèmes le temps nécessaire pour analyser les données et contribuent à la protection contre les actions nuisibles décrites ci-avant. Presque tous les sites utilisent des cookies. Les 25 sites Internet belges les plus visités utilisent tous des cookies lorsqu'on les visite. Ces sites Internet utilisent les cookies à des fins statistiques et pour bien d'autres raisons encore. La majorité de ces sites Internet ne communiquent pas au sujet de leurs pratiques en matière de cookies à l'aide d'un message clair en haut de leur site. Facebook prévoit par contre une telle mention et nous expliquons également comment nous utilisons les cookies (comme le cookie « datr ») à des fins de sécurité dans notre politique d'utilisation des cookies. La Commission vie privée belge nous a toutefois contraints de mettre fin à l'utilisation du cookie « datr » lorsque des internautes ne disposant pas d'un compte Facebook visitent Facebook en Belgique. Du fait que nous ne pouvons pas utiliser cet outil d'aide, nous devons considérer toute visite de notre service via un navigateur non reconnu en Belgique comme danger potentiel et prendre des mesures supplémentaires pour contribuer à votre sécurité et à celles des autres sur Facebook. Pour la protection des comptes de personnes et de nos services, nous devons obliger aussi les personnes qui ne disposent pas d'un compte Facebook à se connecter pour afficher le contenu de pages publiques et d'autres contenus qui sont disponibles pour tous sur Internet en dehors de la Belgique (où nous pouvons bien utiliser le cookie datr). Nous comprenons que ces mesures peuvent malheureusement limiter et perturber votre .expérience sur Facebook Nous vous remercions de nous aider à continuer à offrir une expérience sûre sur Facebook à notre communauté belge. »

Par courrier du 9 décembre 2015, Facebook a fait savoir à la Commission qu'elle avait appliqué l'ordonnance intégralement.

(...)

20. Par courrier du 31 mars 2016, Facebook a fait savoir qu'elle adapterait de nouveau sa politique d'utilisation des cookies, sa bannière cookie et la procédure technique de ses cookies (notamment le moment auquel elle place des cookies).

21. Une des principales modifications de la politique d'utilisation des cookies de Facebook concerne les non-utilisateurs de Facebook. Désormais, Facebook utiliserait des informations sur le comportement de navigation tant des utilisateurs que des non-utilisateurs pour procéder à un profilage à des fins publicitaires. Les utilisateurs et non-utilisateurs de Facebook seraient dans cette optique mis sur un pied d'égalité. Facebook a par ailleurs indiqué que la nouvelle politique d'utilisation des cookies serait plus transparente, plus particulièrement en ce qui concerne le nom, le contenu, la finalité et la durée de vie des cookies que Facebook utilise.

22. Dans son courrier du 31 mars 2016, Facebook a également fait comprendre qu'elle adapterait sa « bannière cookie » conformément aux changements apportés au contenu de sa politique d'utilisation des cookies La bannière cookie reprendrait désormais le texte suivant : 'Nous utilisons des cookies pour aider à personnaliser le contenu, ajuster et mesurer les publicités sur mesure et vous offrir une expérience plus sûre. En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations sur et en dehors de Facebook via les cookies. Pour plus d'informations, y compris sur le contrôle que vous pouvez exercer à cet égard . <politique d'utilisation des cookies>'.

23. En ce qui concerne le placement de cookies, Facebook avait indiqué que certaines actions ne donneraient plus lieu au placement de cookies. Par exemple, le changement de la langue du site ne serait plus considéré par Facebook comme un "consentement" de la part de l'utilisateur.

24. Facebook a introduit sa nouvelle bannière cookie et sa nouvelle politique en mai 2016. Pour les non-utilisateurs de Facebook en Belgique, les pages web publiques de Facebook sont restées inaccessibles jusqu'en novembre 2016. La nouvelle bannière cookie et la nouvelle politique étaient toutefois déjà introduites dans les autres pays européens.

5.

Dans l'intervalle, le demandeur actuel avait introduit la présente procédure au fond par un exploit d'huissier signifié le 11.09.2015.

Dans la présente procédure, la Commission vie privée vise toujours la façon dont Facebook suit le comportement de navigation des utilisateurs Internet, tant des personnes qui disposent d'un compte Facebook que des utilisateurs non inscrits des services Facebook que des non-utilisateurs, au moyen des « social plug-ins », cookies et pixels susmentionnés.

Selon la Commission vie privée, les défenderesses violent toujours la législation en matière de respect de la vie privée, à plusieurs égards et plus gravement encore qu'auparavant.

La Commission vie privée souligne le fait que le référé susmentionné diffère en trois points de la présente procédure au fond :

- le référé portait uniquement sur l'enregistrement par Facebook du comportement de navigation de personnes ne disposant pas d'un compte Facebook, tandis que la présente procédure vise également l'enregistrement du comportement de navigation de personnes disposant d'un compte Facebook ;
- le référé portait uniquement sur l'enregistrement par Facebook du comportement de navigation au moyen de « social plug-ins » et de cookies appelés « datr », tandis que la présente procédure au fond vise également l'enregistrement au moyen d'autres cookies (à savoir les cookies « c_user », « xs », « sb », « fr » et « lu ») et au moyen des « pixels ».

6.

Lorsqu'une page web est créée sur Internet, son propriétaire publie ou présente son propre contenu stocké sur ses serveurs (serveur « First-party » ou « première partie »), mais il n'est pas rare qu'il propose également du contenu d'autres sites web stocké sur les serveurs « tiers » de ces sites web (serveur « third party » ou « tierce partie »).

Quand un utilisateur souhaite consulter une page web (demande http), le navigateur envoie automatiquement certaines informations à chaque serveur « première partie » et « tierce partie » sur lequel le contenu demandé est enregistré. Ces informations sont généralement l'adresse IP utilisée par l'appareil (PC, ordinateur portable, smartphone) pour effectuer la demande, l'URL du site web qui a transmis le lien au site web de la première partie, ainsi que tous les cookies préalablement placés par le site web vers lequel le navigateur a envoyé une demande de contenu (que ce soit la « première partie » ou la « tierce partie »).

Le serveur de la première partie envoie ensuite les informations de la page web vers le navigateur. Ces informations sont notamment, outre le contenu de la page web de la première partie, les instructions pour que le navigateur charge le contenu de la tierce partie choisi pour la page web par le concepteur du site web.

Le navigateur de l'internaute relève ces informations sans aucune intervention ni demande des serveurs de la tierce partie et il envoie une demande http à ces derniers afin d'obtenir le contenu nécessaire pour poursuivre le chargement du site web. Ces demandes http portent généralement sur (1) une adresse IP ; (2) l'URL du site web de la première partie ; (3) le système d'exploitation du navigateur ; (4) le type de navigateur, et (5) les cookies (précédemment) placés par le site web de la tierce partie à partir duquel le navigateur demande le contenu tiers.

Les « social plug-ins » de Facebook sont des composants de site web (des éléments de code logiciel) mis à disposition des concepteurs de sites web externes par Facebook. Il s'agit par exemple du bouton « J'aime » (ou pictogramme de la main dont le pouce est levé) ou du bouton « Partager ». Ces modules sociaux permettent aux utilisateurs de Facebook de partager le contenu d'un site Internet externe par le réseau social. Les sites web externes intégrant un social plug-in placent par conséquent un morceau de code logiciel de Facebook sur leur site. Lorsqu'un utilisateur consulte un site web contenant l'un de ces social plug-ins Facebook, son navigateur établit automatiquement une connexion avec le (il envoie une demande http au) serveur Facebook, après quoi le navigateur de l'internaute charge directement la fonctionnalité du « plug-in » sur le serveur de Facebook. Selon le demandeur, en pratiquant de la sorte, Facebook reçoit automatiquement certaines informations sur les sites web consultés, notamment l'adresse Internet (« URL ») de la page web consultée, l'adresse IP du visiteur et le moment de la consultation.

Les cookies sont de petits fichiers de données envoyés par un serveur web au navigateur du visiteur de ce site et que le navigateur conserve pour l'utiliser ultérieurement. Un cookie peut enregistrer des informations. Généralement, les navigateurs sont conçus de manière à ce que les cookies qui y sont enregistrés soient automatiquement transférés au serveur web qui les a envoyés quand le navigateur envoie de nouvelles demandes http à ce serveur.

La Commission vie privée affirme que le tableau « Browser Cookies », qui peut à présent être consulté au moyen d'un hyperlien contenu dans la politique d'utilisation des cookies de Facebook, montre que Facebook utilise les cookies visés ici, notamment aux finalités suivantes :

- vérifier l'identité des utilisateurs Facebook (cookies « c_user » et « xs ») ; pour des raisons de sécurité, pour l'intégrité du site et des produits, pour restaurer des comptes et identifier les comptes potentiellement piratés (cookie « datr ») et pour vérifier les connexions (cookie « sb ») ;
- diffuser, mesurer et améliorer la pertinence des publicités (cookie « fr ») ;
- enregistrer le choix de l'utilisateur Facebook de rester connecté (cookie « lu »).

Les défenderesses expliquent que Facebook place les cookies « datr » et « sb » (« secure browser » ou navigateur sécurisé) à des fins de sécurité et d'intégrité du site et que, bien qu'à son avis ce ne soit pas nécessaire à strictement parler, elle obtient toujours l'autorisation pour ce faire (par la bannière cookie) de l'internaute qui interagit directement avec le service Facebook. Le cookie « datr » contient des informations identifiant le navigateur d'un internaute de façon unique. Il reste présent sur le disque dur de l'utilisateur

pendant deux ans. Le cookie « sb » contient un « identificateur » de navigateur qui, selon Facebook, est uniquement vérifié lorsqu'un détenteur de compte se connecte. Il permet au service Facebook de vérifier si le détenteur du compte a déjà utilisé précédemment ce navigateur. Toujours selon Facebook, ce cookie est conçu pour faciliter le processus de connexion et d'authentification des détenteurs de comptes en s'assurant que le navigateur est sûr. Le cookie « sb » est placé sur les navigateurs lors de la première connexion d'un détenteur de compte. Sa durée de vie est de deux ans.

Les défenderesses expliquent également que Facebook utilise le cookie « c_user » pour vérifier l'identité des détenteurs de compte, lorsqu'ils se connectent au service Facebook et interagissent avec ce dernier, mais aussi qu'il a une fonction de sécurité. Le cookie « c_user » contient un « identifiant » numérique unique, que le service Facebook relie au détenteur de compte effectif connecté et, selon Facebook, il augmente également la fonctionnalité et l'expérience de l'utilisateur. Facebook décrit le cookie « xs » comme un cookie d'identification complémentaire, qu'elle utilise en lien avec le cookie « c_user », dans le but de vérifier l'authenticité des détenteurs de compte. Ce cookie contient une série de signes alphanumériques qui renvoient notamment à la session « identificateur » et à la valeur d'authentification (attribuée par Facebook à une session spécifique ouverte par un détenteur de compte) offrant des possibilités de recherche et de protection supplémentaires. Selon Facebook, ces deux cookies sont uniquement placés dans le navigateur des détenteurs de compte quand ceux-ci se connectent au service Facebook, ils sont supprimés au moment de la déconnexion ou de la désactivation de leurs comptes Facebook. Si ce n'est pas le cas, leur durée de vie maximale est de 90 jours à compter de la dernière interaction du détenteur de compte avec le service Facebook.

Les défenderesses expliquent en outre que le cookie « lu » est un cookie d'identification complémentaire, qui n'est plus utilisé, car ses fonctionnalités peuvent être entièrement prises en charge par les cookies « c_user » et « xs ». Selon Facebook, les cookies « c_user », « lu » et « xs » ont été et sont tous expressément mentionnés dans la politique d'utilisation des cookies des Services Facebook et les détenteurs de compte donnent explicitement leur consentement au moment où ils décident de s'inscrire auprès des Services Facebook.

Enfin, les défenderesses expliquent que le cookie « fr » est utilisé à des fins publicitaires, de mesure et d'optimisation. Le cookie contient une série de signes alphanumériques attribués (i) au navigateur (pour les utilisateurs non inscrits et les non-utilisateurs) ou (ii) au navigateur et aux ID utilisateurs (les « user ID » ; pour les détenteurs de compte, lorsqu'ils sont connectés), ainsi que d'autres informations qui ne concernent pas l'identification et portent sur l'utilisation et le traitement de ce cookie (par exemple le moment de l'installation du cookie). Le cookie « fr » est utilisé pour envoyer des publicités plus pertinentes en fonction des activités du détenteur de compte ou de l'utilisateur (non-)inscrit (« fondées sur l'intérêt » ou des publicités ciblées en fonction du comportement en ligne). Le cookie « fr » a une durée de vie de 90 jours à compter de la dernière interaction de l'utilisateur (non-)inscrit ou du détenteur de compte avec le service Facebook ou sur un site web d'un tiers contenant un Pixel Facebook et autorisant l'installation de cookies), ou moins si un utilisateur efface les cookies de son navigateur avant le terme de cette période de 90 jours.

Les défenderesses avancent que le cookie « fr » est explicitement mentionné dans la politique d'utilisation des cookies des Services Facebook et que les détenteurs de compte et

les utilisateurs non inscrits donnent également leur consentement explicite par l'intermédiaire de la bannière cookies (les détenteurs de compte également, lorsqu'ils décident de s'inscrire auprès des Services Facebook). Selon Facebook, l'utilisation du cookie « fr » placé lors de la visite de sites web de tiers ayant recours à des pixels Facebook, est subordonnée à la condition que ces tiers fournissent des informations complètes et obtiennent le consentement explicite pour l'installation de cookies Facebook.

Les pixels sont des éléments de code logiciel placés sur une page web à l'intention des exploitants de sites web externes, qui permettent la collecte par ces exploitants d'information sur leur public. Contrairement aux « social plug-ins », un pixel est un point invisible à l'œil nu. Ce pixel Facebook établit automatiquement une connexion entre le navigateur Internet d'un internaute et les serveurs de Facebook au moment où l'internaute charge une page Internet sur laquelle ce pixel se trouve. Selon le demandeur, les propriétaires de sites web peuvent demander à Facebook d'utiliser les informations collectées à l'aide de pixels à des fins publicitaires (par exemple pour montrer ultérieurement, sur Facebook, aux visiteurs de leur site web des publicités ciblées) ou pour obtenir des « statistiques de groupe-cible ». Selon les défenderesses, les réseaux publicitaires et autres entreprises en ligne utilisent des pixels de façon généralisée et quotidiennement pour les aider à réaliser des mesures et à optimiser les publicités. Ils jouent en outre un rôle très important dans les publicités en ligne. Ils fonctionnent souvent avec des cookies publicitaires et ils enregistrent quand un navigateur déterminé consulte une page spécifique.

7.

La Commission vie privée souligne le fait que le rapport de recherche susmentionné (2015) montre que chaque fois qu'une personne ne détenant pas de compte visitait un site du domaine Facebook.com, Facebook plaçait automatiquement un cookie « datr » sur le disque dur, sans en informer activement l'internaute (Facebook prévoyait uniquement un hyperlien grisé vers sa politique d'utilisation des cookies au bas de chaque page web). Lorsque cet utilisateur consultait ensuite un site web contenant un bouton social plug-in de Facebook, son navigateur établissait généralement une connexion avec le serveur de Facebook dans le but de récupérer le plug-in. En raison de cette connexion, les informations contenues dans le cookie datr (enregistrées sur le disque dur de l'utilisateur) sont envoyées aux serveurs de Facebook.

La Commission vie privée a déjà dénoncé ces pratiques dans la procédure en référé.

En évoquant un rapport technique complémentaire du 24.02.2017, la Commission vie privée affirme à présent que Facebook place des cookies d'identification persistants et uniques, tant chez les utilisateurs (détenteurs de compte) que chez les non-utilisateurs de ses services de réseau social (non détenteurs de compte), lorsqu'ils interagissent avec une page web appartenant au domaine facebook.com et qu'elle place également un cookie de ce type chez les internautes qui consultent un site web contenant un pixel Facebook. Lorsque la personne concernée consulte par la suite un site web contenant un bouton de social plug-in ayant les mêmes conséquences que celles décrites ci-avant : les informations des cookies Facebook enregistrées sur le disque dur de l'internaute sont envoyées aux serveurs Facebook qui savent que cet internaute spécifique a navigué sur un site web spécifique sur lequel se trouve le bouton social plug-in.

En résumé, la Commission vie privée reproche à Facebook d'utiliser les technologies mentionnées ci-dessus pour :

- regarder par-dessus l'épaule des personnes pendant qu'elles naviguent d'un site web à l'autre et utiliser ensuite les informations collectées pour profiler le comportement de navigation et, sur cette base, leur montrer des publicités ciblées, sans informer suffisamment les personnes concernées, ni obtenir leur consentement valable ;
- appliquer ces pratiques, que la personne concernée se soit inscrite ou pas sur le réseau social Facebook.

Comme indiqué précédemment, le 12.04.2017, la Commission vie privée a émis une Recommandation d'initiative complémentaire n° 03/2017.

III. ACTIONS

8.

La partie demanderesse demande au tribunal :

De se déclarer internationalement compétent pour connaître des actions intentées contre Facebook Inc. Et Facebook Ireland, ou à tout le moins de poser les questions préjudicielles suivantes à la Cour de justice :

1)

L'article 28, paragraphes 1, 3 et 6 de la Directive 95/46 du Parlement européen et du Conseil, du 24 octobre 1995 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, lu conjointement aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens que (1) une autorité de contrôle qui, en application des dispositions nationales de la loi en vigueur en application de l'article 28 de ladite directive s'est vu confier le pouvoir d'ester en justice, doit pouvoir exercer ce pouvoir devant le juge compétent de son propre État membre, et (2) ce juge est par conséquent compétent pour se prononcer sur cette action, en cas de violations des dispositions nationales établies en exécution de ladite directive suite à des traitement des données à caractère personnel sur le territoire de cet État membre, même si le responsable du traitement n'est pas établi dans cet État membre ?

2)

Le principe de finalité du droit de l'Union et le principe de protection juridictionnelle effective qu'il exécute, doit-il être interprété en ce sens que ces principes, dans une situation telle que celle qui est présentée dans l'instance principale, s'opposent à une règle processuelle nationale sur pied de laquelle l'autorité de contrôle ne peut citer à comparaître devant une instance judiciaire de son État membre, une personne responsable du traitement établie à l'étranger, au motif de violation de dispositions nationales adoptées en

exécution de la Directive 95/46 qui ont eu lieu sur le territoire de l'État membre de l'autorité de contrôle ?

Déclarer l'action recevable et fondée ;

Par conséquent, condamner Facebook Inc., Facebook Ireland et Facebook Belgium *in solidum*, à tout le moins l'une à défaut de l'autre, à ;

A.

à cesser, l'égard de tout internaute établi sur le territoire belge :

(1) de placer le cookie « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent offrant une fonctionnalité et une utilisation comparables lorsqu'il navigue sur une page web du domaine Facebook.com ou qu'il aboutit sur le site d'un tiers, sans préalablement :

(a) recevoir, de façon claire et compréhensible, des informations complètes et exactes sur :

- les circonstances dans lesquelles Facebook place ces cookies et les collecte ultérieurement ;
- les finalités pour lesquelles Facebook utilise ces cookies ;
- la nature des données collectées par Facebook lorsqu'il consulte un site contenant un social plug-in Facebook, par exemple l'adresse Internet (URL) de ce site web ;
- les destinataires ou les catégories de destinataires des données collectées ;
- l'existence de son droit d'opposition d'accès et de rectification ;
- la durée de conservation des données collectées par l'intermédiaire des cookies et des social plug-ins ;

(b) avoir librement, spécifiquement et indubitablement consenti, tant à l'installation qu'à l'utilisation de ces cookies, pour autant qu'elles ne soient pas strictement nécessaires à la fourniture du service expressément demandé par l'utilisateur et, lorsqu'il s'est déconnecté de Facebook ou s'est désactivé, il n'a pas librement, spécifiquement et indubitablement consenti à la poursuite de l'utilisation de ces cookies ;

(c) a eu la possibilité de refuser l'installation de ces cookies, pour autant qu'ils ne soient pas strictement nécessaires à la fourniture du service qu'il a expressément demandé, sans que cela limite ou complique l'accès au domaine Facebook.com ;

(2) la collecte des cookies « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent offrant une fonctionnalité et une utilisation comparables, au moyen de social plug-ins et pixels Facebook ou outils technologiques similaires sur les sites web de tiers, d'une façon excessive au regard des finalités des cookies concernés, étant entendu que :

(a) la collecte systématique de cookies à des finalités de sécurité lors de la consultation de pages web étrangères au domaine facebook.com, est excessive lorsque :

la personne concernée (1) ne possède pas de compte Facebook ou n'est pas connectée, et (2) ne tente pas d'utiliser les social plug-ins (par exemple en cliquant dessus) ;

(b) la collecte systématique de cookies à des fins publicitaires lors de la consultation de pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée a fait savoir qu'elle ne souhaite pas que son comportement de navigation soit utilisé à des fins publicitaires ;

(c) la collecte systématique de cookies pour vérifier l'identité d'un utilisateur de Facebook ou pour enregistrer le fait qu'il a décidé de rester connecté lorsqu'il consulte des pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée n'est pas connectée et ne tente pas d'utiliser les social plug-ins (par exemple en cliquant dessus) ;

B.

à l'égard de tout internaute établi sur le territoire belge, cesser de fournir des informations raisonnablement susceptibles de tromper la personne concernée sur la portée réelle des mécanismes mis à disposition par Facebook pour que cette dernière puisse gérer l'utilisation des cookies ;

C.

la destruction, sous la supervision d'un expert informatique désigné par les parties, aux frais des défenderesses, de toutes les données à caractère personnel obtenues au sujet de chaque internaute sur le territoire belge au moyen de cookies et de social plug-ins d'une façon dont la cessation a été demandée ci-dessus et exiger cette même destruction des tiers auxquels les défenderesses ont transmis ces données ;

D.

la publication, aux frais des défenderesses, du jugement à intervenir ou d'un résumé de ce dernier défini par le tribunal, sous une forme ou d'une manière définies par le tribunal (1) sur le site web www.facebook.com lorsqu'il est consulté par un internaute établi sur le territoire belge, pendant 3 mois à compter de la signification du jugement à intervenir, et (2) dans les journaux de la presse écrite belge De Standaard, De Morgen, Het Nieuwsblad, Le Soir, La Libre et La Dernière Heure dans les 10 jours ouvrables qui suivent la signification du jugement à intervenir ;

Le tout sous peine d'une astreinte, in solidum, à tout le moins l'une à défaut de l'autre, de 250 000 EUR par jour d'infraction à compter de la signification du jugement à intervenir ;

- Condamner les défenderesses aux dépens, en ce compris les frais de citation, les frais de signification et l'indemnité de procédure, cette dernière taxée à ce stade dans le chef de chacune des défenderesses à 1 440 EUR.

Frais :

- frais de citation : non taxé
- frais de signification non taxé
- indemnité de procédure par défenderesse : 1 440 euros.

La partie en intervention volontaire demande au tribunal :

De se déclarer internationalement compétent pour connaître des actions intentées contre Facebook Inc. Et Facebook Ireland, ou à tout le moins de poser les questions préjudicielles suivantes à la Cour de justice :

1)

L'article 28, paragraphes 1, 3 et 6 de la Directive 95/46 du Parlement européen et du Conseil, du 24 octobre 1995 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, lu conjointement aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne, doit-il être interprété en ce sens que (1) une autorité de contrôle qui, en application des dispositions nationales de la loi en vigueur en application de l'article 28 de ladite directive s'est vu confier le pouvoir d'ester en justice, doit pouvoir exercer ce pouvoir devant le juge compétent de son propre État membre, et (2) ce juge est par conséquent compétent pour se prononcer sur cette action, en cas de violations des dispositions nationales établies en exécution de ladite directive suite à des traitements des données à caractère personnel sur le territoire de cet État membre, même si le responsable du traitement n'est pas établi dans cet État membre ?

