Date de réception : 29/10/2019

Affaire C-645/19

Demande de décision préjudicielle

Date de dépôt :

30 août 2019

Juridiction de renvoi :

Hof van beroep te Brussel (Belgique)

Date de la décision de renvoi :

8 mai 2019

Parties requérantes :

Facebook Ireland Limited

Facebook INC.

Facebook Belgium BVBA

Partie défenderesse :

Gegevensbeschermingsautoriteit

[OMISSIS]
[OMISSIS]
[OMISSIS]

Hof van beroep

Brussel

(Cour d'appel de Bruxelles, Belgique)

Arrêt

[OMISSIS]

[Or. 2]

EN CAUSE DE :

1. FACEBOOK IRELAND LIMITED, [OMISSIS] **première appelante,** [OMISSIS]

2. FACEBOOK INC., [OMISSIS] **deuxième appelante,** [OMISSIS]

3. FACEBOOK BELGIUM B.V.B.A., [OMISSIS] **troisième appelante,** [OMISSIS]

contre le jugement du Nederlandstalige rechtbank van eerste aanleg Brussel (tribunal de première instance néerlandophone de Bruxelles, Belgique) du 16 février 2018,

CONTRE :

1. La GEGEVENSBESCHERMINGSAUTORITEIT (Autorité de protection des données), [OMISSIS] première intimée *, [Or. 3]

2. La GEGEVENSBESCHERMINGSAUTORITEIT (Autorité de protection des données), [OMISSIS] seconde intimée **,

[OMISSIS]

I. L'appel interjeté

[détails de procédure relatifs à l'appel interjeté]

[OMISSIS]

La GEGEVENSBESCHERMINGSAUTORITEIT (Autorité de protection des données, Belgique, ci-après l'« APD ») est désormais partie à la procédure devant le [hof van beroep te Brussel (cour d'appel de Bruxelles, Belgique, ci-après également le « hof » ou la « juridiction de céans »), en tant que venant aux droits à la fois de M. Willem DEBEUCKELAERE en sa qualité de président de la Commissie ter bescherming van de Persoonlijke Levenssfeer (Commission de la protection de la vie privée, Belgique, ci-après la « Commission vie privée ») et de la Commission vie privée, partie intervenant volontairement.

* Ndt : En tant que venant aux droits du demandeur en première instance, M. Willem Debeuckelaere en sa qualité de président de la Commission vie privée.

** Ndt : En tant que venant aux droits de l'intervenante volontaire en première instance, la Commission vie privée.

[OMISSIS] **[Or. 4]**

II. Les abréviations couramment utilisées et le cadre juridique

II.1.

APD	L'Autorité de protection des données, telle que définie à l'article 3 de la wet van 3 december 2017 (loi du 3 décembre 2017) [1]

L'APD présente la liste suivante des abréviations utiles à la lisibilité du présent arrêt :

WVP	Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)
WEC	Wet van 13 juni 2005 betreffende de elektronische communicatie (loi du 13 juin 2005 relative aux communications électroniques)
Directive 95/46	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 (JO 1995, L 281, p. 31)
Directive 2002/58	Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37)
Directive 2009/136	Directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) nº 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs (JO 2009,

[1] *« Il est institué auprès de la Chambre des représentants une "Autorité de protection des données"*. Elle succède à la Commission de la protection de la vie privée. [OMISSIS] ».

	L 337, p. 11)
RGPD	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 **[Or. 5]** traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO 2016, L 119, p. 1)
Loi APD	Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (loi du 3 décembre 2017 portant création de l'Autorité de protection des données)
Loi-cadre	Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel).
Groupe article 29	Jusqu'au 25 mai 2018, l'organe faîtier des commissions vie privée des 28 États membres de l'Union, institué par l'article 29 de la directive 95/46. Ce groupe a ensuite été remplacé, conformément à l'article 49, paragraphe 2 * RGPD, par le Comité européen de la protection des données (European Data Protection Board, EDPB) [2]. Les missions du Groupe article 29 comprenaient notamment toute question relative à l'application des dispositions nationales d'application des directives 95/46 et 2002/58. Le Groupe article 29 communiquait régulièrement des avis et publiait des documents de travail et résolutions concernant divers thèmes ayant trait à la protection de la vie privée et des données à caractère personnel, afin de promouvoir une application harmonisée des directives dans les États membres de l'Union. Ses avis et autres documents sont publics et peuvent être consultés sur son site Internet [3].