Le principe d'efficacité du droit de l'Union et le principe de protection juridictionnelle effective qu'il exécute, doit-il être interprété en ce sens que ces principes, dans une situation telle que celle qui est présentée dans l'instance principale, s'opposent à une règle processuelle nationale sur pied de laquelle l'autorité de contrôle ne peut citer à comparaître devant une instance judiciaire de son État membre, une personne responsable du traitement établie à l'étranger, au motif de violation de dispositions nationales adoptées en exécution de la Directive 95/46 qui ont eu lieu sur le territoire de l'État membre de l'autorité de contrôle ?

Déclarer l'action du requérant recevable et fondée ;

Par conséquent, condamner Facebook Inc., Facebook Ireland et Facebook Belgium *in solidum*, à tout le moins l'une à défaut de l'autre :

A.

à cesser, à l'égard de tout internaute établi sur le territoire belge :

(1) de placer le cookie « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent offrant une fonctionnalité et une utilisation comparables lorsqu'il navigue sur une page web du domaine facebook.com ou qu'il aboutit sur le site d'un tiers, sans préalablement :

(a) recevoir, de façon claire et compréhensible, des informations complètes et exactes sur :

- les circonstances dans lesquelles Facebook place puis collecte par la suite ces cookies ;
- les finalités pour lesquelles Facebook utilise ces cookies ;
- la nature des données collectées par Facebook lorsqu'il consulte un site contenant un social plug-in Facebook, par exemple l'adresse Internet (URL) de ce

site web ;
- les destinataires ou les catégories de destinataires des données collectées ;
- l'existence de son droit d'opposition d'accès et de rectification ;
- la durée de conservation des données collectées par l'intermédiaire des cookies et des social plug-ins ;

(b) avoir librement, spécifiquement et indubitablement consenti, tant à l'installation qu'à l'utilisation de ces cookies, pour autant qu'elles ne soient pas strictement nécessaires à la fourniture du service expressément demandé par l'utilisateur et, lorsqu'il s'est déconnecté de Facebook ou s'est désactivé, il n'a pas librement, spécifiquement et indubitablement consenti à la poursuite de l'utilisation de ces cookies ;

(c) a eu la possibilité de refuser l'installation de ces cookies, pour autant qu'ils ne soient pas strictement nécessaires à la fourniture du service qu'il a expressément demandé, sans que cela limite ou complique l'accès au domaine Facebook.com ;

(2) la collecte des cookies « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent offrant une fonctionnalité et une utilisation comparables, au moyen de social plug-ins et pixels Facebook ou outils technologiques similaires sur les sites web de tiers, d'une façon excessive au regard des finalités des cookies concernés, étant entendu que :

(a) la collecte systématique de cookies à des finalités de sécurité lors de la consultation de pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée : (1) ne possède pas de compte Facebook ou n'est pas connectée, et (2) ne tente pas d'utiliser les social plug-ins (par exemple en cliquant dessus) ;

(b) la collecte systématique de cookies à des fins publicitaires lors de la consultation de pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée a fait savoir qu'elle ne souhaite pas que son comportement de navigation soit utilisé à des fins publicitaires ;

(c) la collecte systématique de cookies pour vérifier l'identité d'un utilisateur de Facebook ou pour enregistrer le fait qu'il a décidé de rester connecté lorsqu'il consulte des pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée n'est pas connectée et ne tente pas d'utiliser les social plug-ins (par exemple en cliquant dessus) ;

B.

à l'égard de tout internaute établi sur le territoire belge, cesser de fournir des informations raisonnablement susceptibles de tromper la personne concernée sur la portée réelle des mécanismes mis à disposition par Facebook pour que cette dernière puisse gérer l'utilisation des cookies ;

C.

la destruction, sous la supervision d'un expert informatique désigné par les parties, aux frais des défenderesses, de toutes les données à caractère personnel obtenues au sujet de chaque internaute sur le territoire belge au moyen de cookies et de social plug-ins d'une

façon dont la cessation a été demandée ci-dessus et exiger cette même destruction des tiers auxquels les défenderesses ont transmis ces données ;

D.

la publication, aux frais des défenderesses, du jugement à intervenir ou d'un résumé de ce dernier défini par le tribunal, sous une forme ou d'une manière définies par le tribunal (1) sur le site web www.facebook.com lorsqu'il est consulté par un internaute établi sur le territoire belge, pendant 3 mois à compter de la signification du jugement à intervenir, et (2) dans les journaux de la presse écrite belge De Standaard, De Morgen, Het Nieuwsblad, Le Soir, La Libre et La Dernière Heure dans les 10 jours ouvrables qui suivent la signification du jugement à intervenir ;

- Le tout sous peine d'une astreinte, in solidum, à tout le moins l'une à défaut de l'autre, de 250 000 EUR par jour d'infraction à compter de la signification du jugement à intervenir ;
- Condamner les défenderesses aux dépens, en ce compris les frais de citation, les frais de signification et l'indemnité de procédure, cette dernière taxée à ce stade dans le chef de chacune des défenderesses à 1 440 EUR.

Frais :

- frais de citation : non taxé
- frais de signification non taxé
- indemnité de procédure par défenderesse : 1 440 euros.

Les **défenderesses** demandent au tribunal :

- Se déclarer internationalement incompétent ;
- à titre subsidiaire, avant de se prononcer sur sa compétence, soumettre au moins la question préjudicielle suivante à la Cour de justice :
  « Les principe généraux du droit public coutumier international doivent-ils être présumés primer sur le Traité de Lisbonne et le droit de l'UE, notamment la Directive 95/46/CE, pour ce qui est de l'applicabilité des règles de protection des données des États membres et l'exercice de la compétence par les tribunaux nationaux dans des affaires dans lesquelles cette réglementation doit être appliquée ? »
- à titre encore plus subsidiaire, déclarer l'action principale et l'intervention volontaire totalement, à tout le moins partiellement, irrecevable, à tout le moins inadmissible ;
- à titre encore plus subsidiaire, rejeter l'action principale et l'intervention volontaire comme infondée ;
- et dans tous les cas, condamner la partie demanderesse aux dépens, taxés dans le chef de chacune des défenderesses à 1 440 euros d'indemnité de procédure, et la partie en intervention à une indemnité de procédure taxée pour chacune des défenderesses à 1 440 euros.

Frais :

- indemnité de procédure par défenderesse : 1 440 euros.

IV. ÉVALUATION

4.1. Compétence

9.

Les défenderesses avancent en premier lieu le fait que les tribunaux belges ne sont pas internationalement compétents pour connaître de cette affaire (du moins à l'égard de Facebook, Inc. en Facebook Ireland) et elles invoquent à cet égard notamment l'arrêt susmentionné de la Cour d'appel de Bruxelles du 29.06.2016 qui a estimé ne pas être compétente à l'égard de Facebook, Inc. et Facebook Ireland. Elles estiment que le raisonnement juridique développé par la Cour dans cet arrêt (considérants 12 et 45), est également valable en la présente procédure au fond.

La Commission vie privée estime que les tribunaux belges sont effectivement compétents pour connaître du litige. Pour former cet avis, elle s'appuie sur divers motifs :

- à titre principal : le principe de territorialité du droit international public et des liens substantiels suffisants avec le territoire belge ;
- à titre subsidiaire : l'applicabilité du droit privé belge ;
- à titre plus subsidiaire : l'art. 32, § 3 de la loi du 8 décembre 1992 ;
- à titre encore plus subsidiaire : l'art. 32, §3 de la loi du 8 décembre 1992, interprétation conforme à l'article 28, alinéas 1, 3 et 6 de la Directive 95/46 ;
- à titre encore plus subsidiaire : le principe d'efficacité du droit de l'Union.

10.

La Commission vie privée avance, à titre principal, que la compétence internationale du tribunal doit être définie suivant les règles de compétences du droit international public et pas du droit privé international, puisque la Commission vie privée intervient en la cause en vertu de son autorité publique (« *acta iure imperii* »).

Selon la Commission vie privée, le fondement concret de la compétence internationale des tribunaux belges est le principe de territorialité du droit international public, qui relève du droit international coutumier et est directement intégré dans le régime moniste belge et peut dès lors être invoqué par le présent tribunal. Selon la Commission vie privée, le principe de territorialité du droit international public permet aux organismes d'un État d'exercer la compétence sur des actes commis sur son territoire ou qui y produisent leurs effets, s'il existe des liens substantiels suffisants avec cet État, en l'occurrence la Belgique.

Aux dires de la Commission vie privée, ces liens sont notamment attestés par le fait que les infractions retenues se déroulent, ou à tout le moins sortent leurs effets, sur le territoire belge, où se trouvent les personnes dont Facebook traite les données, ainsi que leurs appareils sur lesquels elle place ses technologies, et que le site du réseau social et ses activités de marketing ciblent le territoire belge, sur lequel Facebook possède également un établissement physique.

11.

Les défenderesses le contestent. Selon elles, dans le contexte de la présente cause, la Commission vie privée exerce des compétences dites « horizontales », qui n'ont pas pour objet de garantir l'intérêt de l'État, mais des intérêts particuliers (violation de la vie privée de personnes privées), de sorte que l'action n'est pas exclusivement régie par le droit international public. Quand bien même ce serait le cas, l'état de droit et le droit (constitutionnel) belge s'opposent à ce que les règles du droit international coutumier accordent directement une compétence aux tribunaux belges, toujours selon les défenderesses. Ces dernières précisent que l'Union européenne a déjà endossé la compétence de légiférer en matière de protection de la vie privée par l'adoption de la Directive 95/46/CE. Aux dires des défenderesses, l'éventuelle liberté d'exercer une compétence conformément aux principes du droit international public est par conséquent soumise aux limitations découlant du droit de l'UE, sur pied duquel le droit irlandais de protection de la vie privée s'applique en la cause et les tribunaux irlandais sont compétents. Si les tribunaux belges s'appropriaient la compétence en vertu du droit international coutumier, cela constituerait une ingérence injustifiée dans la compétence des tribunaux irlandais.

12.

Le tribunal constate que l'affaire qui lui est soumise contient des points de rattachement à plusieurs ordres juridiques, étant donné qu'il s'agit d'internautes qui se trouvent sur le territoire belge et que deux des trois défenderesses que la Commission vie privée accuse de violer la loi belge de protection de la vie privée sont établies à l'étranger (Facebook Ireland en Irlande et Facebook, Inc. aux États-Unis).

Dans la présente procédure, la Commission vie privée avance pour la première fois expressément la nécessité pour le tribunal de vérifier sa compétence en vertu du droit international public et pas en vertu du droit privé international.

Le droit privé international est le droit (supra)national contenant des règles qui définissent (i) quel droit national s'applique aux rapports juridiques de droit privé ayant des points de rattachement avec plusieurs ordres juridiques, (ii) quel tribunal est internationalement compétent et (iii) la façon dont d'autres États reconnaîtront et appliqueront éventuellement la décision judiciaire. Les relations de droit privé sont les relations qui unissent des personnes privées ou des personnes privées et les pouvoirs publics qui interviennent en tant que particulier.

Le droit (public) international est l'ensemble des règles qui régissent les relations internationales. Il a notamment pour objet de délimiter la compétence des sujets de droit international public (espace, temps, personnes et matière), pour trancher et prévenir les litiges entre eux (coexistence) et pour leur permettre de collaborer au niveau international (coopération, par exemple par la création d'organes et d'institutions internationaux, notamment pour protéger les intérêts communs qui ne peuvent faire l'objet d'une protection unilatérale)[3].

[3] Cf. M. Bossuyt et J. Wouters, Grondlijnen van internationaal recht, Anvers, Intersentia, 2005, p. 3- 5.

L'émergence d'Internet et son développement particulièrement rapide a confronté la communauté internationale à des questions sur le droit applicable aux situations dans lesquelles des entreprises en ligne / sites web établis dans un État déterminé (dans l'Union européenne / EEE ou en dehors de ceux-ci) traitent des données à caractère personnel de personnes établies dans d'autres États[4] et, le cas échéant, quels tribunaux sont compétents. Le tribunal suit la position de l'auteur Christopher Kuner, selon lequel la législation en matière de protection des données ne peut être purement et simplement cataloguée comme ayant une nature exclusivement de droit privé ou de droit public. En effet, elle est issue de plusieurs sources du droit, par exemple le droit de la protection des consommateurs, les droits de l'homme, etc., et qu'il convient de vérifier, dans chaque cas concret, s'il s'agit d'une affaire relevant du droit privé ou du droit public. Ainsi, les actions entreprises par une autorité de contrôle relèvent du droit public, tandis que le droit privé s'applique aux relations contractuelles et extracontractuelles entre des particuliers et une entreprise en ligne[5]*.

Par conséquent, dans un litige contractuel (par exemple entre Facebook et un détenteur de compte) ou extracontractuel (par exemple entre Facebook et un internaute qui ne possède pas de compte Facebook), les tribunaux nationaux devront vérifier, en s'appuyant sur le droit privé international, s'ils sont compétents pour connaître du litige et, dans l'affirmative, quel droit s'applique[6]. Actuellement en Belgique, dans les affaires civiles et commerciales, il s'agit du règlement Bruxelles I(bis), ou du Code de droit privé international du 16 juillet 2004 (CDIP), selon qu'il existe des points de rattachement avec d'autres États, au sein de l'UE ou en dehors de celle-ci.

Le tribunal rejoint l'affirmation de la Commission vie privée selon laquelle elle n'intervient pas en la cause en tant que particulier, mais en tant que pouvoir public dans le cadre des compétences qui lui sont octroyées en qualité « d'autorité de contrôle » nationale. Dans son arrêt du 29 juin 2016, la Cour d'appel de Bruxelles a d'ailleurs également déjà estimé que la Commission vie privée intervenait en qualité de « pouvoir public *sensu lato* (conformément à l'article 23 LVP, la CPVP a été « instituée auprès de la Chambre des représentants » - elle fait donc partie du pouvoir législatif) à l'encontre de diverses sociétés commerciales ». Par conséquent, en la présente cause, le tribunal ne doit pas vérifier sa compétence en vertu du droit privé international, mais en vertu du droit international public.

13.

Le droit (public) international peut s'appliquer à l'ensemble de la communauté internationale, à une région limitée (par exemple l'Union européenne) ou entre deux États. Les sources du droit international sont notamment les traités, le droit international coutumier et les principes généraux du droit.

---

[4] Cf. également Groupe de travail « article 29 », Document de travail du 30 mai 2002, disponible surhttp://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf.

[5] voir également C. Kuner, Data Protection Law and International Jurisdiction on the Internet (Part 1), Int J Law Info Tech, 11 mars 2010, p. 9 et 10, cf. pièce A.18 des défenderesses.

[6] Cf. I. Samoy, e.a., Facebook maakt privéberichten openbaar: een casus contractuele aansprakelijkheid? Juristenkrant 5 décembre 2012, p. 10.

Pour qu'il soit question d'une coutume en tant que source du droit international, celui qui l'invoque doit prouver qu'il existe une pratique des états uniforme, stable et suffisamment étendue (ce que l'on peut notamment déduire des lois internes et de décisions judiciaires) et une « *opinio iuris* », c'est-à-dire une conviction que l'on peut agir de la sorte. Dans la mesure où il est souvent difficile de prouver l'existence de ces « règles », les États procèdent parfois à la codification de ces règles dans des traités[7]. Il n'existe pas de hiérarchie de principe entre les traités et le droit international coutumier, de sorte qu'en cas de conflit entre les deux, la dernière règle prime sur la première, étant entendu que la règle particulière prime sur la règle générale, quand bien même celle-ci est ultérieure. Le droit international coutumier fait partie intégrante de l'ordre juridique belge [8] et les règles de droit interne ne peuvent ignorer des principes du droit international coutumier[9]. Les principes généraux du droit sont, eux aussi, une source autonome de droit international, ils peuvent jouer un rôle devant les tribunaux et les cours internes.

Dans le droit international, la juridiction ou la compétence est le pouvoir que les États peuvent exercer sur des personnes, des choses ou des événements. Elles peuvent être divisées en juridiction législative, judiciaire et d'application ou de contrainte (par exemple la détention de personnes ou la saisie de biens)[10] [11].

La compétence peut aussi être divisée en juridiction territoriale, fonctionnelle et extraterritoriale. En principe, étant donné sa souveraineté, un État a pleine compétence sur les personnes, les choses et les événements sur son territoire. Les états peuvent également avoir une juridiction extraterritoriale (législative et judiciaire) sur les personnes, les choses et les événements hors de son territoire, en fonction d'un lien de nationalité (principe de personnalité active et passive), les intérêts de la sécurité (principe de protection) ou le caractère punissable de certains faits (principe d'universalité). La doctrine (internationale) contient également d'autres principes dans lesquels les états peuvent puiser leur compétence, par exemple la théorie des effets.

14.

Les parties présentent les opinions de divers experts auxquels ils ont demandé un avis sur la compétence des tribunaux belges pour connaître de l'action de la Commission vie privée dans la présente procédure. Ils abordent non seulement les règles coutumières du droit international public, mais aussi les règles européennes en matière de protection de la vie privée (ce qui est logique, comme nous le verrons ultérieurement).

Le prof. M. Ryngaert estime que les juges belges sont compétents en la présente cause, en vertu du principe de territorialité du droit coutumier, selon lequel les États peuvent exercer leur compétence sur des actes commis sur leur territoire ou qui y produisent leurs effets. La territorialité objective signifie qu'un État peut exercer sa compétence lorsqu'un acte initié à

[7] voir. M. Bossuyt et J. Wouters, Grondlijnen van internationaal recht, Anvers, Intersentia, 2005, p. 105 ; P.h. Kooijmans, Internationaal recht in vogelvlucht, Kluwer, Deventer, 2002, p. 11.
[8] Cass. 25 janvier 1906, Pas. 1906,1,109, Cases 11.4.
[9] Cf. en relation avec le principe du droit international coutumier : Cass. 12 février 2003, disponible sur le site http://www.cass.be (27 février 2003).
[10] Cf. M. Bossuyt et J. Wouters, Grondlijnen van internationaal recht, Anvers, Intersentia, 2005, p. 285-286.
[11] Cf. M. Bossuyt et J. Wouters, Grondlijnen van internationaal recht, Anvers, Intersentia, 2005, p. 286.

l'étranger produit ses effets sur le territoire de l'État concerné. En vertu de la territorialité subjective, un État peut exercer sa compétence sur un acte initié sur son territoire, mais qui produit ses effets à l'étranger. À l'instar de la théorie de l'ubiquité, qui rend les juges belges compétents pour les délits pénaux dont un élément constitutif a eu lieu sur le territoire belge, l'exercice de la compétence sur l'Internet et le cybermonde repose sur le principe de territorialité et la théorie de l'ubiquité (cet expert invoque ultérieurement des exemples en matière de cybercriminalité). Dès qu'une activité a un lien substantiel suffisant avec le territoire belge, ce qui, de l'avis du prof. M. Ryngaert est le cas en l'occurrence, le droit belge s'applique et tous les organes de l'État, tant la Commission vie privée que les tribunaux belges, sont internationalement compétents en vertu de ce principe de territorialité. Le prof. M. Ryngaert invoque également la pratique d'autres États tels que les Pays-Bas, dont l'autorité nationale s'est déclarée compétente pour exercer un contrôle à l'égard du traitement par Facebook Inc. des données à caractère personnel des utilisateurs établis aux Pays-Bas.

Le prof. M. Wautelet fait également remarquer que, pour déterminer le droit applicable dans les matières relevant du droit public, il suffit de vérifier si une situation déterminée tombe sous le coup de l'application de la législation concernée. Cela signifie que, dès que la Commission vie privée estime que Facebook viole la législation belge de protection de la vie privée, elle peut exercer les compétences qui lui ont été confiées par la loi, en ce compris le droit de son président de soumettre tout litige concernant l'application de la loi du 8 décembre 1992 et ses mesures d'exécution au tribunal de première instance, étant entendu que la juridiction de la Commission vie privée et des tribunaux belges doit être confrontée aux règles du droit international public et que les tribunaux belges (en-dehors des matières du droit privé international) ne sont internationalement compétents que si le droit belge s'applique. Partant, le tribunal doit donc vérifier si la législation belge de protection de la vie privée s'applique en l'occurrence. Si oui, le tribunal est compétent. Si non il doit se déclarer internationalement incompétent.

Le prof. M. Tom Ruys souligne le fait qu'en droit international public, le principe de territorialité est le point de convergence le plus accepté et le plus évident pour exercer une juridiction et qu'à l'inverse, généralement, les États ne peuvent exercer une juridiction extraterritoriale que si elle se justifie en vertu d'un principe de compétence permissif. Il cite à cet égard le principe de la personnalité active, le (très controversé) principe de la personnalité passive, le principe de protection (qui cible la garantie des intérêts de l'État) et le principe de l'universalité (pour les délits les plus graves). Il souligne par ailleurs le fait que la juridiction, et principalement la compétence d'exécution, ne peut s'appuyer que sur un principe de compétence largement accepté. Le prof. M. Ruys décrit en outre la doctrine des effets comme étant un prolongement du principe objectif de territorialité, en ce sens que cette doctrine lui apporte une concrétisation extraterritoriale. Le principe de base en la matière est que les États peuvent établir une juridiction à l'égard d'un comportement qui a lieu en dehors de leur territoire, mais qui a néanmoins des conséquences substantielles sur leur territoire. Cet expert relève que la doctrine des effets n'est pas exempte de controverse et, surtout, qu'elle n'est pas extensible à l'infini, car dans le domaine d'Internet, elle implique un risque de surrèglementation et de chevauchement de juridiction (puisque virtuellement, chaque État pourrait se déclarer compétent à l'égard d'informations disponibles sur Internet). Selon le prof. M. Ruys, ce principe doit donc être restreint et appliqué strictement par l'examen du caractère raisonnable, afin d'éviter des conflits de

compétence interétatiques. Selon le prof. M. Ruys, le prof. M. Ryngaert ne considère pas l'examen du caractère raisonnable comme une norme contraignante pour le juge national, mais il lui substitue une approche de subsidiarité : les États doivent laisser l'exercice de la juridiction à l'état qui entretient les liens les plus forts avec les faits concernés, sauf s'il apparaît que cet état n'assume pas sa responsabilité réglementaire. Selon le prof. M. Ruys, le tribunal doit vérifier concrètement s'il existe un lien suffisamment clair et substantiel avec le territoire belge et se déclarer incompétent si les organes administratifs et judiciaires d'un autre État sont compétents. Il souligne également le fait que les règles du droit coutumier, notamment la doctrine des effets (qui est en soi toujours controversée), définit uniquement les limites extrêmes dans lesquelles les autorités nationales et les juges sont à même d'exercer leur compétence. Prof. M. Ruys relève par conséquent que le tribunal doit dans un premier temps vérifier la compétence de la Commission vie privée (et du tribunal) en matière de protection de la vie privée, puis dans un second temps, si cette compétence est conforme aux règles de juridiction inscrites dans le droit international public.

L'auteur Christopher Kuner, auquel plusieurs experts font référence, suggère que l'Internet complique fortement l'application du principe de territorialité, car il peut s'avérer pratiquement impossible de localiser une action en ligne dans un État déterminé, mais que l'art. 4 (1) (c) de la Directive 95/46/CE (voir infra) semble former une expression du principe de territorialité objectif, puisqu'il se base, au moins en partie, sur l'accomplissement d'un acte (l'utilisation d'un appareillage au sein de l'UE)[12]. Ce même auteur qualifie la doctrine des effets, en vertu de laquelle un État devient compétent en vertu du fait que des actes posés en dehors de son territoire ont des effets substantiels au sein de cet État, comme étant le fondement de juridiction le plus controversé (et fortement critiqué), tout en constatant que cette doctrine semble s'être largement répandue dans les questions juridictionnelles concernant les comportements sur Internet et que l'art. 4 (1) (c) de la Directive 95/46/CE peut également être considéré comme une application de la doctrine des effets, car elle se concentre plus largement sur les conséquences du traitement des données dans l'UE et la protection des citoyens de l'UE[13].

15.

Le tribunal se déclare d'accord sur l'affirmation du prof. M. Ruys, selon laquelle le tribunal doit vérifier les compétences dont jouit la Commission vie privée, en qualité d'« autorité *sensu lato* » (et dans la foulée, éventuellement le tribunal) en la présente affaire et si elle exerce ces compétences dans le respect des règles de juridiction du droit public international.

Dans ce contexte, il ne faut pas perdre de vue que l'État belge, par son appartenance à l'Union européenne, a cédé certaines compétences à cette dernière. Ce faisant, l'État belge a « limité » sa souveraineté en diverses matières et, avec les autres États membres, il a volontairement créé un système juridique contraignant tant pour ces états membres que pour leurs ressortissants[14].

---

[12] C. Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1"), disponible sur le site https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1496847, p. 18.
[13] Ibidem, p. 20-21.
[14] M. Wathelet et S. Van Raepenbusch, De betrekkingen tussen de grondwettelijke hoven en de andere

Le « droit de l'Union » englobe des règles qui voient le jour tant par le fait des États membres que par des actions des institutions et organismes communautaires. Le « droit primaire de l'Union » englobe les normes directement adoptées par les États membres comme étant « constituantes » et qui forment, avec les principes généraux du droit (dont la Cour de justice garantit le respect), les normes « constitutionnelles » du droit de l'Union. Le droit « dérivé » de l'Union, à savoir les règles créées par les institutions et organismes, est soumis à l'application des normes primaires et au contrôle de légalité de la Cour européenne de justice. Les principes généraux du droit jouent un rôle dans l'interprétation et l'application des dispositions conventionnelles et autres normes du droit communautaire. Dans la mesure où l'Union européenne a l'intention de s'inscrire dans l'ordre juridique international, lorsqu'elle exerce ses compétences, elle se droit de respecter le droit international. Certains principes du droit international consacrés dans des conventions ou qui ont acquis la force du droit coutumier, priment en qualité de principes généraux du droit de l'Union. Par conséquent, dans l'interprétation et l'application du droit de l'Union, la Cour de justice tient compte du droit international coutumier, ainsi que des principes du droit international (par exemple le principe de territorialité comme limite à la portée des compétences de l'Union européenne ; voir également infra). Dans la mesure où les dispositions conventionnelles et les actions directement applicables des institutions européennes (par exemple également les directives) priment sur toute règle de droit national, notamment les « l'ordre constitutionnel d'un État membre », les instances judiciaires des États membres sont également tenues d'interpréter le droit national à la lumière des dispositions du droit de l'Union, afin d'assurer ainsi le plein effet du droit de l'Union.[15]

L'Union européenne n'a pas omis d'intervenir dans le domaine de la protection des données à caractère personnel, initialement par l'adoption de la Directive 95/46/CE du 24 octobre 1995[16] puis, à compter du 25 mai 2018, par l'application du « Règlement général sur la protection des données »[17], qui révoque la Directive 95/46/CE. Pour ce qui est de la présente procédure, le tribunal doit par conséquent également tenir compte de la Directive 95/46/CE.

Les défenderesses font remarquer, à juste titre, qu'il existe une différence entre, d'une part, la question de l'application territoriale des législations nationales de protection de la vie privée et, d'autre part, les compétences en soi des autorités nationales de contrôle. Il est dès lors important d'examiner plus en détail l'interaction entre les deux. Le tribunal remarque d'ores et déjà que la Cour européenne de justice s'est déjà prononcée sur le sujet

---

nationale rechterlijke instanties: rapport van het Hof van Justitie van de Europese Gemeenschappen in XIIe Congres van de Conferentie van Europese Grondwettelijke Hoven, p. 10 e.s.

[15] K. Lenaerts et P. Van Nuffel, Europees recht in hoofdlijnen, Anvers, Maklu, 1999, p. 611 e.s.; cf. e.a. Aussi CEDJ 15 juillet 1964 (arrêt Costa/E.N.E.L); CEDJ 9 mars 1978 (arrêt Simmenthal); voir également Cass. 14 janvier 2016, F.14.0015.N, www.cass.be : « Il ressort de la primauté du droit de l'Union européenne que le juge doit donner la priorité à la disposition d'une directive par rapport à une disposition du droit national contraire et qu'il est tenu de ne pas faire application de cette dernière disposition ».

[16] *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, Journal officiel de l'UE du 23 novembre 1995, L281, p. 0031-0050.*

[17] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Journal officiel de l'UE du 4 mai 2016, L119/1 e.s.*

dans son arrêt « Weltimmo » (voir infra).

16.

Pour ce qui est de la compétence de l'autorité de contrôle, l'art. 28 de la Directive 95/46/CE prescrit ce qui suit :

« 1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. Chaque autorité de contrôle dispose notamment :

- *de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle ;*
- *de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques ;*
- *du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.*

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié.

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État

membre.

Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

7. Les États membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès. »

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, précise les compétences de la commission vie privée (belge). En vertu de cette loi, la Commission est compétente pour émettre des avis ou recommandations sur toute matière relative à l'application des principes fondamentaux de la protection de la vie privée, dans le cadre de cette loi, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel (art. 29 et 30), et d'examiner les plaintes signées et dates qui lui sont adressées (art. 31). La Commission vie privée peut également peut requérir le concours d'experts et procéder à un examen sur place (art. 32 § 1). La Commission dénonce au procureur du Roi les infractions dont elle a connaissance (article 32, § 2, LVP) ; 32 § 2). 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 vie privée peut soumettre au tribunal de première instance tout litige concernant l'application de la loi du 8 décembre 1992 et ses mesures d'exécution. La loi du 8 décembre 1992 contient également des sanctions pénales (art. 38-43).

Dans la foulée du Règlement général sur la protection des données, le 25 mai 2018, la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, entrera en vigueur en Belgique, abrogeant dans le même temps les chapitres VII et VIIbis (relatifs à la Commission vie privée et aux comités sectoriels) de la loi du 8 décembre 1992. L'Autorité de protection des données remplacera la Commission vie privée ; un service d'inspection pourra enquêter et la chambre contentieuse pourra adopter diverses mesures, notamment ordonner que le traitement soit rendu conforme à la législation, imposer des amendes administratives, ordonner la suspension de flux transfrontaliers de données vers un autre État ou une institution internationale (mesures qui peuvent faire l'objet d'un recours auprès de la « Cour des marchés », c'est-à-dire une section de la Cour d'appel de Bruxelles).

Cette Autorité aura par conséquent des compétences plus étendues que celles de la Commission vie privée dans le cadre législatif actuel. Si à l'heure actuelle, la Commission vie privée peut formuler des avis et recommandations, dénoncer au procureur du Roi les infractions dont elle a connaissance et soumettre les litiges susmentionnés aux cours et tribunaux ordinaires, l'Autorité de protection des données est également compétente pour mener une enquête administrative (par le biais de son service d'inspection), avant (i) de transmettre le dossier au président de la chambre contentieuse (ii) au procureur du Roi si les faits sont susceptibles de constituer une infraction pénale, (iii) de classer un dossier sans suite et (iv) de le transmettre à une autorité de protection des données d'un autre État. La chambre contentieuse est une juridiction administrative qui peut appliquer des sanctions.

Si les autorités de contrôle d'autres États disposent d'ores et déjà, en vertu de leur droit national, de compétences administratives pour ordonner elles-mêmes, après enquête, des mesures ou imposer des amendes à la suite d'une violation de la législation nationale en matière de protection de la vie privée, la loi belge relative à la protection de la vie privée ne

le permet donc pas encore (cf. Imposition d'amendes par l'autorité hongroise dans l'affaire Weltimmo, qui a formé appel de cette décision devant le juge hongrois, voir infra). L'actuelle loi du 8 décembre 1992 donne toutefois au président de la Commission vie privée le droit de soumettre tout litige concernant l'application de ladite loi et de ses mesures d'exécution au tribunal de première instance ; en vertu de la législation belge actuelle, la Commission vie privée ne peut par conséquent exercer utilement ses compétences d'autorité de contrôle belge que si elle peut demander, dans le prolongement de cette action, au juge belge d'imposer certaines mesures dans le respect de la législation belge.

17.

Aux termes de l'art. 3bis, la loi belge relative à la protection de la vie privée s'applique territorialement (souligné par le tribunal) :

> 1° lorsque le traitement est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public ;
>
> 2° lorsque le responsable du traitement n'est pas établi de manière permanente sur le territoire de la Communauté européenne et recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge. Dans les cas visés au paragraphe 2°, le responsable du traitement doit désigner un représentant établi sur le territoire belge, sans préjudice d'actions qui pourraient être introduites contre le responsable du traitement lui-même.

L'art. 3bis a été introduit par la loi du 11 décembre 1998[18] transposant la Directive 95/46/CE du 24 octobre 1995. Les travaux préparatoires de la loi du 11 décembre 1998 expliquent ce qui suit à cet égard souligné et mis en gras par le tribunal) :

« Cet article constitue la transposition de l'article 4 de la directive européenne. L'objectif de l'article 4 consiste à veiller à ce que tous les traitements de données à caractère personnel effectués au sein de la Communauté, tombent sous l'application de la législation d'un des États membres, de sorte que personne ne soit exclu de la protection à laquelle il a droit en vertu de la directive (considérant 18 de la directive). Le critère utilisé par la directive pour constater quel est l'État membre dont la législation doit être appliquée, est le lieu de l'établissement pour lequel le traitement est effectué. Afin de déterminer quel est l'État membre dont la législation doit être appliquée, il convient de se poser la question : sur le territoire de quel État membre se situe l'établissement, dans le cadre des activités duquel le traitement est effectué ? Ce n'est donc pas le lieu du traitement qui est déterminant, ni le lieu du siège principal ou la résidence du responsable du traitement. La question est : ***dans le cadre des activités de quel établissement du responsable le traitement est-il effectué et sur quel territoire se situe cet établissement*** *? Il est fort possible que le traitement (par exemple une étude de marché) soit effectué en Belgique, mais qu'il soit effectué dans le cadre des*

[18] Loi transposant la directive 95/46/CE du 24 octobre 1995 du parlement européen et du Conseil 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, MB 03.02.1999, entrée en vigueur le 01-09-2001.

activités d'un établissement du responsable dans un autre État membre. Dans ce cas, la législation de cet autre État membre est d'application. Afin d'éviter toute ambiguïté le considérant 21 de la directive européenne prévoit que cette réglementation ne préjuge pas des règles de territorialité en matière de droit pénal. Dans certains cas il ne sera pas toujours aussi facile de déterminer de quel établissement émane un traitement de données à caractère personnel. Des entreprises situées dans différents États membres, mais faisant partie du même groupe, confient parfois la gestion de la banque de données contenant les données à caractère personnel ou relatives aux clients à une seule entreprise du groupe. Dans la mesure où chaque entreprise de ce groupe traite des données, même à l'aide de la banque centrale de données, ce traitement est soumis à la législation de l'État membre dans lequel est établie l'entreprise qui utilise la banque centrale de données. (...) En plus de la question de savoir quelle législation est applicable, il convient naturellement de déterminer également quel est le responsable du traitement dans cette situation, ou en d'autres termes, quelle est la personne qui décide de la finalité et des moyens du traitement. La réponse à cette question est, entre autres, importante parce que le responsable qui possède un établissement sur le territoire de plusieurs États membres doit prendre les mesures nécessaires afin que chaque établissement satisfasse aux obligations imposées par la législation nationale applicable.

Le considérant 19de la directive dit 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 ». En raison de leur importance ces précisions sont intégrées au texte de l'article 3bis (...). Le même considérant dit également « 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 ». Lorsqu'un seul et même responsable est établi sur le territoire de plusieurs États membres il doit, pour chacun de ses établissements, se conformer aux obligations de la législation applicable. Afin d'éviter qu'une personne de la Communauté ne jouisse d'aucune protection lors du traitement de données à caractère personnel parce que le responsable du traitement n'a pas d'établissement dans un État membre de la Communauté européenne, un autre critère est utilisé pour déterminer la législation applicable dans ce cas. Le critère déterminant à cet égard, est l'État membre dans lequel sont situés les moyens à l'aide desquels les traitements de données à caractère personnel sont effectués. Le terme « moyens » recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit de données à caractère personnel par le territoire, tels que les câbles, les routers, etc.

Lorsque le responsable du traitement est établi sur le territoire belge et traite, dans le cadre des activités de cet établissement, des données à caractère personnel dans un pays en dehors de la Communauté européenne, ce traitement sera régi par la loi belge. Ceci pourrait, par exemple, signifier qu'une entreprise pharmaceutique établie en Belgique, collecte, dans le cadre de ses expériences pharmacologiques, des données relatives à la santé en Afrique afin de les traiter ensuite en Belgique. Lors de la collecte de ces données en Afrique, l'entreprise belge devra alors appliquer les principes de la loi belge. L'article 4, paragraphe 2, de la directive européenne dispose que : « dans le cas visé au paragraphe I, point c). » (...) Les circonstances décrites au paragraphe I^er^, point c), renvoient à la situation où « le responsable du traitement n'est pas établi sur le territoire de la Communauté » L'obligation de désigner un représentant en Belgique peut par conséquent uniquement être imposée aux

responsables qui ne sont pas établis sur le territoire de la Communauté européenne. ».

L'art. 4 de la Directive 95/46/CE du 24 octobre 1995 prescrit comme suit :

« 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. »

18.

La jurisprudence de la Cour européenne de justice explique (i) comment l'art. 4 de la Directive 95/46/CE doit être interprété et (ii) quelles sont les compétences des autorités nationales de contrôle.

Dans l'arrêt C-131/12 du 13 mai 2014 (Google Spain SL et Google Inc. Contre Agencia Espanola de Protección de Datos (AEPD) et Mario Costeja Gonzalez) la Cour européenne de justice semble s'être basée, d'une part sur le principe de territorialité et, d'autre part, sur la théorie des effets. La Cour de Justice a en effet estimé :

«

45 Par sa première question, sous a), la juridiction de renvoi demande, en substance, si l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'une ou plusieurs des trois conditions suivantes sont réunies :

- *l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre, ou*

- *la société mère désigne une filiale implantée dans ledit État membre comme son représentant et comme étant responsable du traitement de deux fichiers spécifiques contenant les données des clients ayant conclu des services publicitaires avec cette entreprise, ou*

- *la succursale ou la filiale établie dans un État membre transmet à la société mère, basée en dehors de l'Union, les réclamations et les injonctions que lui adressent aussi bien les intéressés que les autorités compétentes en vue d'obtenir le respect du droit à la protection des données à caractère personnel, même lorsque cette collaboration a lieu de manière volontaire.*

46 En ce qui concerne la première de ces trois conditions, la juridiction de renvoi relève que Google Search est exploité et géré par Google Inc. et qu'il n'est pas établi que Google Spain réalise en Espagne une activité directement liée à l'indexation ou au stockage d'informations ou de données contenues dans les sites web de tiers. Cependant, l'activité de promotion et de vente des espaces publicitaires, dont s'occupe Google Spain pour l'Espagne, constituerait la partie essentielle de l'activité commerciale du groupe Google et pourrait être considérée comme étant étroitement liée à Google Search.

47 M. Costeja González, les gouvernements espagnol, italien, autrichien et polonais ainsi que la Commission estiment que, compte tenu du lien indissociable entre l'activité du moteur de recherche exploité par Google Inc. et celle de Google Spain, cette dernière doit être considérée comme un établissement de la première, dans le cadre des activités duquel le traitement de données à caractère personnel est effectué. En revanche, selon Google Spain, Google Inc. et le gouvernement hellénique, l'article 4, paragraphe 1, sous a), de la directive 95/46 ne trouve pas à s'appliquer dans l'hypothèse de la première des trois conditions énumérées par la juridiction de renvoi.

48 À cet égard, il convient tout d'abord de relever que le considérant 19 de la directive 95/46 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 ».

49 Or, il n'est pas contesté que Google Spain se livre à l'exercice effectif et réel d'une activité au moyen d'une installation stable en Espagne. Étant en outre dotée d'une personnalité juridique propre, elle constitue ainsi une filiale de Google Inc. sur le territoire espagnol et, partant, un «établissement» au sens de l'article 4, paragraphe 1, sous a), de la directive 95/46.

50 Afin de satisfaire au critère établi à cette disposition, encore faut-il que le traitement de données à caractère personnel par le responsable de celui-ci soit « effectué dans le cadre des activités » d'un établissement de ce responsable sur le territoire d'un État membre.

51 Google Spain et Google Inc. contestent que ce soit le cas dès lors que le traitement de données à caractère personnel en cause au principal est effectué exclusivement par Google Inc., qui exploite Google Search sans aucune intervention de la part de Google Spain, dont l'activité se limite à la fourniture d'un soutien à l'activité publicitaire du groupe Google qui est distincte de son service de moteur de recherche.

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.

58 Dans ces conditions, il ne saurait être accepté que le traitement de données à caractère personnel effectué pour les besoins du fonctionnement dudit moteur de recherche soit soustrait aux obligations et aux garanties prévues par la directive 95/46, ce qui porterait atteinte à l'effet utile de celle-ci et à la protection efficace et complète des libertés et des droits fondamentaux des personnes physiques qu'elle vise à assurer (voir, par analogie, arrêt L'Oréal e.a., EU:C:2011:474, points 62 et 63), notamment celui au respect de leur vie privée, à l'égard du traitement des données à caractère personnel, auquel cette directive accorde une importance particulière ainsi que le confirment notamment son article 1er, paragraphe 1, et ses considérants 2 et 10 (voir, en ce sens, arrêts Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 70; Rijkeboer, C-553/07, EU:C:2009:293, point 47, ainsi que IPI, C-473/12, EU:C:2013:715, point 28 et jurisprudence citée).

59 Dans la mesure où la première des trois conditions énumérées par la juridiction de renvoi suffit à elle seule pour conclure qu'un établissement tel que Google Spain satisfait au critère prévu à l'article 4, paragraphe 1, sous a), de la directive 95/46, il n'est pas nécessaire d'examiner les deux autres conditions.

60 Il découle de ce qui précède qu'il convient de répondre à la première question, sous a), que l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre. »

Dans son arrêt C-230/14 du 1er octobre 2015 (Weltimmo s.r.o. contre Nemzeti Adatvédelmi és Információszabadség Hatósag) la Cour a estimé comme suit à propos de l'art. 4 de la Directive 95/46 (souligné par le tribunal) :

« *19 Par ses première à sixième questions, qu'il y a lieu d'examiner ensemble, la juridiction de renvoi demande en substance si les articles 4, paragraphe 1, sous a), et 28, paragraphe 1, de la directive 95/46 doivent être interprétés en ce sens que, dans des circonstances telles que celles en cause au principal, ils permettent à l'autorité de contrôle d'un État membre d'appliquer sa législation nationale sur la protection des données à l'égard d'un responsable de traitement, dont la société est immatriculée dans un autre État membre et qui exploite un site Internet d'annonces immobilières concernant des biens immobiliers situés sur le territoire du premier de ces deux États. Elle demande en particulier s'il est pertinent que cet État membre soit celui :*

- *vers lequel l'activité du responsable du traitement des données à caractère personnel est tournée ;*
- *où les biens immobiliers concernés sont situés ;*
- *à partir duquel les données relatives aux propriétaires de ces biens sont communiquées ;*
- *dont ceux-ci sont ressortissants, et*
- *dans lequel les propriétaires de cette société habitent.*

20 S'agissant du droit applicable, la juridiction de renvoi mentionne plus particulièrement les droits slovaque et hongrois, le premier de ces droits étant celui de l'État membre dans lequel le responsable du traitement des données à caractère personnel concernées est immatriculé et le second étant celui de l'État membre visé par les sites Internet en cause au principal, sur le territoire duquel les biens immobiliers faisant l'objet des annonces publiées sont situés.

21 À cet égard, il convient de constater que l'article 4 de la directive 95/46, intitulé «Droit national applicable», qui figure au chapitre Ier de cette directive, intitulé «Dispositions générales», régit précisément la question posée.

22 L'article 28 de la directive 95/46, intitulé « Autorité de contrôle », est, en revanche, consacré au rôle et aux pouvoirs de cette autorité. En vertu de cet article 28, paragraphe 1, celle-ci est chargée de surveiller l'application, sur le territoire de l'État membre dont elle relève, des dispositions adoptées par les États membres en application de cette directive. Conformément à l'article 28, paragraphe 6, de ladite directive, l'autorité de contrôle exerce les pouvoirs dont elle est investie, indépendamment du droit national applicable au traitement des données à caractère personnel.

23 C'est donc au regard non pas de l'article 28 de la directive 95/46, mais de l'article 4

de cette dernière qu'il convient de déterminer le droit national applicable au responsable de ce traitement.

24 Aux termes de l'article 4, paragraphe 1, sous a), de la directive 95/46 chaque État membre applique les dispositions nationales, qu'il arrête en vertu de cette directive aux traitements de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre.

25 Au vu de l'objectif poursuivi par la directive 95/46, consistant à 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, l'expression « dans le cadre des activités d'un établissement » ne saurait recevoir une interprétation restrictive (voir, en ce sens, arrêt Google Spain et Google, C-131/12, EU:C:2014:317, point 53).

26 Afin d'atteindre cet objectif et d'éviter qu'une personne soit exclue de la protection qui lui est garantie par cette directive, le considérant 18 de ladite directive énonce qu'il est nécessaire que tout traitement de données à caractère personnel effectué dans l'Union européenne respecte la législation de l'un des États membres et qu'il est opportun de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un État membre à l'application de la législation de cet État.

27 Le législateur de l'Union a ainsi prévu un champ d'application territorial, de la directive 95/46 particulièrement large, qu'il a inscrit à l'article 4 de celle-ci voir, en ce sens, arrêt Google Spain et Google, C-131/12, EU:C:2014:317, point 54).

28 S'agissant, en premier lieu, de la notion d'«établissement», il convient de rappeler que le considérant 19 de la directive 95/46 énonce 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 (arrêt Google Spain et Google, C-131/12, EU:C:2014:317, point 48). Ce considérant précise, par ailleurs, que, lorsqu'un même responsable est établi sur le territoire de plusieurs États membres, il doit s'assurer, notamment en vue d'éviter tout contournement, que chacun des établissements remplit les obligations prévues par le droit national applicable aux activités de chacun d'eux.

29 Il en découle, ainsi que l'a relevé en substance M. l'avocat général aux points 28 et 32 à 34 de ses conclusions, une conception souple de la notion d'établissement, qui écarte toute approche formaliste selon laquelle une entreprise ne serait établie que dans le lieu où elle est enregistrée. Ainsi, afin de déterminer si une société, responsable d'un traitement de données, dispose d'un établissement, au sens de la directive 95/46, dans un État membre autre que l'État membre ou le pays tiers où elle est immatriculée, il convient d'évaluer tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans cet autre État membre, en tenant compte de la nature spécifique des activités économiques et des prestations de services en question. Cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur internet.

30 À cet égard, il y a lieu, notamment, de considérer, au vu de l'objectif poursuivi par

cette directive, consistant à assurer une protection efficace et complète du droit à la vie privée et à éviter tout contournement, que la présence d'un seul représentant peut, dans certaines circonstances, suffire pour constituer une installation stable si celui-ci agit avec un degré de stabilité suffisant à l'aide des moyens nécessaires à la fourniture des services concrets concernés, dans l'État membre en question..

31 En outre, afin de réaliser ledit objectif, il y a lieu de considérer que la notion d'«établissement», au sens de la directive 95/46, s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable.

32 En l'occurrence, l'activité exercée par Weltimmo consiste, à tout le moins, dans l'exploitation d'un ou de plusieurs sites Internet d'annonces immobilières concernant des biens situés en Hongrie, qui sont rédigés en langue hongroise et dont les annonces deviennent payantes au terme d'un délai d'un mois. Il y a donc lieu de constater que cette société se livre à une activité réelle et effective en Hongrie.