II.2.

L'APD décrit comme suit la législation applicable :

> *« La WVP a été adoptée le 8 décembre 1992.*
>
> *Jusqu'au 25 mai 2018, la directive 95/46 était la directive "de base" en matière de vie privée. Elle a été transposée en droit belge par une*

* Ndt : il s'agit, semble-t-il, de l'article 68.

2 [OMISSIS]

3 [OMISSIS]

modification de la WVP par la Wet 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens (loi du 11 décembre 1998 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 de données à caractère personnel et à la libre circulation de ces données).

La directive 2002/58 est la directive dite "vie privée et communications électroniques", elle dispose qu'elle "précise et complète" la directive 95/46. L'article 5, paragraphe 3, de la directive 2002/58 (qui concerne notamment les "cookies") a été transposé en droit belge dans l'article 129 WEC.

La directive 2002/58 par la directive 2009/136. La modification de l'article 5, paragraphe 3, de la directive 2002/58 a été transposée en droit belge par une modification de l'article 129 WEC **[Or. 6]** *par l'article 90 de la Wet van 10 juli 2012 houdende diverse bepalingen inzake elektronische communicatie [loi du 10 juillet 2012. portant des dispositions diverses en matière de communications électroniques (Ndt : dite "loi Telecom")]*

À compter du 25 mai 2018, la directive 95/46 a été abrogée et remplacée par le RGPD (article 94, paragraphe 1, et article 99, paragraphe 2). Conformément à l'article 94, paragraphe 2, RGPD, les références faites à la directive 95/46 s'entendent comme faites au RGPD. L'article 129 WEC a été maintenu.

La loi APD a été adoptée le 3 décembre 2017 (Moniteur belge du 10 janvier 2018). À compter du 25 mai 2018, l'Autorité de protection des données (APD) succède juridiquement à la Commission vie privée (articles 3 et 110).

La loi-cadre a été adoptée le 30 juillet 2018 (Moniteur belge du 5 septembre 2018). Cette loi régit, entre autres, les questions liées à la protection des données dans les cas où le RGPD a donné la possibilité ou a imposé aux États membres d'établir des règles détaillées. Son article 280 a abrogé la WVP ».

III. La procédure devant la juridiction de première instance

[déroulement de la procédure devant le rechtbank van eerste aanleg (tribunal de première instance, Belgique)]

[OMISSIS] **[Or. 7]** [OMISSIS] **[Or. 8]** [OMISSIS] **[Or. 9]** [OMISSIS] **[Or. 10]** [OMISSIS] **[Or. 11]** [OMISSIS]

Le jugement attaqué disposait ce qui suit : **[Or. 12]**

[OMISSIS]

Déclare l'action du demandeur fondée dans la mesure qui suit :

Ordonne aux trois défenderesses les mesures suivantes :

A. en ce qui concerne **tout internaute sur le territoire belge**, cesser :

1) de placer le cookie « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent ayant des fonctionnalités et une utilisation similaires lors de l'accès à une page Web du domaine facebook.com ou à un site Web tiers, sans que l'internaute ait, au préalable

a) été informé complètement et précisément, de manière claire et compréhensible :

– des circonstances dans lesquelles Facebook place ces cookies sur son disque dur et les recueille ensuite ;

– des finalités pour lesquelles Facebook applique ces cookies ;

– de la nature des données recueillies par Facebook lorsqu'il visite un site Web qui contient un module (plug-in) social de Facebook, comme l'adresse Internet (URL) de ce site Web ;

– des destinataires ou les catégories de destinataires des données recueillies,

– de l'existence de ses droits d'opposition, d'accès et de correction ;