33 En outre, il ressort notamment des précisions apportées par l'autorité de contrôle hongroise que Weltimmo dispose d'un représentant en Hongrie, qui est mentionné dans le registre des sociétés slovaque sous une adresse située en Hongrie et qui a cherché à négocier avec les annonceurs le règlement des créances impayées. Ce représentant a servi de relais entre cette société et les plaignants et a représenté celle-ci au cours des procédures administrative et judiciaire. En outre, ladite société a ouvert un compte bancaire en Hongrie, destiné au recouvrement de ses créances et elle utilise une boîte aux lettres sur le territoire de cet État membre pour la gestion de ses affaires courantes. Ces éléments, qu'il appartient à la juridiction de renvoi de vérifier, sont susceptibles d'établir, dans une situation telle que celle en cause au principal, l'existence d'un « établissement », au sens de l'article 4, paragraphe 1, sous a), de la directive 95/46.

34 Il importe, en second lieu, de savoir si le traitement des données à caractère personnel concerné est effectué « dans le cadre des activités » de cet établissement.

35 La Cour a déjà considéré que l'article 4, paragraphe 1, sous a), de la directive 95/46 exige que le traitement de données à caractère personnel en question soit effectué non pas «par» l'établissement concerné lui-même, mais uniquement «dans le cadre des activités» de celui-ci (arrêt Google Spain et Google, C-131/12, EU:C:2014:317, point 52).

36 En l'occurrence, le traitement en cause au principal consiste, notamment, dans la publication, sur les sites Internet d'annonces immobilières de Weltimmo, de données à caractère personnel relatives aux propriétaires de ces biens ainsi que, le cas échéant, dans l'utilisation de ces données pour les besoins de la facturation des annonces au terme d'un délai d'un mois.

37 À cet égard, il convient de rappeler que, s'agissant en particulier d'Internet, la Cour a déjà eu l'occasion de constater que l'opération consistant à faire figurer, sur une page Internet, des données à caractère personnel est à considérer comme un «traitement», au sens de l'article 2, sous b), de la directive 95/46 (arrêts Lindqvist, C-101/01, EU:C:2003:596, point 25, et Google Spain et Google, C-131/12, EU:C:2014:317, point 26).

38 Or, il ne fait pas de doute que ce traitement a lieu dans le cadre des activités, décrites au point 32 du présent arrêt, auxquelles se livre Weltimmo en Hongrie.

39 Partant, sous réserve des vérifications rappelées au point 33 du présent arrêt, qu'il

appartient à la juridiction de renvoi d'effectuer aux fins d'établir, le cas échéant, l'existence d'un établissement du responsable du traitement en Hongrie, il y a lieu de considérer que ce traitement est réalisé dans le cadre des activités de cet établissement et que l'article 4, paragraphe 1, sous a), de la directive 96/46 permet, dans une situation telle que celle en cause au principal, l'application du droit hongrois relatif à la protection des données à caractère personnel.

40 La circonstance que les propriétaires des biens faisant l'objet des annonces immobilières sont de nationalité hongroise n'est, en revanche, aucunement pertinente aux fins de déterminer le droit national applicable au traitement des données en cause au principal.

41 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre aux première à sixième questions de la manière suivante :

- *l'article 4, paragraphe 1, sous a), directive 95/46 doit être interprété en ce sens qu'il permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est immatriculé, pour autant que celui-ci exerce, au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué ;*
- *afin de déterminer, dans des circonstances telles que celles en cause au principal, si tel est le cas, la juridiction de renvoi peut, notamment, tenir compte du fait, d'une part, que l'activité du responsable dudit traitement, dans le cadre de laquelle ce dernier a lieu, consiste dans l'exploitation de sites Internet d'annonces immobilières concernant des biens immobiliers situés sur le territoire de cet État membre et rédigés dans la langue de celui-ci et qu'elle est, par conséquent, principalement, voire entièrement, tournée vers ledit État membre et, d'autre part, que ce responsable dispose d'un représentant dans ledit État membre, qui est chargé de recouvrer les créances résultant de cette activité ainsi que de le représenter dans des procédures administrative et judiciaire relatives au traitement des données concernées ;*
- *en revanche, est dénuée de pertinence la question de la nationalité des personnes concernées par ce traitement de données. »*

Dans l'arrêt « Weltimmo », la Cour de juste s'est également prononcée sur les compétences des autorités nationales si le droit national ou le droit d'un autre État membre s'applique (souligné par le tribunal) :

« 42 La septième question n'est posée que dans l'hypothèse où l'autorité de contrôle hongroise considérerait que Weltimmo dispose, non pas en Hongrie, mais dans un autre État membre, d'un établissement, au sens de l'article 4, paragraphe 1, sous a), de la directive 95/46, exerçant des activités dans le cadre desquelles le traitement des données à caractère personnel concernées est effectué.

43 Par cette question, la juridiction de renvoi demande, en substance, si, dans le cas où l'autorité de contrôle hongroise parviendrait à la conclusion que le droit applicable au traitement des données à caractère personnel est non pas le droit hongrois, mais le droit d'un autre État membre, l'article 28, paragraphes 1, 3 et 6, de la directive 95/46 devrait être interprété en ce sens que cette autorité ne pourrait exercer que les pouvoirs prévus à l'article 28, paragraphe 3, de cette directive, conformément au droit de cet autre État membre, et ne pourrait infliger de sanctions.

(...)

46 Il convient d'examiner, en second lieu, quels sont les pouvoirs de cette autorité de contrôle, à la lumière de l'article 28, paragraphes 1, 3 et 6, de la directive 95/46.

47 Il résulte de l'article 28, paragraphe 1, de cette directive que chaque autorité de contrôle mise en place par un État membre veille au respect, sur le territoire de cet État membre, des dispositions adoptées par les États membres en application de la directive 95/46.

48 En vertu de l'article 28, paragraphe 3, de la directive 95/46 ces autorités de contrôle disposent notamment de pouvoirs d'investigation, tels que le pouvoir de recueillir toutes les informations nécessaires à l'accomplissement de leur mission de contrôle, et de pouvoirs effectifs d'intervention, tels que ceux d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou d'adresser un avertissement ou une admonestation au responsable du traitement.

49 Compte tenu du caractère non exhaustif des pouvoirs ainsi énumérés à cette disposition ainsi que de la marge de manœuvre dont disposent les États membres pour la transposition de la directive 95/46, il y a lieu de considérer que ces pouvoirs d'intervention peuvent comprendre celui de sanctionner le responsable du traitement de données en lui infligeant, le cas échéant, une amende.

50 Les pouvoirs accordés aux autorités de contrôle doivent être exercés conformément au droit procédural de l'État membre dont elles relèvent.

51 Il ressort de l'article 28, paragraphes 1 et 3, de la directive 95/46 que chaque autorité de contrôle exerce l'ensemble des pouvoirs qui lui ont été conférés sur le territoire de l'État membre dont elle relève, afin d'assurer sur ce territoire le respect des règles en matière de protection des données.

52 Cette application territoriale des pouvoirs de chaque autorité de contrôle est confirmée à l'article 28, paragraphe 6, de cette directive, lequel énonce que chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément à l'article 28, paragraphe 3, de ladite directive et cela indépendamment du droit national applicable. Cet article 28, paragraphe 6, précise également que chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre et que les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

53 Cette disposition est nécessaire pour assurer la libre circulation des données à caractère personnel dans l'Union, tout en veillant au respect des règles visant à protéger la vie privée des personnes physiques prévues par la directive 95/46. En effet, en l'absence de ladite disposition, dans le cas où le responsable du traitement des données à caractère personnel serait soumis à la loi d'un État membre, mais enfreindrait le droit à la protection de la vie privée des personnes physiques dans un autre État membre, notamment en tournant son activité vers cet autre État membre sans pour autant y être établi, au sens de cette directive, il serait difficile, voire impossible, pour ces personnes de faire respecter leur droit à cette protection.

54 Il résulte ainsi de l'article 28, paragraphe 6, de la directive 95/46 que l'autorité de

contrôle d'un État membre, qui est saisie par des personnes physiques d'une réclamation relative au traitement des données à caractère personnel les concernant, sur le fondement de l'article 28, paragraphe 4 de cette directive, peut examiner cette réclamation indépendamment du droit applicable, et, par conséquent, même si le droit applicable au traitement des données concernées est celui d'un autre État membre.

55 Toutefois, dans cette hypothèse, les pouvoirs de cette autorité ne comprennent pas nécessairement l'ensemble de ceux dont elle est investie conformément au droit de l'État membre dont elle relève.

56 En effet, ainsi que M. l'avocat général l'a relevé au point 50 de ses conclusions il découle des exigences résultant de la souveraineté territoriale de l'État membre concerné, du principe de légalité et de la notion d'État de droit que le pouvoir de répression ne peut, en principe, s'exercer en dehors des limites légales dans lesquelles une autorité administrative est habilitée à agir, dans le respect du droit de l'État membre dont elle relève.

57 Ainsi, lorsqu'une autorité de contrôle est saisie d'une plainte, conformément à l'article 28, paragraphe 4, de la directive 95/46, cette autorité peut exercer ses pouvoirs d'investigation indépendamment du droit applicable et avant même de savoir quel est le droit national qui est applicable au traitement en cause. Cependant, si elle parvient à la conclusion que le droit d'un autre État membre est applicable, elle ne saurait imposer des sanctions en dehors du territoire de l'État membre dont elle relève. Dans une telle situation, il lui appartient, en exécution de l'obligation de coopération que prévoit l'article 28, paragraphe 6, de cette directive, de demander à l'autorité de contrôle de cet autre État membre de constater une éventuelle infraction à ce droit et d'imposer des sanctions si ce dernier le permet,, en s'appuyant, le cas échéant, sur les informations qu'elle lui aura transmises.

58 L'autorité de contrôle saisie d'une telle plainte peut, dans le cadre de cette coopération, être amenée à effectuer d'autres investigations, sur les instructions de l'autorité de contrôle de l'autre État membre.

59 Il s'ensuit que, dans une situation telle que celle en cause au principal, dans l'hypothèse où le droit applicable serait celui d'un État membre autre que la Hongrie, l'autorité de contrôle hongroise ne pourrait exercer les pouvoirs de sanction que le droit hongrois lui a confiés.

60 Il résulte des considérations qui précèdent qu'il convient de répondre à la septième question que, dans l'hypothèse où l'autorité de contrôle d'un État membre saisie de plaintes, conformément à l'article 28, paragraphe 4, de la directive 95/46, parviendrait à la conclusion que le droit applicable au traitement des données à caractère personnel concernées est non pas le droit de cet État membre, mais celui d'un autre État membre, l'article 28, paragraphes 1, 3 et 6, de cette directive doit être interprété en ce sens que cette autorité de contrôle ne pourrait exercer les pouvoirs effectifs d'interventions qui lui ont été conférés conformément à l'article 28, paragraphe 3, de ladite directive ***que sur le territoire de l'État membre dont elle relève****. Partant, elle saurait infliger de sanctions sur la base du droit de cet État membre au responsable du traitement de ces données qui n'est pas établi sur ce territoire, mais devrait, en application de l'article 28, paragraphe 6, de la même directive, demander à l'autorité de contrôle relevant de l'État membre dont le droit est applicable d'intervenir. »*

Dans son arrêt C-191/15 du 28 juillet 2016 (Verein för Konsumenteninformation - Amazon)

la Cour de Justice a estimé (souligné par le tribunal) :

« 72 Par sa quatrième question, sous b), la juridiction de renvoi cherche à savoir, en substance, si l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un traitement de données à caractère personnel effectué par une entreprise de commerce électronique est régi par le droit de l'État membre vers lequel cette entreprise dirige ses activités.

73 Aux termes de l'article 4, paragraphe 1, sous a), de la directive 95/46, chaque État membre applique les dispositions nationales qu'il arrête en vertu de ladite directive aux traitements de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre.

74 Il en découle qu'un traitement de données effectué dans le cadre des activités d'un établissement est régi par le droit de l'État membre sur le territoire duquel est situé cet établissement.

75 S'agissant, en premier lieu, de la notion d'« établissement » au sens de l'article 4, paragraphe 1, sous a), de la directive 95/46, la Cour a déjà précisé qu'elle s'étend à toute activité réelle et effective, même minime, exercée au moyen d'une installation stable (arrêt d'octobre 2015, Weltimmo, C-230/14, EU:C:2015:639, point 31).

76 À cet égard, comme l'a relevé M. l'avocat général au point 119 de ses conclusions, si la circonstance que l'entreprise responsable du traitement de données ne possède ni filiale ni succursale dans un État membre n'exclut pas qu'elle puisse y posséder un établissement au sens de l'article 4, paragraphe 1, sous a), de la directive 95/46, un tel établissement ne saurait exister du simple fait que le site Internet de l'entreprise en question y est accessible.

77 Il convient plutôt d'évaluer, ainsi que la Cour l'a déjà relevé, tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans l'État membre en question (voir, en ce sens, arrêt du 1er octobre 2015, Weltimmo, C-230/14, EU:C:2015:639, point 29).

78 S'agissant, en second lieu, du point de savoir si le traitement des données à caractère personnel concerné est effectué « dans le cadre des activités » de cet établissement, au sens de l'article 4, paragraphe 1, sous a), de la directive 95/46, la Cour a déjà rappelé que cette disposition exige que le traitement de données à caractère personnel en question soit effectué non pas « par » l'établissement concerné lui-même, mais uniquement « dans le cadre des activités » de celui-ci (arrêt du 1er octobre 2015, Weltimmo, C-230/14, EU:C:2015:639, punt 35).

79 Il appartient à la juridiction de renvoi de déterminer, à la lumière de cette jurisprudence et en tenant compte de toutes les circonstances pertinentes de l'affaire en cause au principal, si Amazon EU procède au traitement des données en question dans le cadre des activités d'un établissement situé dans un État membre autre que le Luxembourg.

80 Ainsi que l'a relevé M. l'avocat général au point 128 de ses conclusions, *si la juridiction de renvoi venait à établir que l'établissement dans le cadre duquel Amazon EU procède au traitement de ces données est situé en Allemagne il appartiendrait au droit allemand de régir ce traitement.*

81 Au vu de ce qui précède, il y a lieu de répondre à la quatrième question, sous b), que l'article 4, paragraphe 1, sous a), de la directive 95/46 doit être interprété en ce sens qu'un

traitement de données à caractère personnel effectué par une entreprise de commerce électronique est régi par le droit de l'État membre vers lequel cette entreprise dirige ses activités s'il s'avère que cette entreprise procède au traitement des données en question dans le cadre des activités d'un établissement situé dans cet État membre. Il appartient à la juridiction nationale d'apprécier si tel est le cas.

19.

Comme indiqué, Facebook est un site de réseau social en ligne mondial et gratuit, qui peut (faire) adresser des publicités extrêmement ciblées aux internautes individuels, où qu'ils se trouvent dans le monde, grâce aux informations qu'elle collecte sur les personnes au moyen de son site de réseau, ses modules sociaux, cookies, pixels, etc.

Les défenderesses ne peuvent raisonnablement contester que Facebook traite, au moyen de ses cookies, social plug-ins et pixels, des données à caractère personnel aux termes de la Directive 95/46/CE (cf. Les définitions de l'art. 2, a) et b) de la Directive). En effet, il est un fait que grâce à ces techniques, Facebook collecte et conserve notamment des informations sur des personnes identifiables à l'aide de leur(s) adresse(s) IP et de leurs identifiants uniques contenus dans les cookies, d'autant plus qu'à l'heure actuelle, les ordinateurs portables et smartphones, etc. sont de plus en plus utilisés par une seule personne.

L'Art. 2, d de la Directive définit le « Responsable du traitement » comme étant « *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; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire* ».

L'Art. 2, e de la Directive définit le « sous-traitement » comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

Les défenderesses expliquent que Facebook Ireland a été constituée en 2010 en qualité de responsable de tous les traitements de données des utilisateurs établis en dehors des États-Unis et du Canada et qu'elle exerce effectivement cette responsabilité au sein de l'UE. Elles invoquent notamment en la matière la politique d'utilisation des données des Services Facebook disponible à l'adresse https://www.facebook.com/policy.php, pièce 3 des défenderesses).

C'est à juste titre que la Commission vie privée souligne que dans le cadre de l'art. 4, alinéa 1, a) de la Directive 95/46/CE, le lieu d'établissement précis du responsable du traitement des données à caractère personnel (dans l'UE ou en dehors de celle-ci) n'est pas pertinent.

À la lumière de la jurisprudence de la Cour de justice, concrètement, en la présente procédure, le tribunal doit vérifier si la législation belge de protection de la vie privée s'applique, ce qui est le cas si Facebook Ireland et / ou Facebook Inc. Exerce, au moyen d'une installation stable sur le territoire de la Belgique, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué, ou encore, si le

responsable du traitement des données à caractère personnel procède au traitement des données concernées dans le cadre des activités d'un établissement situé en Belgique.

La question qui se pose par conséquent est de savoir quelles activités Facebook Belgium exerce exactement.

Les pièces présentées montrent que Facebook Belgium fait partie de « Facebook - concern » et qu'elle a été constituée le 31 mai 2011 par les sociétés de droit américain « Facebook Global Holdings II » et « Facebook Global Holdings I ». Son objet statutaire consiste notamment en activités relatives aux affaires publiques, au lobbying, au public spécialisé et aux ONG, aux médias, à la gestion de crise, aux recherches et études, à la formation (notamment aux médias) (voir pièce G.1 du demandeur).

Dans leurs conclusions de synthèse, les défenderesses expliquent que Facebook Belgium est une entité constituée pour se concentrer sur les relations avec les institutions de l'UE (au moment des conclusions, cinq collaborateurs se chargeaient de ces activités) et apporter un support aux publicitaires clients de Facebook Ireland installés en Belgique (au moment des conclusions, trois collaborateurs se chargeaient de ces activités). Elles soulignent aussi le fait que Facebook Belgium ne joue aucun rôle dans la façon dont Facebook Ireland contrôle précisément l'utilisation des données reçues par l'intermédiaire des cookies et que Facebook Belgium sprl n'utilise pas les données en question.

La Commission vie privée souligne le fait que les défenderesses ont affirmé en référé que « *deux membres du personnel (de Facebook Belgium) sont en contact avec des entreprises belges dans le but de leur apporter des services de support dans le domaine du marketing et de la vente d'espaces publicitaires par Facebook Ireland », que deux collaborateurs de Facebook Belgium sprl « apportent à Facebook Ireland un support dans le domaine de la publicité » et que Facebook Belgium « collabore à la commercialisation d'espace publicitaire* ».

Le rapport annuel joint aux comptes annuels émis par les gérants de Facebook Belgium à l'intention de l'assemblée générale des actionnaires concernant la politique menée durant l'exercice clôturé au 31.12.2014 (pièce G.2 du demandeur), indique que la principale activité menée par l'entreprise en 2014 consistait à assister la « politique publique » (« public policy ») et les services de vente et de marketing du Groupe Facebook et que fin 2014, l'entreprise comptait cinq collaborateurs. Les gérants de Facebook Belgium décrivent les principaux risques et incertitudes auxquels l'entreprise fait face comme (i) l'émergence de réseaux sociaux concurrents vers lesquels les utilisateurs de Facebook pourraient se tourner, (ii) une atteinte à la sécurité et un crash éventuel du site web qui détruiraient la confiance que les utilisateurs portent au site et (iii) des problèmes liés à la protection de la vie privée, qui pourraient réduire le nombre d'utilisateurs et, (iv) une récession mondiale qui pourrait entraîner une diminution des dépenses publicitaires.

Selon le rapport de politique des gérants pour l'exercice clôturé le 31.12.2015 (pièce G.3 du demandeur), la principale activité de Facebook Belgium consistait à soutenir la politique publique du Groupe Facebook et que l'entreprise employait quatre collaborateurs à la fin de l'année 2015. Dans la mesure où l'entreprise fournit également des services de vente et de marketing au groupe Facebook, les gérants décrivent les seuls risques et incertitudes auxquels l'entreprise peut être confrontée comme (i) l'impossibilité de conserver les clients existants et d'attirer de nouveaux clients ou une diminution de l'intérêt pour les produits Facebook, (ii) l'incertitude due à la compétitivité du secteur et (iii) la perte de membres du

personnel essentiels ou l'impossibilité d'attirer à l'avenir du personnel hautement qualifié.

Les autres pièces présentées (notamment poste vacant) montrent également que Facebook Belgium s'occupe de la politique publique du groupe Facebook. Elle effectue également un travail de lobbying auprès des pouvoirs publics et des hommes et femmes politiques, en leur fournissant des informations sur les produits et activités de Facebook, en répondant aux questions des hommes et femmes politiques et des régulateurs et en contribuant au développement de la réglementation du secteur de l'Internet. Elle entretient par ailleurs des contacts avec les médias et d'autres organisations dans le but de promouvoir les objectifs politiques de Facebook. Elle émet également des avis internes aux équipes de Facebook sur la politique publique en fonction de l'évolution des produits, services et policies (traduit librement « lignes politiques »).

La Commission vie privée souligne également le fait qu'un représentant de Facebook Ireland a déclaré durant l'audience du 29.04.2015 que quelques collaborateurs de Facebook Belgium sont des spécialistes du marketing qui mènent des activités de marketing pour les produits publicitaires de Facebook ici en Belgique (voir pièce D.1 du demandeur et les pièces E.1.a et E.1.b). Elle présente en outre plusieurs pièces concernant des collaborateurs de Facebook et au vu desquelles il apparaît qu'ils se concentrent sur les activités de vente et de marketing sur le territoire belge (voir pièces H.1 à H.6 incluses du demandeur, notamment « *Alexis Lebedoff doit convaincre des entreprises de poster des publicités à côté de votre profil* »).

Dans l'affaire « Google Spain », la Cour de justice a constaté que le moteur de recherche « Google Search » était exploité par une entreprise dont le siège était établi aux États-Unis, disposant d'une installation stable en Espagne, qui exerçait une activité effective et réelle. Cet établissement assurait la promotion et la vente des espaces publicitaires proposés par « Google Search », dont le moteur de recherche devait assurer la rentabilité économique. Lorsqu'un internaute saisissait un terme dans le moteur de recherche, l'affichage de résultats étant accompagné, sur la même page, de celui de publicités liées aux termes de recherche. Par conséquent, la Cour de justice a estimé que le traitement de données à caractère personnel en question était 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.

Par analogie, le tribunal constate dans la présente affaire que le site de réseau social Facebook est exploité par le groupe Facebook, qui compte diverses sociétés liées telles que Facebook, Inc. et Facebook Ireland, qui proposent les Services Facebook respectivement aux États-Unis, au Canada et en Europe et, dans ce contexte, traite des données à caractère personnel. Le groupe Facebook dispose d'une installation stable en Belgique, Facebook Belgium, qui a sa propre personnalité morale et une activité effective, durable et réelle. Les comptes annuels de Facebook Belgium 2015 mentionnent expressément « *Facebook Inc.* » en tant que « société mère consolidée » (pièce G.3 du demandeur).

Le lien entre l'activité de Facebook Belgium et du groupe Facebook est comparable à celui qui est constaté dans l'affaire « Google Spain ». Lorsque des internautes ont recours aux Service Facebook au sens large ou qu'ils consultent les sites web de tiers comportant des pixels Facebook, leurs données à caractère personnel sont traitées et utilisées à des fins de publicité ciblée. Les activités de l'exploitant des Services Facebook et celles de l'établissement belge sont par conséquent indissociablement liées :

- les activités de Facebook Belgium (support aux publicitaires en Belgique activités de vente et de marketing et lobbying) ont pour objet de rendre (ou de maintenir) le site de réseau social Facebook et ses activités apparentées économiquement rentables ;
- le site du réseau social Facebook et les activités apparentées, notamment le traitement des données à caractère personnel sont également le moyen par lequel l'établissement belge est en mesure d'exercer ses activités.

Le tribunal est par conséquent d'avis qu'il y a en l'espèce une activité commerciale dans le chef de l'établissement du responsable du traitement sur le territoire belge, dans le cadre duquel le traitement en question est effectué. Le fait que Facebook Belgium ne traiterait pas elle-même de données à caractère personnel ou qu'elle interviendrait seulement en qualité d'intermédiaire commercial et ne signerait pas les contrats avec les annonceurs, comme l'avancent les défenderesses n'est pas pertinent, notamment à la lumière de la jurisprudence susmentionnée de la Cour de justice.

En conséquence, en vertu de l'art. 4, alinéa 1, a) de la Directive 95/46/CE, la Belgique peut appliquer sa loi vie privée nationale au traitement des données à caractère personnel mené dans le cadre des activités de Facebook Belgium et Facebook Ireland, qui est le responsable du traitement des données à caractère personnel, doit adopter les mesures nécessaires pour faire en sorte que Facebook Belgium respecte les obligations imposées par la législation nationale applicable.

20.

Comme indiqué précédemment, le président de la Commission vie privée a toujours le droit, en vertu de la loi du 8 décembre 1992 (encore en vigueur) de soumettre tout litige concernant l'application de ladite loi et de ses mesures d'exécution au tribunal de première (art. 32 §3). Vu que la loi du 8 décembre 1992 n'a pas octroyé à la Commission vie privée la compétence d'adopter elle-même des mesures ou d'imposer des sanctions (elle peut toutefois mener une médiation sur la base d'une plaine datée et signée et, éventuellement, dresser un procès-verbal de conciliation), son président peut saisir les tribunaux belge pour leur demander d'imposer certaines mesures dans le but de mettre un terme à de prétendues violations de la vie privée des internautes sur le territoire belge.

Contrairement aux affirmations des défenderesses, il n'y a ici aucune contradiction avec le droit de l'Union, au contraire, cette compétence du président en est précisément la conséquence, ni avec la Constitution belge.

Par conséquent, le présent tribunal est (internationalement) compétent pour connaître de l'action de la Commission vie privée.

4.2. Recevabilité

4.2.1. L'action à l'encontre de Facebook Belgium

21.

Avant tout, les défenderesses avancent que l'action à l'encontre de Facebook Belgium est inadmissible, puisqu'elle ne serait pas la défenderesse adéquate. D'après Facebook, « Seules les personnes morales et entités responsables des actions visées (« les responsables du traitement des données ») peuvent être citées en justice (...) », tandis que « Facebook Belgium n'est pas le responsable du traitement des données litigieuses (pas davantage d'ailleurs que d'aucune autre donnée traitée par le Service Facebook) » et « elle ne fournit pas le service Facebook aux utilisateurs ».

La Commission vie privée fait remarquer, à juste titre, qu'il s'agit du fond de l'affaire, de sorte que le tribunal rejette le moyen d'irrecevabilité avancé.

4.2.2. L'action intentée par le Président de la Commission vie privée - Intervention volontaire

22.

Les défenderesses affirment également que selon la citation l'action a été intentée par monsieur Willem Debeuckelaere « en sa qualité de président de la Commission vie privée » et donc pas au nom de la Commission vie privée elle-même. Elles estiment que seule la Commission vie privée a la qualité nécessaire pour intervenir dans des litiges relatifs à l'application de la loi vie privée du 8 décembre 1992 et que l'action est par conséquent « inadmissible, à tout le moins irrecevable à défaut de qualité pour intenter cette action »

L'article 32 § 3 de 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 prescrit :

« Art. 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. »

*Le tribunal constate que la citation émane de « Monsieur **WILLEM DEBEUCKELAERE**, fonctionnaire, conformément à l'article 32 §3 de 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, **AGISSANT EN SA QUALITÉ DE PRÉSIDENT DE LA COMMISSION BELGE DE LA PROTECTION DE LA VIE PRIVÉE**, numéro d'entreprise 0893.076.921, instaurée conformément à l'article 23 de ladite loi du 8 décembre 1992 auprès de la Chambre des représentants, sise à 1000 Bruxelles, Rue de la Presse 3, Belgique, où il fait élection de domicile ».*

Par conséquent, le tribunal ne peut que constater que la citation émane à juste titre du demandeur, en sa qualité de président de la Commission vie privée, puisque la loi le prescrit de la sorte et qu'il a l'intérêt et la qualité requis pour intenter l'action. La Commission vie privée n'a en effet, à titre personnel, aucune personnalité morale et en vertu de la loi, ce n'est pas elle qui peut ester en justice, mais son président. Contrairement aux affirmations des défenderesses, il n'est pas nécessaire de mentionner encore dans la citation que monsieur Debeuckelaere intente l'action « au nom » de la Commission vie privée, cela constituerait un formalisme inutile et serait superflu eu égard à la formulation de la loi.

L'action du demandeur est par conséquent recevable.

23.

Le 30.06.2017, une requête en intervention volontaire a été déposée par « ***LA COMMISSION POUR LA PROTECTION DE LA VIE PRIVÉE***, *conformément à l'article 23 de ladite loi du 8 décembre 1992, instaurée auprès de la Chambre des représentants, sise à 1000 Bruxelles, Rue de la Presse 3, numéro d'entreprise 0893.076.921, représentée par son président, monsieur Willem Debeuckelaere; agissant en la présente cause conformément à l'article 32 §3 de la loi du 8 décembre 1992* ».

Les défenderesses avance que l'intervention volontaire est irrecevable, car son dispositif reprend uniquement la demande de monsieur Willem Debeuckelaere en sa qualité de demandeur, sans mentionner expressément ce que la partie en intervention volontaire attend comme prononcé au sujet de l'intervention. Selon les défenderesses, il n'est pas question d'une véritable intervention aux termes de l'art. 16, premier alinéa C. jud., parce que la partie en intervention :

(i) n'est pas un tiers en l'occurrence, si l'on suit le raisonnement du demandeur, selon lequel la Commission vie privée est déjà partie « en qualité de demanderesse » ;

(ii) elle ne peut défendre que son propre intérêt, soit en apportant son aide à l'intérêt d'une partie déjà présente, soit en faisant valoir sa propre prétention au droit déjà contesté, alors que la Commission vie privée ne fait en l'occurrence ni l'un ni l'autre.

L'art. 15 C. jud. prescrit que l'intervention est une procédure par laquelle un tiers devient partie à la cause. Elle vise soit à protéger les intérêts de la partie en intervention ou de l'une des parties à l'instance, soit à faire prononcer une condamnation ou faire ordonner une garantie. Aux termes de l'art. 16 C. jud. l'intervention est volontaire lorsque le tiers se présente afin de défendre ses intérêts.

À la troisième page de la requête, nous pouvons lire (traduction libre) : « *La présente requête tend à l'intervention par la Commission vie privée (la CPVP) au cas où Votre tribunal estimerait, per impossibile, que ce moyen des défenderesses est fondé (quod certe non)* ». « Ce moyen » porte sur le moyen des défenderesses traité ci-avant selon lequel l'action intentée par le Président de la Commission vie privée serait irrecevable et que le tribunal a rejeté, puisqu'il est claire qu'il intervient en vertu de la loi et que la Commission vie privée n'est pas en mesure de le faire par elle-même.

Le tribunal constate, pour cette même raison, que la demande en intervention volontaire est irrecevable.

Le tribunal utilise ci-après les termes « la Commission vie privée » pour désigner la partie demanderesse.

4.2.3. Action intentée concernant la LCE[19]

24.

Les défenderesses avancent que l'action de la Commission vie privée pour une prétendue violation de l'art. 129 LCE est dans tous les cas irrecevable, au motif que la Commission vie privée n'est pas compétente pour ester en justice dans le cadre de la LCE. Elles précisent que la présente procédure ne se limite pas à une action basées sur (une interprétation de) l'article 32 §3 de la loi vie privée, qui doit être interprété de façon restrictive, mais porte en réalité sur l'art. 129 LCE (dont relève l'utilisation des cookies), tandis que la LCE n'attribue aucune compétence à la Commission vie privée pour ester en justice, mais bien des compétences d'application à une autre instance, à savoir l'Institut belge des services postaux et des télécommunications (ci-après IBPT).

25.

L'art. 129 de la LCE prescrit :

« *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 autorisé 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. »

Dans ce seul article, la LCE invoque à deux reprises la loi sur la protection de la vie privée. Cela n'a rien d'étonnant, puisque la LCE est la transposition en droit belge de diverses directives, 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

[19] Loi du 13 juin 2005 relative aux communications électroniques, M.B. du 20 juin 2005.

communications électroniques [20]) (J.O.C.E. 31 juillet 2002, L 201/37)[21], qui à son tour spécifie et complète la Directive 95/46/CE.

L'art. 1 (Champ d'application et objectif) de la Directive 2002/58/CE prescrit en effet (souligné par le tribunal) :

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

(…) »

Le considérant 4 de la Directive 2002/58/CE dispose comme suit (souligné par le tribunal) :

« *La directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (5) a traduit les principes définis dans la directive 95/46/CE en règles spécifiques applicables au secteur des télécommunications. La directive 97/66/CE doit être adaptée à l'évolution des marchés et des technologies des services de communications électroniques afin de garantir un niveau égal de protection des données à caractère personnel et de la vie privée aux utilisateurs de services de communications électroniques accessibles au public, indépendamment des technologies utilisées. Il convient, par conséquent, que ladite directive soit abrogée et remplacée par la présente directive.* »

Et le considérant 6 :

« *L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.* »

Et le considérant 10 :

« *Dans le secteur des communications électroniques, la directive 95/46/CE est applicable notamment à tous les aspects de la protection des droits et libertés fondamentaux qui n'entrent pas expressément dans le cadre de la présente directive, y compris les obligations auxquelles est soumis le responsable du traitement des données à caractère personnel et les droits individuels. La directive 95/46/CE s'applique aux services de communications électroniques non publics.*

L'exposé des motifs du projet de loi de la LCE indique également (souligné par le tribunal) :

20

21 cf. art. 1 LCE.

« *La section 2 du chapitre III du titre IV est essentiellement consacrée à la transposition de 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 », ci-après : « la directive vie privée et communications électroniques »). Les dispositions de cette section instaurent à certains endroits un régime spécifique de protection de la vie privée, adapté aux caractéristiques et aux besoins du secteur des communications électroniques. À d'autres endroits, les dispositions de cette section doivent être considérées comme un complément des dispositions de 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 (dénommée ci-après : « la loi sur la vie privée »).*

26.

Le tribunal estime que la Commission vie privée, dont les compétences sont inscrites dans la loi relative à la protection de la vie privée du 8 décembre 1992, est dès lors effectivement compétente pour soumettre la présente action au tribunal, dans la mesure où elle porte sur de prétendues violations de ladite loi du 8 décembre 1992, à laquelle l'art. 129 LCE, qui la précise et la complète, fait expressément référence.

Que le fait que l'art. 32 §3 de la loi relative à la protection de la vie privée (pour ce qui est de l'intervention en justice) mentionne uniquement « la présente loi »[22], tandis que les articles concernant ses autres compétences (notamment l'art. 29 - avis, art. 30 - recommandations, mentionne également d'autres lois contenant des dispositions relatives à la vie privée[23], n'y porte pas préjudice.

La Commission vie privée fait remarquer, à juste titre, que le législateur ne pouvait avoir l'intention de lui accorder des compétences plus restrictives en matière d'action en justice que pour ses autres compétences (il apparaît que ce qui précède est uniquement la conséquence de la manière dont l'art. 32 §3 de la loi relative à la protection de la vie privée a vu le jour ; voir pièces du demandeur sous J.). Il ressort en revanche de l'art. 129 LCE que la loi relative à la vie privée reste pleinement en vigueur dans la mesure où les données à caractère personnel sont traitées.

Concernant les compétences de l'IBTP en matière de protection de la vie privée des utilisateurs, la LCE prescrit :

« *Missions générales de l'Institut en matière de communications électroniques.*

Art. 5. Dans le cadre de l'exercice de ses compétences, l'Institut prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 6 à 8. Ces mesures sont basées sur la nature des problèmes constatés, sont appliquées proportionnellement et justifiées. Elles

---

[22] *« 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 ».*

[23] *« des avis sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel ».*

doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence, de non-discrimination et de neutralité technologique.

(...)

Art. 8. Dans l'accomplissement des tâches qui lui incombent en vertu de la présente loi, l'Institut veille aux intérêts des utilisateurs : (...)

3° en contribuant à assurer un niveau élevé de protection des données à caractère personnel et de la vie privée ;

(...) ».

Ces dispositions n'excluent en aucun cas la compétence de la Commission vie privée en qualité d'autorité de contrôle générale en matière de vie privée, de rendre des avis ou des recommandations, de mener des enquêtes ou d'ester en justice lorsque le traitement des données à caractère personnel intervient dans le cadre de la communication électronique. La loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et télécommunications belges détermine en effet que, dans le cadre de ses compétences, l'IBTP collabore avec la Commission vie privée et lui communique des informations (art. 14 §2, 3°, h).

Le tribunal rejette par conséquent le motif d'irrecevabilité avancé par les défenderesses.

4.2.4. Action relative à l'utilisation de pixels pour obtenir des cookies

27.

Les défenderesses avancent en outre que l'action de la Commission vie privée concernant l'utilisation de pixels, dont il fut question pour la première fois dans les conclusions du demandeur du 31.01.2017, est irrecevable au motif qu'il s'agirait d'une « nouvelle demande » aux termes de l'art. 807 C. jud.

L'article 807 C. jud. prescrit comme suit :

« *La demande dont le juge est saisi peut être étendue ou modifiée, si les conclusions nouvelles, contradictoirement prises, sont fondées sur un fait ou un acte invoqué dans la citation, même si leur qualification juridique est différente.* »

Selon les défenderesses, Facebook reçoit depuis des années, et depuis bien avant la citation du 11.09.2015, des données cookies de pixels intégrés dans des « sites web de tiers », ce que tout expert en informatique pourrait constater, bien que la Commission vie privée n'ait pas jugé nécessaire de s'en plaindre dans la citation. Les défenderesses évoquent également qu'il n'existait pas encore de litige concret à ce sujet entre elles et la Commission vie privée, qui a par ailleurs seulement émis une Recommandation complémentaire à ce sujet le 12.04.2017, longtemps après la citation. D'après les défenderesses, l'action concernant l'utilisation des pixels ne repose donc pas sur un fait ou un acte invoqué dans la citation.

28.

L'article 807 C. jud. permet d'étendre ou de modifier l'objet et d'en modifier la qualification

juridique, à condition que la cause de la demande reste inchangée. La cause de l'action est l'ensemble des faits et / ou actes juridiques ayant déclenché le litige et que le demandeur invoque pour étayer le droit dont il demande la reconnaissance ou la protection[24].

Le tribunal constate que la Commission vie privée a effectivement émis, le 12.04.2017, une Recommandation d'initiative « complémentaire » n° 03/2017.

Dans la citation du 11.09.215, la Commission vie privée dénonçait « *la collecte et l'utilisation par Facebook de données concernant le comportement de navigation d'utilisateurs et de non-utilisateurs de Facebook en Belgique au moyen de social plug-ins et de cookies* » comme étant une « *violation flagrante de la législation sur le respect de la vie privée, e.a. de la LVP et l'article 129 LCE* ». Elle se base pour ce faire sur le rapport de recherche de 2015, qui était alors disponible et dans lequel l'utilisation de pixels n'était pas encore décrite.

Le fait que Facebook utilisait déjà des pixels à cette époque ne signifie pas que la Commission vie privée en était effectivement informée ou qu'elle était à même d'en évaluer l'impact effectif au moment de la citation (11.09.2015). Il s'avère en effet que la Commission vie privée a seulement fait de nouvelles constatations techniques à partir du 29.11.2016, soit après la citation, à la suite de la modification des pratiques et de la politique de cookies de Facebook, qui ont mis en lumière l'utilisation effective des pixels dans certaines circonstances.

Dans tous les cas, les pixels sont « seulement » une autre technologie, complémentaire, utilisée par Facebook en association avec certains cookies (existants), pour traiter des données à caractère personnel dans le même but (pouvoir proposer des publicités ciblées en fonction du profil et du comportement de l'internaute), d'une façon qui, de l'avis de la Commission vie privée, viole la législation belge de protection de la vie privée. Le tribunal estime par conséquent que l'action relative à l'utilisation de pixels repose sur des faits avancés dans la citation et que la cause de la demande ne s'en trouve en aucune façon modifiée.

L'action relative à l'utilisation de pixels est par conséquent recevable.

[24] cf. en ce sens ; S. MOSSELMANS, "Art. 807 Ger. W." in Comm. Ger., p. 107, n° 12.

4.3. Le fond

29.

La Commission vie privée soutient au fond que le traitement par Facebook de données à caractère personnel d'utilisateur et de non-utilisateurs au moyen de cookies, social plug-ins et pixels viole à la fois la loi vie privée du 8 décembre 1992 et l'art. 129 LCE, et notamment que :

- Facebook n'obtient pas l'autorisation valable pour les traitements litigieux, en violation de l'art. 5 de la loi vie privée et de l'art. 129 LCE, et qu'elle ne peut invoquer un autre motif d'admissibilité en vertu de l'art. 5 de la loi vie privée ;
- les traitements litigieux sont abusifs et excessives aux termes de l'art. 4 de la loi vie privée ;
- Facebook viole les droits des personnes concernées en ne les informant pas préalablement et adéquatement au sens de l'art. 9 de la loi vie privée ;

Le traitement contesté des données à caractère personnel concerne trous catégories d'internautes sur le territoire belge :

1. les détenteurs de compte Facebook (qui ont conclu un contrat avec Facebook) ;
2. les utilisateurs non enregistrés des Services Facebook ;
3. les non-utilisateurs des Services Facebook.

Dans sa recommandation complémentaire du 12.04.2017, la Commission vie privée décrit les pratiques concrètes, qu'elle estime contraires à la loi vie privée belge, comme suit (voir également le rapport technique complémentaire du 24.02.2017) :

« *4. Pratiques et politique d'utilisation des cookies actuelles de Facebook*

A) Contexte et description technique

25. Facebook propose aux propriétaires de sites Internet externes différents modules sociaux, dont
les boutons « J'aime » et « Partager ». Ces modules sociaux permettent aux utilisateurs de Facebook de partager le contenu d'un site Internet externe via le réseau social. Dans le même temps, ils permettent aussi à Facebook de suivre le comportement de navigation tant des utilisateurs que des non-utilisateurs de Facebook sur ces sites Internet externes (ce qu'on appelle le « third-party tracking » ou traçage de tiers).[25]

26. Les pratiques de traçage de Facebook au moyen de modules sociaux diffèrent selon les circonstances. Les constatations techniques sont dès lors divisées selon d'une part les personnes concernées, à savoir les utilisateurs et les non-utilisateurs de Facebook, et d'autre part les différents scénarios (connecté, déconnecté, désactivé ou désinscrit).[26]

---

[25] *Le « suivi » ou « traçage » est ici compris comme la collecte d'informations sur les habitudes de navigation d'internautes sur différents sites Internet. Voir aussi la recommandation 04/2015, points 57-61.*

[26] *Les constatations techniques qui sont résumées ci-après ont été mises en œuvre entre le 29 novembre 2016 et le 23 février 2017. Le rapport technique complet ayant pour titre « Le traçage de Facebook via les modules sociaux » peut être consulté sur https://www.privacycommission.be/sites/privacycommission/files/documents/*

B) Principales constatations vis-à-vis des utilisateurs de Facebook

Utilisateurs connectés

27. Si un utilisateur est connecté sur Facebook et qu'il visite une page Internet avec un module social, Facebook reçoit jusqu'à 12 cookies ainsi que l'URL de la page visitée Les cookies reçus comprennent notamment les 5 cookies d'identification unique suivants : c_user (contient l'ID utilisateur Facebook) ; • datr (identification de navigateur et horodatage) ; • fr (ID d'utilisateur et identificateur de navigateur, horodatage, autres données diverses) ; • lu (ID utilisateur et diverses données de connexion) ; et • sb (identificateur de navigateur et horodatage).[27]

28. Ces constatations confirment que Facebook suit le comportement de navigation des utilisateurs connectés au moyen de modules sociaux en dehors du domaine du réseau social Facebook. D'après le tableau "Browser Cookies", que l'on peut consulter à présent via un hyperlien dans la politique d'utilisation des cookies de Facebook, les cookies précités soutiennent les finalités suivantes :

- *c_user : est utilisé pour authentifier l'identité d'utilisateurs de Facebook ;*
- *datr : est utilisé à des fins de sécurité et d'intégrité du site, pour la récupération de comptes et l'identification des comptes potentiellement piratés ;*
- *fr : est utilisé pour diffuser, mesurer et améliorer la pertinence des publicités ;*
- *Lu : est utilisé pour enregistrer si la personne décide de rester connectée ;*
- *Sb : est utilisé pour vérifier les connexions*

Utilisateurs déconnectés

29. Si un utilisateur est déconnecté de Facebook et qu'il visite une page Internet avec un module social, Facebook reçoit au total 6 cookies avec notamment l'URL de la page visitée. Les cookies reçus comprennent les 4 cookies d'identification unique « fr », « datr », « lu » et « sb ».

30. Ces constatations confirment que Facebook suit le comportement de navigation des utilisateurs déconnectés au moyen de modules sociaux en dehors du domaine du réseau social Facebook.

- Utilisateurs désactivés[28]

31. Si un utilisateur a désactivé son compte et visite une page Internet avec un module social, Facebook reçoit au total 5 cookies avec notamment l'URL de la page visitée. Les cookies reçus comprennent les 4 cookies d'identification unique « fr », « datr », « lu » et « sb ».

32. Ces constatations confirment que Facebook suit le comportement de navigation des

---

rapport_technique_03_2017.pdf.

[27] D'après le tableau « Browser cookies » que Facebook met à disposition via un hyperlien dans sa politique d'utilisation des
cookies (Facebook, « Cookies et autres technologies de stockage » ,
https://www.facebook.com/policies/cookies), consulté pour la dernière fois le 10 février 2016.

[28] Les « utilisateurs désactivés » sont des utilisateurs qui ont temporairement désactivé leur compte mais ne l'ont pas supprimé définitivement

utilisateurs désactivés au moyen de modules sociaux en dehors du domaine du réseau social Facebook.

- Utilisateurs désinscrits

33. Le mécanisme d'opt-out pour les publicités ciblées que Facebook propose aux utilisateurs a été quelque peu modifié depuis la recommandation 04/2015. Alors que les utilisateurs devaient auparavant toujours se désinscrire via le site Internet externe de l'European Interactive Digital Advertising Alliance (www.youroniinechoices.eu), ils peuvent à présent aussi se désinscrire des publicités ciblées via les paramètres de publicité de leur compte Facebook. Facebook conseille toutefois encore aux utilisateurs de se désinscrire aussi via le site Internet externe de l'European Interactive Digital Advertising Alliance.

34. Si un utilisateur s'est désinscrit des publicités ciblées de Facebook (« opted-out ») via les paramétrages de publicité de son compte Facebook et/ou le mécanisme d'opt-out proposé par Facebook de l'European Interactive Digital Advertising Alliance et qu'il visite une page Internet avec un module social, Facebook reçoit les cookies d'identification unique « c_user » (si l'utilisateur est connecté), « datr », « lu », « fr » et « sb ». Selon Facebook, un de ces cookies, à savoir le cookie "fr", est précisément utilisé à des fins publicitaires.[29]

35. Ces constatations confirment que Facebook suit le comportement de navigation des utilisateurs au moyen de modules sociaux en dehors du domaine du réseau social Facebook, qu'ils se soient ou non désinscrits des publicités ciblées.

- Modifications les plus importantes

36. Par rapport à la recommandation n° 04/2015, les constatations techniques à l'égard des utilisateurs sont quasiment identiques. Les modifications les plus importantes sont d'une part l'utilisation d'un cookie d'identification unique supplémentaire, baptisé « sb », et d'autre part la possibilité pour les utilisateurs de se désinscrire des publicités ciblées via l'interface Facebook (bien que les constatations techniques en matière de third-party tracking soient restées inchangées).