– de la durée de conservation des données recueillies au moyen des cookies et modules sociaux ; **[Or. 13]**

b) consenti librement, spécifiquement et sans ambiguïté à l'installation et à l'utilisation de ces cookies dans la mesure où ils ne sont pas strictement nécessaires au service expressément demandé par lui ;

et, s'il s'est désabonné ou a désactivé son compte Facebook, consenti librement, spécifiquement et sans ambiguïté à ce que ces cookies continuent d'être utilisés ;

c) eu la possibilité de refuser l'installation de ces cookies, dans la mesure où ils ne sont pas strictement nécessaires pour un service qu'il a expressément demandé, sans que l'accès au domaine facebook.com soit restreint ou entravé ;

2) de recueillir les cookies « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent ayant des fonctionnalités et une utilisation similaires, au moyen de modules sociaux Facebook, de pixels Facebook ou

de moyens technologiques similaires sur des sites tiers, d'une manière excessive eu égard aux objectifs desdits cookies, étant entendu que :

a) la collecte systématique de cookies à des fins de sécurité lors de la visite de pages Web n'appartenant pas au domaine facebook.com est excessive si la personne concernée 1) ne dispose pas d'un compte Facebook ou n'est pas connectée et 2) ne tente pas d'utiliser les modules sociaux (par exemple, en cliquant dessus) ;

b) la collecte systématique de cookies à des fins publicitaires lors de la visite de pages Web n'appartenant pas au domaine facebook.com est excessive si la personne concernée a indiqué qu'elle ne souhaitait pas que des informations sur son comportement de navigation soient utilisées à des fins publicitaires ;

c) la collecte systématique de cookies utilisés pour vérifier l'identité d'un utilisateur de Facebook ou pour enregistrer s'il a choisi de rester connecté à des pages Web ne faisant pas partie du domaine facebook.com est excessive lorsqu'il n'est pas connecté et ne tente pas d'utiliser les modules (plug-ins) sociaux (par exemple, en cliquant dessus) ;

B. en ce qui concerne **tout internaute sur le territoire belge**, cesser la fourniture d'informations qui pourraient raisonnablement induire en erreur les personnes concernées quant à la portée réelle des mécanismes mis à disposition par Facebook pour gérer l'utilisation des cookies par Facebook ;

C. détruire, dans un délai de trois mois à compter de la signification du présent jugement, sous le contrôle d'un expert en TIC à désigner par les parties et aux frais des défenderesses, toutes les données personnelles de chaque internaute sur le territoire belge qu'elles ont obtenues au moyen de cookies et de modules sociaux de la manière dont la cessation est demandée ci-dessus, et d'exiger des tiers auxquels elles ont fourni ces données qu'ils effectuent cette destruction dans ce même délai ; **[Or. 14]**

D. publier, aux frais desdits défenderesses, 1) le présent jugement dans son intégralité sur le site Web www.facebook.com lorsqu'il est consulté par un internaute sur le territoire belge pendant une période de trois mois à compter de la date de signification du présent jugement, et 2) le dispositif du présent jugement dans les journaux belges De Standaard, De Morgen, Het Nieuwsblad et, après traduction en français par un traducteur juré, aux frais des défenderesses également, dans les journaux francophones suivants : Le Soir, La Libre Belgique et La Dernière Heure, dans un délai de quinze jours civils à compter de la date de la signification du présent jugement.

Condamne les défenderesses, à savoir Facebook Inc, Facebook Ireland et Facebook Belgium, in solidum, à payer au demandeur, agissant au titre de l'article 32, pargraphe3, de la loi du 8 décembre 1992 relative à la protection de la vie privée, une astreinte de 250 000 euros par jour civil de retard entamé dans

l'exécution de toute mesure imposée par le présent jugement, sans dépasser 100 000 000 euros.

Condamne l'intervenante volontaire à verser à chacune des défenderesses une indemnité de procédure de 1 440,00 euros (au total 4 320 euros).

Condamne les défenderesses in solidum à payer au demandeur, agissant au titre de l'article 32, paragraphe 3, de la loi du 8 décembre 1992 relative à la protection de la vie privée, les frais de citation, non quantifiés, et chacun d'eux à verser au demandeur une indemnité de procédure de 1 440,00 euros (au total 4 320,00 euros).

IV. Les demandes devant la juridiction de céans

IV.1.