C) Principales constatations vis-à-vis des non-utilisateurs de Facebook

37. Lorsqu'un non-utilisateur visite pour la première fois une page Internet faisant partie du domaine facebook.com[30]*, Facebook affiche en haut de la page une bannière cookie comprenant un lien vers la politique d'utilisation des cookies. Facebook ne place pas de cookie lors du chargement de cette page*

38. Facebook place un cookie d'identification unique « datr » d'une durée de vie de 2 ans dès qu'un non utilisateur interagit avec une page Internet faisant partie du domaine facebook.com, par exemple s'il clique dans un champ à compléter ou s'il ouvre une photo. Les exceptions d'interactions qui ne donnent pas lieu au placement du cookie "datr" sont notamment l'ouverture d'un lien vers la politique d'utilisation des cookies (comprenant aussi les liens au sein de cette page) ou la modification de la langue.[31]

---

[29] *Voir Facebook, « Cookies et autres technologies de stockage », https://www.facebook.com/policies/cookies*

[30] *Il ne s'agit pas ici uniquement de la page d'accueil de Facebook, mais par exemple aussi d'une page Facebook de fans, de la page Facebook d'un magasin, de la page Facebook d'un événement (fête, brocante, etc.).*

[31] *Lorsqu'un non-utilisateur change le paramètre de langue, Facebook place le cookie « locale » qui retient la*

39. Lorsque la personne concernée (navigateur) visite par la suite une page Internet avec un module social de Facebook, Facebook reçoit à nouveau ce cookie d'identification unique « datr » à chaque fois avec notamment l'URL de la page visitée.

40. Ces constatations confirment que Facebook suit le comportement de navigation de non-utilisateurs de Facebook au moyen de modules sociaux en dehors du domaine du réseau social Facebook.

41. Par ailleurs, la Commission a constaté que dans certaines circonstances, Facebook place aussi des cookies chez les non-utilisateurs même lorsqu'ils n'ont pas visité une page Internet faisant partie du domaine facebook.com. La Commission a ainsi pu constater que Facebook place un cookie « fr » chez les non-utilisateurs de Facebook lorsqu'ils visitent les sites hln.be, rtbf.be et gezondheid.be, même si la personne concernée n'a jamais visité auparavant un quelconque site Internet de Facebook. Dans les cas observés, le cookie "fr" était chaque fois placé lors du chargement de ce qu'on appelle un « pixel Facebook ».[32] Des recherches complémentaires effectuées par la Commission révèlent que depuis le 1er août 2016, Facebook place un cookie « fr » sur au moins 10.000 sites Internet à partir d'une position de tierce partie

- Modifications les plus importantes

42. Par rapport à la recommandation 04/2015, Facebook ne place plus d'emblée chez les non-utilisateurs le cookie d'identification unique « datr » lors du chargement d'une page Internet faisant partie du domaine facebook.com, ni sur des sites Internet externes (comme le site Internet d'opt-out de l'European Interactive Digital Advertising Alliance) où Facebook se trouve en position de partie tierce.[33] Facebook postpose à présent le placement de cookies jusqu'au moment où le non-utilisateur interagit avec la page Facebook et après avoir affiché la bannière cookie.

43. Il est à noter qu'en Belgique, contrairement à ce qui vaut dans d'autres pays tels que la France, Facebook ne place pas le cookie "fr" au moment des constatations techniques lorsqu'un non-utilisateur interagit avec une page Internet faisant partie du domaine facebook.com, malgré l'intention de Facebook de proposer aussi des publicités ciblées à des non-utilisateurs. Facebook place par contre bel et bien le cookie « fr » lorsque les non-utilisateurs situés en Belgique visitent certains sites Internet de tiers, dont hln.be, rtbf.be et gezondheid.be.

30.

---

préférence de langue et le cookie de session « x-src » qui est utilisé pour les statistiques et les enquêtes.

[32] De tels pixels Facebook constituent de nouveau une technologie que Facebook met à disposition d'exploitants de sites Internet externes. Cette technologie n'apparaît toutefois pas ici comme un bouton ou icône sur le site Internet externe, mais comme un point invisible à l'œil nu : un pixel. Tout comme pour les modules sociaux de Facebook, le pixel Facebook est un élément de code logiciel élaboré par Facebook. Cet élément de code permet d'établir automatiquement une connexion entre le navigateur Internet d'un internaute et les serveurs de Facebook, et ce au moment où l'internaute charge une page Internet sur laquelle ce pixel se trouve. Voir par exemple Facebook, « Guide complet sur la mise en place du pixel Facebook », https://frfr.facebook.com/business/help/952192354843755..

[33] Cf. le point 72 de la recommandation N°01/2015. 25 Voir Facebook, « Bringing people better ads », 26 mai 2016, disponible à l'adresse https://newsroom.fb.com/news/2016/05/bringing-people-better-ads. »

Si Facebook veut suivre le comportement de navigation des détenteurs de compte Facebook, les utilisateurs des Services Facebook non inscrits et ceux qui ne sont pas des utilisateurs du Service Facebook, au moyen de cookies et autres technologies similaires telles que les pixels, pour leur envoyer ensuite de la publicité ciblée, spécifique en fonction de leur comportement, elle doit tenir compte, à l'égard de chacun de ces utilisateurs, les conditions imposées par la loi de protection de la vie privée et la LCE (art. 129), puisqu'elle stocke, à l'aide des techniques utilisées, des informations dans l'équipement terminal (ordinateur, smartphone, etc.) des internautes, après quoi elle y accède à nouveau, quand les utilisateurs naviguent de nouveau sur certains sites web.

Les dispositions législatives pertinentes sont les suivantes (mise en gras par le tribunal).

Art. 4 de la loi relative à la protection de la vie privée du 8 décembre 1992 :

§ 1. 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 § 1.

Art. 5. de la loi relative à la protection de la vie privée

« 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.

Art. 1 §8 de la loi relative à la protection de la vie privée :

« § 8. Par « consentement de la personne concernée », on entend ***toute manifestation de volonté, libre, spécifique et informée****, par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. »*[34]

Art. 129 LCE :

« *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 autorisé uniquement à condition que :*

2° 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 premier* ***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.* »

Art. 9. de la loi relative à la protection de la vie privée :

« *§ 1.* ***Le responsable du traitement ou son représentant****, doit fournir à la personne*

[34] Cf. également art. 2, h de la directive 95/46/CE : « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

concernée auprès de laquelle il obtient les données la concernant et au plus tard au moment où ces données sont obtenues, au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée :

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;

b) les finalités du traitement ;

c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing ;

d) d'autres informations supplémentaires, notamment :

les destinataires ou les catégories de destinataires des données,

- le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,

- l'existence d'un droit d'accès et de rectification des données la concernant ;

sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la commission de la protection de la vie privée.

§ 2. ***Lorsque les données n'ont pas été obtenues auprès de la personne concernée****, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée :*

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;

b) les finalités du traitement ;

c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant *envisagé à des fins de direct marketing dans ce cas, la personne concernée doit être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de direct marketing ;*

d) d'autres informations supplémentaires, notamment :

- les catégories de données concernées ;

- les destinataires ou les catégories de destinataires ;

- l'existence d'un droit d'accès et de rectification des données la concernant ;

sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du

***traitement**, après avis de la Commission de la protection de la vie privée.*

Le responsable du traitement est dispensé de fournir les informations visées au présent paragraphe :

a) lorsque, en particulier pour un traitement aux fins de statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ;

b) lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Le Roi détermine par arrêté délibéré en Conseil des ministres après avis de la Commission de la protection de la vie privée les conditions pour l'application de l'alinéa précédent.

Lorsque la première communication des données a été effectuée avant l'entrée en vigueur de cette disposition, la communication de l'information doit être effectuée, par dérogation à l'alinéa 1er, au plus tard dans un délai de 3 années suivant la date de l'entrée en vigueur de cette disposition. Cette information ne doit toutefois pas être fournie, lorsque le responsable du traitement était exempté de l'obligation d'informer la personne concernée de l'enregistrement des données en vertu des dispositions légales et réglementaires en application le jour précédant la date de l'entrée en vigueur de cette disposition. »

31.

Facebook soutient avant tout qu'elle obtient le consentement des internautes concernés, au sens de l'art. 5 de la loi vie privée et de l'art. 129 LCE, de placer des cookies, puis de procéder au traitement de données à caractère personnel.

Facebook ne peut cependant stocker les informations des internautes ou y accéder - en plaçant des cookies et en les lisant, en combinaison ou pas avec d'autres technologies telles que les pixels - qu'après (i) avoir suffisamment et précisément **informé** les internautes, notamment sur la finalité du traitement, puis (ii) avoir obtenu le **consentement** des internautes pour le stockage ou l'accès aux informations contenues dans son équipement terminal[35]. Facebook doit en apporter la preuve.

[35] voir notamment l'art. 5 de la loi vie privée et de l'art. 19 LCE ; voir également l'Avis 2/2010 sur la publicité comportementale en ligne (« behavioural advertising ») du 22.06.2010 du Groupe de travail « article 29 » sur la protection des données, pièce K.8. du demandeur.

(a)

Facebook souligne qu'elle obtient le consentement requis, pour les détenteurs de compte Facebook et les utilisateurs des Services Facebook non inscrits, par sa bannière cookies. Quand les internautes se rendent pour la première fois sur le domaine Facebook, cette bannière s'affiche avant l'installation du moindre cookie. Le texte de la bannière cookies est à présent le suivant :

« *Nous utilisons des cookies pour personnaliser le contenu, vous proposer un contenu pertinent et offrir une expérience plus sûre. En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations via les cookies. Pour en savoir plus, notamment sur les dispositions prises sur la protection de la vie privée, consultez la Politique d'utilisation des cookies.* ***politique d'utilisation des cookies****.* »

Selon Facebook, cette bannière informe clairement les détenteurs de comptes Facebook et les utilisateurs non inscrits des Services Facebook qu'en cliquant ou en naviguant sur les Services Facebook, ils donnent leur consentement sur la politique de cookies de Facebook pour les différentes finalités mentionnées dans la première phrase de la bannière (« pour personnaliser le contenu, vous proposer un contenu pertinent » et vous « offrir une expérience plus sûre »). Si les détenteurs de compte Facebook et les utilisateurs non inscrits souhaitent obtenir de plus amples informations à ce sujet, ils peuvent cliquer sur le lien « politique d'utilisation des cookies ». Aucun cookie n'est installé à ce stade

Cela signifie que Facebook place effectivement des cookies chez les détenteurs de compte Facebook et les utilisateurs non inscrits quand ils (i) cliquent sur le site web (à l'exception du lien vers la politique d'utilisation des cookies et dans la politique des cookies, notamment les liens tels que le DDR[36] et sauf quand il sélectionne une autre langue), ou qu'ils (ii) continuent de naviguer sur le site web. Facebook déduit par conséquent de ces deux actes le consentement pour placer des cookies à des fins publicitaires et de sécurité.

La Commission vie privée avait constaté que des cookies (« datr ») étaient néanmoins placés (d'une durée de vie de deux années), lorsque l'utilisateur cliquait sur certains liens contenus dans la politique d'utilisation des cookies, donc au moment où il s'informait encore, alors que selon Facebook, il s'agissait d'un « problème » auquel il a depuis lors été remédié.

Facebook relève ensuite avoir lancé, parallèlement à sa bannière cookies mise à jour, sa **politique d'utilisation des cookies** modifiée, que les détenteurs de compte Facebook et les utilisateurs non inscrits des Services Facebook qui fournit des informations complémentaires sur les cookies, notamment un tableau détaillé contenant une indication spécifique du type de cookies utilisés par les Services Facebook (e.a. identification, objet et durée de vie). La politique d'utilisation des cookies informe les détenteurs de compte et les utilisateurs non enregistrés de Facebook sur les éléments suivants :

« Nous pouvons placer des cookies sur votre ordinateur ou votre appareil et recevoir les informations stockées dans des cookies lorsque vous utilisez ou consultez :

- *Les Services Facebook ;*
- *des services proposés par d'autres compagnies Facebook ; et*
- *des services proposés par d'autres entreprises qui utilisent les Services*

[36] La Déclaration des droits et responsabilités de Facebook.

Facebook (comme des entreprises qui intègrent le bouton J'aime ou les services publicitaires de Facebook à leurs sites web ou leurs apps). »

Facebook estime par conséquent obtenir le consentement informé des détenteurs de compte et des utilisateurs non inscrits de Facebook pour installer des cookies lors d'une visite sur Facebook.com et pour recevoir, par l'intermédiaire de ces cookies, des données à des finalités publicitaires, notamment au moyen de social plug-ins et de pixels placés sur des sites web de tiers.

Facebook relève que les détenteurs de compte Facebook donnent un consentement supplémentaire au moment où ils cliquent sur un bouton « inscription », après avoir été informés des éléments pour lesquels ils donnent leur consentement, comme suit : « En cliquant sur Inscription, vous acceptez nos Conditions et indiquez que vous avez lu notre Politique d'utilisation des données, y compris notre Utilisation des cookies ». D'après Facebook, la « Politique d'utilisation des données » et la « Politique d'utilisation des cookies » contiennent tous les éléments nécessaires pour pouvoir donner un consentement informé, notamment :

- une liste mise à jour des cookies utilisés par Facebook (notamment toutes les informations sur la finalité, la durée de vie, etc.) ;
- des informations indiquant que Facebook utilise les cookies à des fins publicitaires, que Facebook.com place et reçoit au moyen de social plug-ins et de pixels placés sur des sites web de tiers ; des informations sur la façon dont Facebook Ireland traite les informations obtenues au moyen des cookies et sur la façon et la raison pour laquelle elle traite des données à des fins publicitaires.

Selon Facebook, il y a systématiquement consentement indubitable, libre et informé.

Facebook indique ensuite qu'elle n'installe un cookie « fr » chez les non-utilisateurs que lorsque ceux-ci naviguent sur un site web de tiers contenant un pixel Facebook, si le non-utilisateur a donné son consentement pour l'installation de cookies, conformément au mécanisme d'autorisation du site web de tiers qu'il consulte.

(b)

En revanche, de l'avis de la Commission vie privée ni la bannière cookies, ni la politique d'utilisation des cookies, ni la politique générale d'utilisation des données de Facebook ne répondent aux exigences imposées par la Directive 95/46/CE, la loi vie privée et la LCE pour qu'il puisse être question de consentement valable.

La Commission vie privée estime que Facebook n'obtient pas, pour le traitement des données à caractère personnel, même après l'introduction de sa bannière cookies et la modification de sa politique d'utilisation des cookies, le consentement valable aux termes des dispositions susmentionnées. Concrètement, la Commission vie privée estime que :

(a) les informations communiquées par Facebook sont (toujours) insuffisantes, de sorte qu'il n'est pas question de consentement « informé » ;
(b) la façon dont Facebook déduit le consentement est défaillante ;
(c) il n'est pas question de consentement libre ;
(d) il n'est pas question de consentement spécifique ;
(e) le mécanisme de contrôle proposé par Facebook est insuffisant et trompeur.

La Commission vie privée avance que lorsque des non-utilisateurs consultent un site web de

tiers sur lequel se trouve un pixel Facebook (invisible), qui permet de suivre le comportement de navigation, sans indiquer qu'ils souhaitent avoir recours aux Services de Facebook, aucun mécanisme d'information (par exemple une bannière) n'est présentée et aucun consentement valable n'est obtenu.

32.

Le tribunal relève que le **consentement « informé »** signifie que l'internaute concerné doit disposer des renseignements nécessaires pour se faire un avis fiable.

Concernant le devoir d'information le considérant 25 de la Directive 2002/58/CE (la directive vie privée et communications électroniques) : « *Lorsque des dispositifs du type précité, tels que des témoins de connexion, sont destinés à des fins légitimes, par exemple faciliter la fourniture de services de la société de l'information, leur utilisation devrait être autorisée à condition que les utilisateurs se voient donner des informations claires et précises, conformément à la directive 95/46/CE, sur la finalité des témoins de connexion ou des dispositifs analogues de manière à être au courant des informations placées sur l'équipement terminal qu'ils utilisent.* » (souligné par le tribunal).

L'avis 15/2011 du groupe de travail « article 29 »[37], approuvé le 13.07.2011 prescrit notamment :

« *Le dernier élément de la définition du « consentement » – mais pas la dernière exigence, ainsi que nous le verrons plus loin – est qu'il doit être informé.*

Les articles 10 et 11 de la directive imposent l'obligation de fournir des informations aux personnes concernées. L'obligation d'information est donc distincte du « consentement », bien qu'elle y soit, dans de nombreux cas, manifestement liée. Si le « consentement » ne suit pas toujours la fourniture des informations (un autre fondement prévu à l'article 7 peut être utilisé), l'information doit toujours précéder le consentement.

Dans la pratique, cela signifie qu'«un consentement … doit être fondé sur l'appréciation et la compréhension des faits et des conséquences d'une action. La personne concernée doit recevoir, de façon claire et compréhensible, des informations exactes et complètes sur tous les éléments pertinents, en particulier ceux spécifiés aux articles 10 et 11 de la directive, tels que la nature des données traitées, les finalités du traitement, les destinataires d'éventuels transferts et ses droits. Cela suppose également la connaissance des conséquences du refus de consentir au traitement des données en question ».

La Commission vie privée relève à juste titre que les informations communiquées par Facebook - de manière disparate - par la **bannière cookies, la Politique d'utilisation des cookies et la Politique d'utilisation des données**, n'indiquent pas suffisamment clairement que Facebook procède « *systématiquement, sans que la personne concernée n'effectue aucune action* » (par exemple sans cliquer effectivement sur « J'aime ») à la collecte de cookies et autres données (simplement) lorsque la personne concernée consulte un site

[37] Ce groupe, constitué en vertu de l'article 29 de la Directive 95/46/CE, est un organe consultatif européen indépendant dédié à la protection des données et de la vie privée, dont les tâches sont décrites à l'article 30 de la Directive 95/46/CE et à l'article 15 de la Directive 2002/58/CE.

web de tiers contenant des social plug-ins Facebook, même si la personne concernée ne détient pas (plus) de compte Facebook ou n'est pas (plus) inscrite sur Facebook.

Or, il est impossible de le déduire de l'utilisation des termes « ***collecter des informations*** *via les cookies » (dans la bannière cookies) et « Nous* ***pouvons*** *placer des cookies sur votre ordinateur ou votre appareil (...) lorsque vous utilisez ou consultez : (...) des services proposés par d'autres entreprises qui utilisent les Services Facebook (comme des entreprises qui intègrent le bouton J'aime ou les services publicitaires de Facebook à leurs sites web ou leurs apps).* » (cf. Politique d'utilisation des cookies), ni de la Politique d'utilisation des cookies.

Comme l'a fait remarquer l'Autorité néerlandaise compétente pour les données à caractère personnel dans son « Rapport definitieve bevindingen - Onderzoek naar het verwerken van persoonsgegevens van betrokkenen in Nederland door het Facebook-concern »* du 21.02.2017 (pièce N.6 du demandeur) le responsable du traitement peut proposer les informations en plusieurs strates (ce que le Groupe de travail « article 29 » encourage d'ailleurs), mais dans ce cas, les informations doivent être compréhensibles et aisément accessibles[38], ce qui n'est pas le cas en l'occurrence. (* traduction libre : Rapport sur les résultats définitifs - Examen du traitement des données à caractère personnel de personnes concernées aux Pays-Bas par le groupe Facebook) Les personnes concernées doivent en effet « fouiller » dans plusieurs pages web pour trouver les informations (alors qu'elles n'ont aucun devoir de recherche), la première strate avec laquelle elles entrent en contact, à savoir la bannière cookies, n'indiquant pas assez clairement à quelle finalité précise les données à caractère personnel - notamment d'ailleurs aussi des « données sensibles » (par exemple concernant les convictions religieuses ou l'orientation sexuelle) - sont collectées, tandis que la strate suivante (e.a. la Politique d'utilisation des cookies et la Politique d'utilisation des données) ne le précisent pas de façon plus aisément compréhensibles et accessible. Dans la mesure où la bannière cookies ne contient pas des informations suffisantes sur l'impact du traitement des données lorsqu'elles naviguent, les personnes concernées ne sont en outre pas davantage invitées à collecter de plus amples informations, e.a. dans la Politique d'utilisation des cookies et la Politique d'utilisation des données.

Toujours à juste titre, la Commission vie privée relève que Facebook ne communique pas d'avantage des informations claires sur la nature des données collectées lorsque la personne concernée visite un site web de tiers contenant des social plug-ins, alors que l'art. 9 §2, d LVP l'exige. Ainsi, la Politique d'utilisation des cookies que Facebook, en plus des cookies, collecte également les « URL » (adresses Internet) des pages web consultées, ce qui lui permet pourtant précisément de suive le comportement de navigation sur les sites web de tiers. Le fait que la Politique d'utilisation des données confère plus d'information à ce sujet sous la rubrique « Quels types d'informations recueillons-nous ? », comme l'affirme Facebook, ne change rien à l'affaire, étant donné ce qui a déjà été exposé ci-dessus à propos

[38] « *Une lecture 'holistique' de toutes les sources d'information possibles (notamment des informations disponibles 'ailleurs dans les Services Facebook') ne répond toutefois pas l'exigence légale selon laquelle les informations essentielles concernant les traitements de données ayant l'impact le plus important sur la vie privée des personnes concernées doivent être décrites de façon claire et compréhensible dans la première strate d'information. En font dans tous les cas partie le fait que le groupe Facebook traite une multitude de données à caractère personnel à des fins publicitaires, notamment des données sur le comportement de navigation et l'utilisation d'apps en dehors du Service Facebook, même quand l'utilisateur est déconnecté* » (traduction libre) (voir pièce N.6 du demandeur, p. 145).

de la communication d'information « en strates ». La politique d'utilisation des cookies n'évoque pas du tout les données collectées ; la Commission vie privée a constaté qu'un non-utilisateur doit franchir pas moins de cinq étapes pour atteindre les informations contenues dans la Politique générale d'utilisation des données, informations qui sont en outre insuffisantes pour permettre à « une personne concernée moyenne » de déterminer de manière univoque quelles informations Facebook collecte précisément au sujet de son comportement de navigation et dans quelles circonstances.

La Politique d'utilisation des données stipule en effet : « *Nous recueillons des informations lorsque vous visitez ou utilisez des sites web et des applications de tiers qui ont recours à nos Services (par exemple, lorsqu'ils incluent nos boutons J'aime ou Se connecter avec Facebook, ou encore lorsqu'ils font appel à nos services de mesure et de publicité). Ceci comprend des informations sur les sites web et les applications que vous consultez, votre utilisation de nos Services sur ces sites web et applications, ainsi que les informations que le développeur ou l'éditeur de l'application ou du site web partagent avec vous ou avec nous* ». À la lecture de ces dispositions, un internaute moyen ne sait pas clairement que lors de chaque navigation sur un site web et chaque utilisation d'une « app » (application) externe au Service Facebook avec lesquels il existe une possibilité d'interaction, Facebook cartographie systématiquement son comportement de navigation pour lui envoyer / autoriser l'envoi de publicités extrêmement ciblées/d'entreprises avec lesquelles la personne concernée n'a jamais eu de contact direct. La Commission vie privée relève que les informations contenues dans la Politique d'utilisation des données n'est pas pertinente pour ceux qui ne détiennent pas de compte, puisque ces derniers sont uniquement présumés accepter la Politique d'utilisation des cookies et pas la Politique d'utilisation des données.

Pour cette même raison, le tribunal a estimé que les informations communiquées par Facebook au sujet des « destinataires ou des catégories de destinataires » des informations collectées ne sont pas assez transparentes et univoques, et qu'elle ne fournit aucune information sur « l'existence d'un droit d'accès et de rectification des données la concernant », comme prescrit par l'art. 9 §2, d LVP.

La position de Facebook, selon laquelle elle serait dispensée de ce dernier devoir d'information, parce que, pour des raisons techniques et (dans le cas du cookie « datr ») pour des raisons de sécurité, il lui serait impossible d'accorder à la personne concernée le droit d'accès et de rectification des données à caractère personnel, ne peut être suivie. Si Facebook souhaite rassembler des données à caractère personnel à des fins commerciales, au moyen de certains cookies et autres technologies, elle est tenue de prévoir les technologies étalonnées pour garantir le droit d'accès et de rectification aux données traitées. L'Avis 2/2010 du Groupe de travail « article 29 », approuvé le 22.06.2010, montre en outre qu'il existait déjà à cette époque des initiatives de fournisseurs de réseaux publicitaires consistant à donner accès aux catégories de centres d'intérêts auxquelles les personnes concernées ont été associées sur la base du numéro d'identification du cookie, et que ces nouveaux outils permettaient aussi à ces personnes de modifier ou de supprimer ces données (voir pièce K.8. du demandeur, p. 24-25).

Les considérants suivants de la Directive 95/46/CE prescrivent en outre à cet égard :

« *(41) considérant que toute personne doit pouvoir bénéficier du droit d'accès aux données la concernant qui font l'objet d'un traitement, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement; que, pour les mêmes raisons, toute personne*

doit en outre avoir le droit de connaître la logique qui sous-tend le traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1; que ce droit ne doit pas porter atteinte au secret des affaires ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel; que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée ;

(42) considérant que les États membres peuvent, dans l'intérêt de la personne concernée ou en vue de protéger les droits et libertés d'autrui, limiter les droits d'accès et d'information; qu'ils peuvent, par exemple, préciser que l'accès aux données à caractère médical ne peut être obtenu que par l'intermédiaire d'un professionnel de la santé ;

(43) considérant que des restrictions aux droits d'accès et d'information, ainsi qu'à certaines obligations mises à la charge du responsable du traitement de données, peuvent également être prévues par les États membres dans la mesure où elles sont nécessaires à la sauvegarde, par exemple, de la sûreté de l'État, de la défense, de la sécurité publique, d'un intérêt économique ou financier important d'un État membre ou de l'Union européenne, ainsi qu'à la recherche et à la poursuite d'infractions pénales ou de manquements à la déontologie des professions réglementées; qu'il convient d'énumérer, au titre des exceptions et limitations, les missions de contrôle, d'inspection ou de réglementation nécessaires dans les trois derniers domaines précités concernant la sécurité publique, l'intérêt économique ou financier et la répression pénale; que cette énumération de missions concernant ces trois domaines n'affecte pas la légitimité d'exceptions et de restrictions pour des raisons de sûreté de l'État et de défense ; »

La Commission vie privée remarque en outre, à juste titre, que Facebook ne fournit pas davantage d'information sur la durée de conservation des informations collectées à l'aide des cookies et social plug-ins notamment, alors que le groupe de travail « article 29 » estime que la fourniture de ces informations est nécessaire (voir Document de travail 02/2013, adopté le 02.10.2013, pièce K.11 du demandeur).

À l'instar de l'Autorité néerlandaise compétente pour les données à caractère personnel dans son Rapport du 21.02.2017, la Commission vie privée belge avance, à raison, dans la présente procédure, que Facebook fournit des informations trompeuses sur les circonstances dans lesquelles elle utilise les cookies :

« *Nous utilisons des cookies si vous avez un compte Facebook, si vous utilisez les Services Facebook, y compris notre site web et nos apps (que vous soyez inscrit(e) ou connecté(e) ou non), ou si vous consultez d'autres sites web et apps qui ont recours aux Services Facebook (y compris le bouton J'aime et nos outils publicitaires). (...)* ». Si les utilisateurs (non-)inscrits et (non-)connectés peuvent en déduire que leur comportement de navigation est suivi lorsqu'ils utilisent le site et les apps Facebook (par la phrase « que vous soyez inscrit(e) ou connecté(e) ou non »), il n'apparaît plus clairement que c'est également le cas lorsqu'ils consultent d'autres sites web et apps utilisant des Services Facebook (où cette phrase ne figure pas).

Enfin, la Commission vie privée avance à juste titre que le tableau « Browser cookies », qui peut être consulté à partir de la Politique d'utilisation des cookies et contient un récapitulatif des divers cookies, leur durée de vie, leur contenu et leur finalité, n'est pas totalement correct, puisqu'il ne mentionne par exemple pas la finalité publicitaire supplémentaire du cookie « c_user », de sorte que l'exigence de transparence n'est pas respectée.

33.

Le tribunal vérifie ensuite si la façon dont Facebook estime obtenir le consentement pour le traitement des données à caractère personnel est défaillant, parce qu'il **n'est pas univoque, libre et spécifique**, comme l'affirme la Commission vie privée.

Comme indiqué, l'art. 1 §8 de la loi vie privée définit le « consentement » comme toute expression de volonté libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte le traitement des données à caractère personnel. Cette définition a été puisée dans l'art. 2, h de la directive 95/46/CE.

« Spécifique » signifie que l'expression de volonté doit porter sur un traitement ou une catégorie de traitement spécifique et qu'il ne peut dès lors être obtenu en vertu d'une autorisation générale ou pour une série ouverte d'activités de traitement.

L'Avis 15/2011 du Groupe de travail article 29, approuvé le 13.07.2011, précise en la matière qu'un consentement n'est valable que dans un contexte limité, que les divers éléments du traitement doivent être décrits clairement et que le consentement est requis pour chaque élément. Le consentement ne peut être présumé porter sur « toutes les finalités légitimes » du responsable, mais uniquement sur le traitement qui, vu sa finalité, est raisonnable et nécessaire. En ce sens, il est également possible d'obtenir un consentement unique pour plusieurs traitements (par exemple le consentement pour l'installation du cookie englobe aussi le consentement pour la lecture ultérieure de ce cookie), pour autant que la personne concernée pouvait raisonnablement s'attendre à ce que ces traitements aient lieu (voir pièce K.9 du demandeur, p. 19-20).

« Libre » signifie que la personne concernée doit pouvoir exprimer librement sa volonté et qu'elle doit être véritablement en mesure d'exercer un choix. Aux termes de l'Avis 15/2011 du Groupe de travail article 29, approuvé le 13.07.2011, un consentement ne peut être valable que « s'il n'y a pas de conséquences négatives importantes pour la personne concernée si elle ne donne pas son consentement. Si les conséquences du consentement limitent la liberté de choix, il ne peut être question de consentement « libre » (voir pièce K.9 du demandeur, p. 14-15).

Cet avis précise également ce qui suit quant à l'accès aux réseaux sociaux :

« *L'accès aux services d'un réseau social est souvent subordonné à l'acceptation de différents types de traitement de données à caractère personnel. L'utilisateur peut être invité à accepter de recevoir de la publicité comportementale (behavioural advertising) pour pouvoir s'inscrire sur un réseau social, sans autre précision ni autre possibilité. Compte tenu de l'importance qu'ont pris certains réseaux sociaux, certaines catégories d'utilisateurs (comme les adolescents) consentiront à recevoir de la publicité comportementale pour éviter le risque d'être exclus de certaines interactions sociales. Or l'utilisateur devrait être en mesure de donner un consentement libre et spécifique à la réception de publicités comportementales, indépendamment de son accès au réseau social. Une fenêtre distincte pourrait être utilisée pour proposer cette possibilité à*
l'utilisateur Le réseau social offre la possibilité d'utiliser des applications externes. Dans la pratique, il est fréquent que l'utilisateur ne puisse pas utiliser une application s'il n'accepte pas la transmission de ses données au développeur de l'application à différentes fins, y compris la publicité comportementale et la revente à des tiers. Étant donné que l'application

peut fonctionner sans qu'il soit nécessaire de transférer des données à son développeur, le groupe de travail recommande de «détailler» le consentement de l'utilisateur, c'est-à-dire de lui demander un consentement distinct pour la transmission de ses données au développeur à ces différentes fins. Divers dispositifs, comme des fenêtres contextuelles, pourraient être utilisés pour proposer à l'utilisateur la possibilité de sélectionner l'utilisation des données à laquelle il consent (transmission au développeur, services à valeur ajoutée, publicité comportementale, transmission à des tiers, etc.). ».

« Indubitable » signifie que la procédure relative à l'obtention du consentement ne doit laisser aucun doute quant à l'intention de la personne concernée de donner son consentement au traitement des données. Cela implique également, selon l'Avis 15/2011 du Groupe de travail article 29, approuvé le 13.07.2011 (pièce K.9 demandeur, p. 24-25), que des procédures solides doivent être mises en place pour que les personnes concernées donnent leur consentement exprès et clair ou qui aboutissent à un consentement implicite clair. Le responsable du traitement des données doit produire la preuve qu'il a obtenu le consentement. Dans un environnement en ligne, le consentement indubitable peut par exemple être donné au moyen d'une case à cocher sur un formulaire en ligne (ou dans un « *pop-up* »[39]). Le Groupe de travail « article 29 » sur la protection des données estime que le simple fait de naviguer sur un site web et d'y jouer à un jeu, sans que la lecture d'un message à propos du traitement des données à caractère personnel dans un autre lien soit nécessaire pour jouer, ne peut être considéré comme un consentement pour le traitement de ces données à d'autres fins que de jouer à ce jeu (par exemple à des fins publicitaires).

34.

Le tribunal constate que les détenteurs de compte Facebook donnent expressément leur consentement pour l'installation de cookies au moment où ils cliquent sur un bouton « Inscription », après l'affichage de la mention suivante : « *En cliquant sur Inscription, vous acceptez nos Conditions et indiquez que vous avez lu notre Politique d'utilisation des données, y compris notre Utilisation des cookies* ».

Les non-détenteurs de compte qui naviguent pour la première fois sur le site web de Facebook, voient s'afficher la bannière cookie de Facebook : « *En cliquant sur le site ou en le parcourant, vous nous autorisez à collecter des informations via les cookies* ». Le tribunal est d'avis que le fait de continuer à naviguer sur un site web peut générer en soi le consentement valable de la personne concernée pour le traitement de données à caractère personnel. Selon la Commission vie privée, le consentement libre de ceux qui ne détiennent pas de compte Facebook est mis en péril, car la seule façon de ne pas octroyer leur consentement consiste à quitter le site web Facebook, ce qui a pour eux des conséquences négatives, puisque, non seulement ils ne peuvent pas accéder au réseau social (ce qui peut constituer une exclusion sociale partielle, surtout pour les jeunes), mais pas davantage à un grand nombre de pages web d'entreprises et d'autres entités qui ne disposent pas de leur propre page mais sont hébergées sur une page Facebook. Facebook fait remarquer à raison qu'elle est un service commercial privé, qui est précisément financé par les revenus publicitaires. Il ne faut toutefois pas oublier qu'en sa qualité de réseau social, elle jouit

[39] Pop-up = (nouvelle) fenêtre qui s'affiche à l'écran.

d'une position dominante mondiale dans la vie sociale (notamment des jeunes). Par conséquent, elle doit non seulement d'offrir une transparence totale sur le traitement des données qu'elle effectue, mais on peut s'attendre à ce qu'elle examine la possibilité d'offrir un contenu web (par exemple la page Facebook de certaines organisations), sans que le visiteurs doive consentir à l'installation de « tous les cookies » (cf. considérant 25 de la Directive 46/95 : « *L'accès au contenu d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à des fins légitimes* »).

Dans tous les cas, le tribunal constate que tant les détenteurs de compte Facebook que les utilisateurs non inscrits doivent accepter l'installation de tous les cookies et pas seulement une partie d'entre eux. Comme indiqué précédemment, cela pose problème, car Facebook ne les informe pas assez clairement qu'elle collecte systématiquement des données à caractère personnel à leur sujet lorsqu'ils consultent un site web de tiers contenant des social plug-ins Facebook, même s'ils ne détiennent pas de compte Facebook ou qu'ils ne sont plus connectés à Facebook.

Le fait que par sa Politique d'utilisation des cookies, Facebook accorde la possibilité de plusieurs opt-out (pour les détenteurs de compte Facebook)[40] et qu'elle invoque également la possibilité de se désinscrire de la réception de publicités en ligne basées sur l'intérêt en passant par « le site web du European Interactive Digital Advertising Alliance », par « les paramètres de votre appareil mobile » et les « paramètres des cookies dans votre navigateur » (pour tous), ne change rien à la cause. Des constatations techniques ont en effet montré que Facebook collecte toujours des informations sur le comportement de navigation des personnes concernées, même lorsqu'elles ont utilisé l'un des choix mentionnés (voir nouveau rapport technique, pièce A.5., p. 17 e.s.), de sorte que la possibilité offerte de gérer l'utilisation des cookies à des fins publicitaire porte uniquement sur leur *utilisation ultérieure*. De plus, tous les « navigateurs » ou « paramètre des appareils mobiles » ne sont pas configurés de façon à ce que l'utilisateur puisse accepter certains cookies et pas d'autres. C'est pourquoi le Groupe « article 29 » sur la protection des données plaide pour un mécanisme de consentement par opt-in préalable, par lequel la personne concernée doit activement donner son consentement avant que le cookie soit installé, ce qui est effectivement préférable suivant la perspective d'une protection efficace de la vie privée.

La Commission vie privée relève en outre que Facebook, en dépit des « mécanismes de contrôle » proposés, place toujours le cookie « fr » au moyen de son pixel Facebook pour le collecter ensuite par ses social plug-ins, même si la personne concernée a expressément fait savoir qu'elle ne souhaite pas recevoir de publicité ciblée en fonction de son comportement, ce qui est contraire à ses prévisions raisonnables (voir nouveau rapport technique, pièce A.5., p. 17 e.s.). Les nouvelles constatations techniques montrent que c'est une pratique courante depuis le 01.08.2016 sur les 10.000 sites web les plus fréquentés (voir nouveau rapport technique, pièce A.5., p. 11).

[40] En (i) gérant les intérêts au sein de la fonction « préférences publicitaires », (ii) « bloquer les publicités en ligne basées sur l'intérêt au moyen des paramètres publicitaires liés au compte » et (iii) en interrompant l'utilisation des préférences publicitaires en désactivant « Audience Network » de Facebook à l'aide des paramètres publicitaires liés au compte.

Lorsque des non-utilisateurs consultent un site web de tiers sur lequel se trouve un pixel Facebook (invisible), qui permet de suivre le comportement de navigation, sans indiquer qu'ils souhaitent avoir recours aux Services de Facebook, aucun mécanisme d'information (par exemple une bannière) n'est présenté. Les canaux d'information répandus de Facebook (Bannière cookies, Politique d'utilisation des cookies et Politique d'utilisation des données) n'abordent pas davantage les cookies, pixels et social plug-ins de tiers.

Selon Facebook, dans ce cas, le cookie « fr » est uniquement placé lorsque la personne concernée a donné son consentement pour l'installation des cookies selon le mécanisme de consentement utilisé par le site web du tiers. Facebook relève :

- que selon la jurisprudence de la Cour de justice, le responsable du traitement peut invoquer le consentement obtenu par un tiers pour le traitement ultérieur des données à caractère personnel ;
- qu'il lui est techniquement impossible de placer des informations ou un mécanisme de consentement sur un site web géré par un tiers ;
- qu'elle respecte ses obligations en tant que fournisseur de pixels Facebook pour les sites web de tiers en concluant avec ces derniers des contrats contraignants et en exigeant (par l'intermédiaire des conditions générales) qu'ils « *prévoient une communication solide et suffisamment visible afin d'obtenir le consentement nécessaire des utilisateurs* », notamment « *une communication claire et bien visible, sur chaque page web sur laquelle des outils Facebook sont utilisés, associée à une déclaration claire* »[41] et en leur rappelant régulièrement leurs obligations ;
- qu'elle impose aux concepteurs d'application web de tiers de faire une « communication adéquate » sur le fait que « *les tiers, notamment Facebook, peuvent utiliser des cookies, pixels espions et autres technologies de stockage pour rassembler ou recevoir des informations de vos sites web, apps et ailleurs sur l'Internet* ».[42]

La Commission vie privée relève, à raison, que puisque Facebook détermine à la fois la finalité et les moyens du traitement, elle demeure le responsable du traitement des données à caractère personnel au moyen de pixels, et qu'elle est dès lors tenue, ainsi que les propriétaires des sites web de tiers, de respecter les obligations légales. Le tribunal constate que dans tous les cas, une fois encore, les déclarations imposées aux tiers par Facebook ne contiennent pas d'informations suffisantes sur le fait que Facebook suit systématiquement le comportement de navigation des visiteurs de ces sites web au moyen de ses cookies et pixels, même s'ils n'ont pas de compte Facebook ou qu'ils ne sont pas connectés, de sorte que l'on ne peut en déduire un consentement valable.

Facebook ne démontre par conséquent pas qu'elle communique, que ce soit par l'intermédiaire des propriétaires de sites web de tiers ou autrement, des informations suffisantes aux non-utilisateurs de Facebook, ni qu'elle obtient leur consentement valable.

Le tribunal conclut que dans tous les cas décrits, Facebook n'obtient pas le consentement valable aux termes de l'art. 5. a de la loi vie privée et de l'art. 129 LCE pour le traitement des données contesté.

[41] cf. pièce 73 des défenderesse, traduction libre du texte anglais par les défenderesses.
[42] cf. pièce 73 des défenderesse, traduction libre du texte anglais par les défenderesses.

35.

La Commission vie privée avance ensuite que Facebook ne peut davantage invoquer un autre motif d'admissibilité prévu à l'art. 5 de la loi vie privée et que les traitements de données contestés ne répondent pas aux exigences de qualité contenus dans l'art. 4 de la loi vie privée, (qui doivent dans tous les cas être respectés, quand bien même le consentement valable serait obtenu).

Facebook estime quant à elle que les exigences de qualité de l'art. 4 de la loi vie privée sont remplies et que le traitement contesté des données à caractère personnel est également admissible pour les motifs suivants :

- pour les détenteurs de compte Facebook : le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie (art. 5. b de la loi vie privée) ;
- le traitement est nécessaire pour défendre l'intérêt légitime de Facebook (Ireland) (art. 5. F de la loi vie privée) ;
- l'enregistrement technique des informations ou de l'accès aux informations stockées dans l'équipement terminal est strictement nécessaire pour fournir un service demandé expressément par l'abonné ou l'utilisateur final (art. 129 LCE).

Facebook relève à cet égard la nécessité et l'obligation, aux termes de l'art. 16 §4 de la loi vie privée[43] pour sécuriser le service Facebook, que plus de 2 milliards de personnes utilisent chaque mois pour partager des informations personnelles, à l'aide d'un système de sécurité solide et sophistiqué sans précédent (au moyen de cookies de sécurité tels que « datr », renforcé par le cookie « sb »). Selon Facebook, à la lumière de la sécurité nécessaire, toute intrusion éventuelle dans les intérêts de la vie privée des utilisateurs non inscrits est minimale, à plus forte raison puisque :

- les cookies « datr » et « sb » sont des séries aléatoires, associées à un navigateur ou à un appareil et pas à une personne, de sorte que Facebook ne peut identifier les utilisateurs individuels non inscrits ;
- Facebook ne conserve pas d'informations sur l'interaction entre le cookie « sb » d'une part, et les plug-ins et pixels Facebook d'autre part, et elle ne conserve ces informations pour le cookie « datr » que pendant 10 jours.

À cet égard, Facebook relève également que le cookie « c_user » et le cookie « xs » (et le cookie « lu » qui n'est plus utilisé) jouent un rôle déterminant dans le fonctionnement correct et efficace du service Facebook dans la facilitation de la prestation de service aux détenteurs de compte Facebook, tandis que leur durée de vie est limitée à 90 jours. Dans la mesure où ces cookies sont conçus pour contribuer au processus d'authentification et de connexion des détenteurs de compte Facebook, ils ne sont jamais placés sur le navigateur

[43] Art. 16 §8 de la loi vie privée : « *Afin de garantir la sécurité des données à caractère personnel, le (responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent 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.* »

d'utilisateurs non inscrits et des non-utilisateurs, du moins selon Facebook.

Pour ce qui est du cookie « fr », Facebook affirme qu'il est également utilisé à des fins légitimes, à savoir pour de la publicité basée sur le comportement de navigation, des mesures et l'optimisation, qui sont le cœur de l'expérience utilisateur sur laquelle comptent les détenteurs de compte Facebook et ses utilisateurs non inscrits. Selon Facebook, ces personnes souhaitent que le réseau social leur fournisse le contenu le plus pertinent, ce qu'elle peut faire grâce aux revenus publicitaires, sans que les personnes concernées doivent payer pour ce faire. Dans ce cas également, Facebook affirme ne pas être à même d'identifier les utilisateurs individuels non inscrits et les non-utilisateurs à l'aide du cookie « fr », parce que pour eux (contrairement aux détenteurs de compte Facebook), ce cookie contient uniquement une série de signes alphanumériques qui ne peuvent être reliés à leur adresse IP qu'au moyen de journaux d'impression (notamment les plug-ins sociaux et les pixels sur les sites web de tiers). Enfin, Facebook évoque également la possibilité « d'opt-out » et la durée de vie limitée du cookie « fr » (90 jours).

36.

La Commission vie privée ne conteste pas que Facebook a un devoir de sécurité à l'égard des données à caractère personnel qu'elle traite, ce qui constitue un intérêt légitime aux termes de l'art. 5. F de la loi vie privée, mais elle relève à raison que le traitement envisagé doit être « nécessaire » pour réaliser cet intérêt et qu'il doit primer sur les droits et libertés fondamentales de la personne concernée. « Nécessaire » signifie dès lors que l'intérêt légitime ne peut être atteint ou seulement d'une façon disproportionnellement plus complexe en l'absence du traitement de données concerné.

Le tribunal rejoint la position de la Commission vie privée, selon laquelle la collecte systématique de données à caractère personnel d'utilisateurs et de non-utilisateurs au moyen de social plug-ins placés sur les sites web de tiers n'est pas nécessaire (encore moins « strictement nécessaire » aux termes de l'art. 129 LCE), du moins non-proportionnelle pour atteindre l'objectif de sécurité, et que le même raisonnement vaut pour le motif d'admissibilité invoqué, visé à l'art. 5.b de la loi vie privée, à l'égard des détenteurs de compte Facebook (« traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie »).

De plus, l'art. 4 de la loi vie privée cité précédemment requiert notamment que les données à caractère personnel :

- soient traitée loyalement et licitement (principe de licéité) ;
- 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 (le principe de finalité).
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement (principe de proportionnalité) ;

Pour qu'un traitement soit loyal, il faut que les données soient obtenues en toute transparence, qu'elles ne soient pas conservées plus longtemps que de nécessaire et que le traitement ultérieur ne soit pas contraire aux prévisions raisonnables de la personne

concernée[44]. La Commission vie privée relève, à juste titre, que les informations défaillantes, telles qu'elles sont décrites précédemment, entravent non seulement le consentement valable, mais aussi le traitement loyal des données à caractère personnel, puisque Facebook place et collecte, sans en informer suffisamment les internautes, systématiquement et sans qu'ils ne posent d'acte (par exemple en partageant le contenu d'une page web à l'aide du bouton « Partager » ou en cliquant sur « J'aime »), des cookies et autres données, à des fins publicitaires, quand les internautes naviguent sur un site web d'un tiers sur lequel un social plug-in Facebook a été placé. Pour le reste, le tribunal renvoie à ce qui a déjà été exposé précédemment dans le cadre du « consentement informé ».

Le fait que Facebook, en dépit des « mécanismes de contrôle » décrits ci-avant, place encore le cookie « fr » au moyen de son pixel Facebook pour le collecter ensuite par ses social plug-ins, même si la personne concernée a expressément fait savoir qu'elle ne souhaite pas recevoir de publicité ciblée en fonction de son comportement, est en outre, comme exposé ci-avant, contraire à ses prévisions raisonnables et à l'art. 129 LCE.

Le tribunal suit en outre la position de la Commission vie privée, selon laquelle, dès que Facebook a placé les cookies contestés, persistants et d'identification unique (e.a. « c_user », « xs », « datr », « sb », « fr » et « lu »), la *collecte* de données à caractère personnel au moyen de cookies et de plug-ins est superflue (vu les finalités pour lesquelles elles sont traitées) dans les cas suivants :

- pour les cookies utilisés à des fins publicitaires (cookies « fr ») : dès que la personne concernée a expressément fait savoir qu'elle ne souhaitait plus recevoir de publicité sur la base de son comportement de navigation (auquel cas le simple intérêt économique de Facebook ne peut justifier cette ingérence dans la vie privée) :
- pour les cookies utilisés à des fins de sécurité (par exemple les cookies « datr » et « sb ») : quand Facebook les collecte dans la « position de tiers », soit sur des sites qui ne font pas partie du domaine facebook.com, sans que la personne concernée ne clique sur le social plug-in, étant donné :
  - qu'il est possible de proposer des social plug-ins qui n'envoient pas d'informations avant que le visiteur du site web de tiers ne tente d'utiliser ce social plug-in (ce que Facebook faisait d'ailleurs jusqu'en mars 2015) ;
  - la collecte systématique de cookies de sécurité n'est pas une mesure de sécurité suffisante, car elle peut aisément être contournée par des personnes ayant de mauvaises intentions et disposant de l'expertise requise ; de plus, en l'occurrence, il s'agit précisément de la collecte de données lors de la navigation sur des sites web de tiers hors du domaine Facebook, sans que cette dernière ne démontre qu'une attaque de la plate-forme Facebook pourrait se produire au moyen de plug-ins qui ne sont pas utilisés par des internautes qui accèdent à une page en dehors du domaine Facebook.
  - la considération des intérêts penche en faveur du visiteur du site web de tiers, étant donné la nature de l'ingérence (qui permet de collecter des informations sensibles, par exemple sur la santé ou les convictions politiques des personnes), son ampleur (les plug-ins sont présents sur un très grand nombre de sites web) et leur durée (les cookies « datr » et « sb » ont une durée de pas moins de deux

[44] Voir aussi D. DE BOT, Verwerking van persoonsgegevens, Anvers, Kluwer, 2001, p. 115.

ans, sauf si la personne concernée - détentrice ou pas de compte Facebook - les supprime activement). Le fait que Facebook ne conserve pas, ou seulement pendant une durée limitée (cookie « datr »), les informations obtenues au moyen des social plug-ins ne change rien à l'affaire, puisque le comportement de navigation sera encore suivi et pourra être collecté pendant deux ans. L'argument selon lequel Facebook ne serait pas à même d'identifier les utilisateurs individuels non inscrits, au motif que les cookies sont associés à un seul navigateur ou appareil déterminé et pas à une personne, n'est pas pertinent. Il a déjà été décidé précédemment qu'il s'agissait bien ici de « données à caractère personnel ». Dans la pratique, Facebook peut effectivement identifier les utilisateurs du navigateur, à l'aide du navigateur et de l'identifiant unique du cookie, puisque, dans leur grande majorité, les ordinateurs portables et smartphones (et donc aussi le navigateur) sont utilisés par une seule personne.

- pour les cookies utilisés dans le but de vérifier l'identité des utilisateurs de Facebook (par exemple « c_user » et « xs ») ou pour enregistrer le choix de la personne de rester connecter : quand Facebook les collecte dans la « position de tiers », soit sur des sites web qui ne font pas partie du domaine facebook.com, sans que la personne concernée ne clique sur le social plug-in pour la même raison.

37.

Facebook avance que la Commission vie privée ne n'aurait pas fait preuve d'indépendance dans son dossier, car d'une part, elle aurait agi sur instruction et à la demande d'un membre du gouvernement belge (l'ancien Secrétaire d'État à la Protection de la vie privée, Bart Tommelein) et, d'autre part, elle viserait uniquement Facebook et pas d'autres réseaux publicitaires et entreprises en ligne (belges) ayant recours à des technologies et des mécanismes de consentement similaires. Par conséquent, selon Facebook, tous les actes de la Commission belge de la vie privée, en ce compris la présente procédure, sont, dès le début, entachés de nullité, de sorte que pour cette seule raison déjà, l'action doit être déclarée non fondée.

Le tribunal estime toutefois que rien ne montre que la Commission vie privée n'aurait pas agi en toute indépendance. Aux termes de la loi vie privée du 8 décembre 1992, la Commission vie privée est un organe indépendant, instaurée auprès de la Chambre des représentants. Toute personne peut déposer une plainte auprès de la Commission vie privée qui a le droit, en vertu de la loi, d'émettre des avis ou recommandations de sa propre initiative (ou à la demande du Gouvernement, du Parlement ou des parlements régionaux). Le simple fait qu'un membre du gouvernement (le Secrétaire d'État à la protection de la vie privée) - à l'instar des internautes, des médias et du Parlement - ait manifesté de vives inquiétudes quant aux pratiques de Facebook, ne signifie pas que la Commission vie privée aurait agi sur ses instructions. Facebook n'apporte pas la moindre preuve de ses affirmations.

Il appartient en outre au pouvoir discrétionnaire de la Commission vie privée de déterminer sur quelles entreprises elle estime opportun de mener une enquête et d'entreprendre d'éventuelles démarches judiciaires. Le tribunal estime que rien ne prouve que la Commission vie privée discriminerait de la sorte Facebook au regard d'autres réseaux publicitaires (belges) comparables, sans compter que l'on peut s'interroger sur l'existence

d'autres réseaux publicitaires « comparables » à Facebook, vu la position dominante (mondiale) de cette dernière.

38.

Facebook avance aussi que les **mesures exigées** par la Commission vie privée ne trouvent aucun fondement, explicite ou implicite, dans la loi vie privée.

Selon Facebook, la reprise par le tribunal des mesures exigées au point A (cesser d'installer et de collecter des cookies sans que les conditions imposées soient respectées), susciterait inévitablement des problèmes d'interprétation, de sorte qu'aucune astreinte ne peut y être associée.

D'après Facebook, les mesures sous B (cesser de communiquer des informations trompeuses) et C (supprimer toutes les données contraires à la législation de protection de la vie privée), ne peuvent être ordonnées par le tribunal civil.

Facebook estime en outre que les mesures de réparation sollicitées par la Commission vie privée équivaudraient à un mécanisme de sanction et d'amende qui n'est pas prévu par la loi et qui concerneraient uniquement Facebook. De plus, cette dernière estime que la Commission vie privée demande au tribunal d'adopter une décision de nature réglementaire, ce qui constituerait une violation de l'art. 6 C. jud.

Cet art. 28.3 de la Directive 95/46/CE, qui prescrit que toute autorité de contrôle est compétente pour « ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire », ne permet pas de déduire que la compétence d'ester en justice se limiterait à demander un jugement purement déclaratif ou interprétatif, à plus forte raison dans une matière qui touche aux droits fondamentaux de la personne concernée.

Comme indiqué précédemment, le tribunal estime qu'en vertu de la législation belge actuelle, la Commission vie privée ne peut exercer utilement ses compétences d'autorité de contrôle belge que si elle peut demander au juge belge qu'il adopte des mesures, conformément à la législation belge.

La Commission vie privée relève à juste titre que l'historique de l'art. 32 §3 de la loi vie privée, ainsi que les travaux préparatoires de la loi vie privée du 8 décembre 1992 (voir e.a. les pièces J.1 et J.5 du demandeur) que l'intention du législateur était que le juge puisse adopter, dans le cadre d'une action de la Commission vie privée, une décision « contraignante » et donc exécutoire en complément nécessaire à la compétence consultative de la Commission vie privée qui, en vertu de la législation belge, ne peut imposer des mesures de réparation telles qu'un ordre « de faire supprimer les données » (voir pièce J.1 du demandeur, p. 9) ou - dans le prolongement - un ordre de ne plus traiter les données à caractère personnel en violation de la législation vie privée.

Surabondamment, le tribunal relève que le Président de ce même tribunal a d'ores et déjà décidé ce qui suit dans son ordonnance en référé du 09.11.2015 (traduction libre) :

« *L'action ne tend pas à entendre prononcer une interdiction de constituer un profil à des fins publicitaires, mais à contraindre les défenderesses à respecter les obligations qui leur incombent en leur qualité de responsable du traitement lorsqu'elles collectent les données du cookie datr chez les non-utilisateurs de Facebook au moyen des social plug-ins placés sur*

les sites web de tiers. Elles incluent en effet l'obligation pour les défenderesses de mettre elles-mêmes fin à la violation du principe de proportionnalité.

De plus, il s'agit de violations de très grande ampleur : il ne s'agit pas de la seule violation du droit fondamental d'une personne, mais d'un énorme groupe de personnes. La Belgique compte en effet un nombre incalculable d'internautes qui ne détiennent pas de compte Facebook, mais qui aboutissent t de temps à autre sur une page web du domaine facebook.com, en conséquence de quoi, un cookie datr Facebook est placé à leur insu sur leur ordinateur. D'autre part, le nombre de sites web sur lesquels les social plug-ins Facebook sont présents se compte en millions, de sorte qu'il est pratiquement impossible d'y échapper. Il s'agit souvent d'informations très sensibles qui dévoilent par exemple la santé, les convictions religieuses, l'orientation sexuelle ou les convictions politiques.

Le fait que les défenderesses collectent des données sur le comportement de navigation de millions de résidents en Belgique ayant décidé de ne pas devenir membre du site de réseau social Facebook constitue une violation manifeste de la loi vie privée, indépendamment de l'usage qu'elle fait des données.

Dans la mesure où la violation des articles 4§l et 5 de la loi vie privée touche à l'ordre public belge, la mesure sollicitée n'est pas disproportionnée. »

Le tribunal ne peut que suivre cet avis.

Il est exact que l'on ne peut demander au tribunal d'expliquer une disposition légale sans l'appliquer à un cas concret (art. 6 C. jud). Le tribunal constate toutefois qu'il a été saisi à la suite de pratiques concrètes de Facebook, constatées par la Commission vie privée et qui, comme le confirme le tribunal dans le présent jugement, sont contraires à la législation belge de protection de la vie privée, de sorte qu'il peut adopter des mesures visant à mettre fin à ces violations concrètes.

39.

Le tribunal ordonne par conséquent de cesser d'installer les cookies « c_user », « xs », « datr », « sb », « fr » ou « lu » (etc.) et de les collecter, tant qu'elle n'aura pas rendu sa politique et ses pratiques conformes à la législation belge sur la vie privée, telle que décrite concrètement dans le dispositif du présent jugement.

Contrairement à ce que soutient Facebook, cela ne pose pas de problème d'interprétation. Dans ce jugement, le tribunal a confirmé la position de la Commission vie privée sur les diverses violations de la loi vie privée, comme indiqué dans ses recommandations. Il appartient à Facebook de s'adresser à la Commission belge de la vie privée et elle est toujours libre de se concerter sur le sujet avec cette dernière.

Le tribunal ordonne également de cesser de fournir des informations qui pourraient raisonnablement tromper la personne concernée sur la portée réelle des mécanismes mis à disposition par Facebook pour que cette dernière puisse gérer l'utilisation des cookies, comme indiqué ci-après.

Toutes les données à caractère personnel obtenues de la même façon, en violation de la législation belge de protection de la vie privée, doivent être détruites, comme le demande la Commission vie privée et comme indiqué ci-après.

Le tribunal accède également à la demande de la Commission vie privée de publier le présent jugement, aux frais des défenderesses, sur le site web www.facebook.com, à compter de la signification du présent jugement et pendant trois mois, et d'en publier le dispositif dans les quotidiens belges De Standaard, De Morgen et Het Nieuwsblad, ainsi qu'une traduction du dispositif en français, réalisée par un traducteur assermenté, aux frais des défenderesses dans les quotidiens Le Soir, La Libre Belgique et La Dernière Heure, dans les 15 jours qui suivent la signification du présent jugement.

Le tribunal estime que les mesures imposées doivent être associées à une astreinte afin d'exercer la pression nécessaire en vue de leur respect. Lors de la fixation de l'ampleur du montant de l'astreinte, le tribunal tient principalement compte de la puissance financière du condamné et de la résistance prévue à l'exécution de la condamnation (voir notamment K. WAGNER, "Dwangsom 2003- 2009" in: Vlaamse Conferentie bij de Balie te Antwerpen (ed.), Meester van het proces. Topics gerechtelijk recht, Gand, Larcier, 2010, (I) 7). Vu les milliards de bénéfices annuels, l'astreinte demandée est de 250.000 euros par jour de non-respect de chacune des mesures susmentionnées dans les délais impartis, semble adéquate pour être suffisamment dissuasive.

40.

Les défenderesses soutiennent que les mesures peuvent uniquement être imposées à **Facebook Ireland**, car elle serait la seule responsable du traitement des données et, par conséquent, elle seule pourrait être sujette aux obligations découlant de la loi belge relative à la protection de la vie privée.

Le tribunal constate toutefois que **Facebook Inc.** Est également (co)responsable du traitement des données à caractère personnel des internautes sur le territoire belge.

L'art. 1 §4 de la loi vie privée définit le « responsable du traitement » comme la personne physique ou morale, l'association de fait ou l'autorité publique qui seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.

Si plusieurs parties définissent la finalité (le motif pour lequel le traitement a lieu) et les moyens du traitement, elles sont conjointement responsables du traitement des données.

Dans son Avis 1/2010, le Groupe « article 29 » sur la protection des données précise notamment à propos des notions de « responsable du traitement » et de « sous-traitant » (voir p. 22, 23 et 37) :

« *Dans le cadre d'une coresponsabilité, la participation des parties à la détermination conjointe peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. En effet, lorsqu'il y a pluralité d'acteurs, ils peuvent entretenir une relation très proche (en partageant, par exemple, l'ensemble des finalités et des moyens d'une opération de traitement) ou, au contraire, plus distante (en ne partageant que les finalités ou les moyens, ou une partie de ceux-ci). Dès lors, un large éventail de typologies de la coresponsabilité doit être examiné, et leurs conséquences juridiques évaluées, avec une certaine souplesse pour tenir compte de la complexité croissante de la réalité actuelle du traitement de données.*

(...)

L'appréciation pourrait toutefois être différente si plusieurs acteurs décidaient de créer une

infrastructure commune afin de poursuivre leurs propres finalités individuelles. En créant cette infrastructure, ces acteurs déterminent les éléments essentiels des moyens à utiliser et deviennent coresponsables du traitement des données, du moins dans cette mesure, même s'ils ne partagent pas nécessairement les mêmes finalités.

(...)

La détermination de la «finalité» du traitement entraîne la qualification de responsable du traitement (de fait). En revanche, la détermination des «moyens» du traitement peut être déléguée par le responsable du traitement, pour autant qu'elle concerne des questions techniques ou d'organisation. Mais les questions sensibles qui sont fondamentales pour la licéité du traitement, comme les données à traiter, la durée de conservation, l'accès, etc., doivent être déterminées par le responsable du traitement. »

À cet égard, le tribunal rejoint l'analyse de la Nederlandse Autoriteit Persoonsgegevens (NAP) en son rapport du 21.02.2017, selon lequel :

- (Traduction libre) le groupe Facebook est formé par Facebook Inc. et toutes ses filiales (notamment Facebook Ireland et Facebook Belgium) et la compétence décisionnelle pour toutes les opérations financières et les résultats d'exploitation résident exclusivement dans le chef du « Chief Operating Decision Maker » (à savoir le CEO) de Facebook Inc., de sorte que cette dernière dispose d'un contrôle sur les moyens financiers affectés au traitement des données à caractère personnel des utilisateurs néerlandais (et en ce même sens également belges) des Services Facebook ;
- le traitement de données forme le cœur même du modèle d'exploitation du groupe Facebook et la plus grande partie des recettes (95 %) du Groupe est générée par les publicités et le traitement des données à caractère personnel, de sorte que le contrôle sur les finances implique également le contrôle des finalités et des moyens du traitement des données.

Les pièces déposées montrent que Facebook Inc. a été constituée en 2004 et qu'elle a commencé à utiliser les sociale plug-ins et, par conséquent, a initié le traitement des données dès 2008, alors que Facebook Ireland a seulement été constituée en 2008-2009 et a été mise en avant en qualité de responsable du traitement des données à caractère privé des utilisateurs en Europe en 2010 seulement (selon le NAP en 2012). Les pièces déposées montrent en outre que le nouveau traitement des données joue un rôle dans l'affichage de publicités ciblées en fonction du comportement de navigation et de l'utilisation des applications en dehors du Service Facebook, dans le but d'augmenter les recettes mondiales générées dans le monde entier au profit du groupe Facebook.

Comme le relève, à juste titre, la Commission vie privée, le fait que Facebook Ireland soit « sur papier » (par des contrats conclus entre Facebook Inc. et sa filiale Facebook Ireland, mais aussi dans les Conditions d'utilisation et la Politique d'utilisation des données) soit présentée comme responsable du traitement n'enlève rien au fait que Facebook Inc. définisse toujours, *de facto*, les finalités et les moyens du traitement. En atteste le fait que dans sa communication financière, Facebook Inc. Considère également les utilisateurs européens comme étant « ses » utilisateurs, qui ont une incidence sur « ses » revenus et ses frais, etc. Les nouvelles conditions d'utilisation ont par ailleurs été introduites simultanément dans le monde entier en 2015. Facebook Inc. Exerce en outre le contrôle final sur le développement et le lancement de nouveaux services, aussi en Europe, et elle

est responsable du stockage de toutes les données à caractère personnel rassemblées, sans qu'elle le fasse uniquement « pour le compte » de sa filiale Facebook Ireland (dont elle est actionnaire à 100 %). Contrairement à ce que prétendent les défenderesses, Facebook Inc. Ne peut par conséquent être considérée uniquement comme le « sous-traitant des données à caractère personnel » pour Facebook Ireland, mais elle est également « responsable du traitement des données ».

Étant donné le lien économique fort qui unit Facebook Inc., Facebook Ireland et Facebook Belgium, comme décrit précédemment dans l'analyse des activités de l'établissement belge, qui a mené le tribunal à la conclusion que ces activités et celles de l'exploitant du Service Facebook sont indissociablement liées, les mesures peuvent également être appliquées à l'établissement belge, à savoir Facebook Belgium, dont les activités contribuent au financement du site de réseau social.

L'action de la Commission vie privée est par conséquent fondée à l'encontre des trois défenderesses, dans la mesure décrite dans le dispositif du présent jugement.

V. FRAIS DE L'INSTANCE

41.

En vertu de l'article 1017 C. jud, tout jugement définitif renvoie, même de plein droit, la partie qui succombe aux frais. La partie en intervention volontaire, dont l'action est déboutée au motif qu'elle est irrecevable, est condamnée au paiement d'une indemnité de procédure de 1 440 euros à chacune des 3 parties défenderesses. Les défenderesses sont les parties qui succombent au regard de la partie demanderesse, de sorte que le tribunal les condamne aux frais de la présente procédure, aux frais de citation et de mise au rôle (non taxés) dans le chef du demandeur et à 1 440,00 euros d'indemnité de procédure, dus séparément par chaque défenderesse.

PAR CES MOTIFS

LE TRIBUNAL

Constate que les dispositions de la loi du 15 juin 1935 relative à l'emploi des langues en matière judiciaire, telles que modifiées, ont été respectées.

Se prononce contradictoirement,

Précise le jugement interlocutoire du 02.11.2017,

Se déclare internationalement compétent pour connaître de l'action du demandeur.

Déclare l'action du demandeur recevable.

Déclare l'action en intervention volontaire irrecevable.

Déclare l'action du demandeur fondée dans la mesure suivante :

Ordonne les mesures suivantes à l'égard des trois demanderesses :

A. à l'égard de **chaque internaute sur le territoire belge,** de cesser :

(1) de placer le cookie « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent offrant une fonctionnalité et une utilisation comparables lorsqu'il navigue sur une page web du domaine facebook.com ou qu'il aboutit sur le site d'un tiers, si ce n'est, moyennant le respect préalable des conditions suivantes :

(a) recevoir, de façon claire et compréhensible, des informations complètes et exactes sur :

- les circonstances dans lesquelles Facebook place ces cookies et les collecte ultérieurement ;
- les finalités pour lesquelles Facebook utilise ces cookies ;
- la nature des données collectées par Facebook lorsqu'il consulte un site contenant un social plug-in Facebook, par exemple l'adresse Internet (URL) de ce site web ;
- les destinataires ou les catégories de destinataires des données collectées ;
- l'existence de son droit d'opposition d'accès et de rectification ;
- la durée de conservation des données collectées par l'intermédiaire des cookies et des social plug-ins ;

(b) avoir librement, spécifiquement et indubitablement consenti, tant à l'installation qu'à l'utilisation de ces cookies, pour autant qu'elles ne soient pas strictement nécessaires à la fourniture du service expressément demandé par l'utilisateur et, lorsqu'il s'est déconnecté de Facebook ou s'est désactivé, il n'a pas librement, spécifiquement et indubitablement consenti à la poursuite de l'utilisation de ces cookies ;

(c) a eu la possibilité de refuser l'installation de ces cookies, pour autant qu'ils ne soient pas strictement nécessaires à la fourniture du service qu'il a expressément demandé, sans que cela limite ou complique l'accès au domaine Facebook.com ;

(2) la collecte des cookies « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent offrant une fonctionnalité et une utilisation comparables, au

moyen de social plug-ins et pixels Facebook ou outils technologiques similaires sur les sites web de tiers, d'une façon excessive au regard des finalités des cookies concernés, étant entendu que :

(a) la collecte systématique de cookies à des finalités de sécurité lors de la consultation de pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée : (1) ne possède pas de compte Facebook ou n'est pas connectée, et (2) ne tente pas d'utiliser les social plug-ins (par exemple en cliquant dessus) ;

(b) la collecte systématique de cookies à des fins publicitaires lors de la consultation de pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée a fait savoir qu'elle ne souhaite pas que son comportement de navigation soit utilisé à des fins publicitaires ;

(c) la collecte systématique de cookies pour vérifier l'identité d'un utilisateur de Facebook ou pour enregistrer le fait qu'il a décidé de rester connecté lorsqu'il consulte des pages web étrangères au domaine facebook.com, est excessive lorsque la personne concernée n'est pas connectée et ne tente pas d'utiliser les social plug-ins (par exemple en cliquant dessus) ;

B. à l'égard de **tout internaute établi sur le territoire belge**, cesser de fournir des informations raisonnablement susceptibles de tromper la personne concernée sur la portée réelle des mécanismes mis à disposition par Facebook pour que cette dernière puisse gérer l'utilisation des cookies ;

C. la destruction, dans les trois mois qui suivent la signification du présent jugement, sous la supervision d'un expert informatique désigné par les parties, aux frais des défenderesses, de toutes les données à caractère personnel obtenues au sujet de chaque internaute sur le territoire belge au moyen de cookies et de social plug-ins d'une façon dont la cessation a été demandée ci-dessus et exiger des tiers auxquels les défenderesses ont transmis ces données de les détruire dans ce même délai ;

D. la publication, aux frais des défenderesses, (1) du présent jugement dans son ensemble sur le site web www.facebook.com lorsqu'il est consulté par un internaute établi sur le territoire belge, pendant 3 mois à compter de la signification du présent jugement, et (2) le dispositif du présent jugement dans les journaux de la presse écrite belge De Standaard, De Morgen, Het Nieuwsblad, et, après traduction en français par un traducteur assermenté, aux frais des défenderesses, dans les journaux francophones suivants : Le Soir, La Libre Belgique en La Dernière Heure, dans les 15 jours calendrier suivant la signification du présent jugement.

Ordonne à la charge des défenderesses, à savoir Facebook, Inc., Facebook Ireland et Facebook Belgium, *in solidum*, et pour le compte du demandeur, agissant en vertu de l'article 32, §3 de la loi vie privée du 8 décembre 1992, l'application d'une astreinte de 250 000 euros par jour calendrier entamé de retard dans l'exécution de toute mesure imposée par le présent jugement, avec un maximum de 100 000 000 euros.

Condamne la partie en intervention volontaire à payer à chaque partie défenderesse une indemnité de procédure de 1 440,00 euros (au total 4 320 euros).

Condamne les parties défenderesse *in solidum* à payer au demandeur, agissant en vertu de l'article 32, §3 de la loi vie privée du 8 décembre 1992, les frais de citation, non taxés, et chacune d'elles à payer au demandeur une indemnité de procédure de 1 440,00 euros (soit au total 4 320,00 euros).

Ainsi prononcé en audience publique le 16 février 2018, conformément à l'article 782bis, premier alinéa, C. jud., par le président, assisté du greffier, de la 24e chambre du tribunal de première instance néerlandophone de Bruxelles, composé pour le prononcé du jugement, de :

Monsieur Ph. Joos de ter Beerst, vice-président,

Madame K. Vereist, juge,

Madame D. Fransens, juge,

Madame L. DEMESMAEKER, greffier adjoint.