Les parties **FACEBOOK** concluent [OMISSIS] qu'il plaise au hof :

> *« – Déclarer l'appel recevable et fondé, pour annuler les griefs exposés ci-dessus et l'arrêt attaqué et, partant, statuer à nouveau :*
>
> *– se déclarer incompétent à l'égard des trois appelantes ;*
>
> *– à titre subsidiaire : déclarer les demandes principales et subsidiaire intégralement ou au moins partiellement inadmissibles ou à tout le moins irrecevables ;*
>
> *– à titre plus subsidiaire, renvoyer à la Cour de justice les questions préjudicielles suivantes :*
>
> [OMISSIS] **[Or. 15]** [OMISSIS] [questions proposées à la Cour, voir point 5.1 ci-après]
>
> *– à titre encore plus subsidiaire : de rejeter les demandes comme non fondées, et*
>
> *– en tout état de cause : condamner les intimées aux dépens des deux procédures, pour les appelantes, estimés à 1 440 euros chacune en frais de justice. »*

IV.2.

En tant que venant aux droits du demandeur initial, à savoir : [OMISSIS] M. **WILLEM DEBEUCKELAERE, agissant en sa qualité de PRÉSIDENT DE LA COMMISSION VIE PRIVÉE BELGE** [OMISSIS] l'APD conclut [OMISSIS] qu'il plaise au hof :

« *Confirmer le jugement a quo comme suit et, statuant à nouveau :*

Se déclarer compétent sur le plan international pour prendre connaissance de l'action du concluant à l'encontre de Facebook Inc., Facebook Ireland en Facebook Belgium ;

Déclarer l'action du concluant recevable, ou à tout le moins saisir la Cour de justice de la question préjudicielle suivante relative à la compétence :

[OMISSIS] **[Or. 16]** [OMISSIS] [questions proposées au hof, voir également point 5.1 ci-après]

Si par impossible l'action du concluant était déclarée irrecevable, en raison du défaut de qualité du concluant pour continuer à agir dans la présente procédure, déclarer l'appel des appelantes également irrecevable, en raison de ce défaut de qualité du concluant ;

Déclarer fondée l'action du concluant et, en conséquence :

Constater que Facebook Inc. et Facebook Ireland ont enfreint, en ce qui concerne les traitements de données à caractère personnel en cause, avant le 25 mai 2018, les articles 4, 5 et 9 WVP et l'article 129 WEC ;

Constater que Facebook Inc. et Facebook Ireland ont enfreint, en ce qui concerne les traitements de données à caractère personnel en cause, à compter du 25 mai 2018, les articles 5, 6, 7,12 et 14 RGPD et l'article 129 WEC ;

Ordonner à Facebook Inc., Facebook Ireland et Facebook Belgium les mesures suivantes :

A. en ce qui concerne tout internaute sur le territoire belge, cesser :

B.

1) de placer le cookie « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent ayant des fonctionnalités et une utilisation similaires lors de l'accès à une page Web du domaine facebook.com ou à un site Web tiers, sans que l'internaute ait, au préalable :

a) été informé complètement et précisément, de manière claire et compréhensible :

– *des circonstances dans lesquelles Facebook place ces cookies sur son disque dur et les recueille ensuite ;*

– *des finalités pour lesquelles Facebook applique ces cookies ;*

– *de la nature des données recueillies par Facebook lorsqu'il visite un site Web qui contient un module social de Facebook, comme l'adresse Internet (URL) de ce site Web ;*

– *des destinataires ou les catégories de destinataires des données recueillies,*

– *de l'existence de ses droits d'opposition, d'accès et de correction ;*

– *de la durée de conservation des données recueillies au moyen des cookies et modules sociaux ;*

b) consenti librement, spécifiquement et sans ambiguïté à l'installation et à l'utilisation de ces cookies dans la mesure où ils ne sont pas strictement nécessaires au service expressément demandé par lui ;

et, s'il s'est désabonné ou a désactivé son compte Facebook, consenti librement, spécifiquement et sans ambiguïté à ce que ces cookies continuent d'être utilisés ;

c) eu la possibilité de refuser l'installation de ces cookies, dans la mesure où ils ne sont pas strictement nécessaires pour un service qu'il a expressément demandé, sans que l'accès au domaine Facebook.com soit restreint ou entravé ;

2) de recueillir les cookies « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent ayant des fonctionnalités et une utilisation similaires, au moyen de modules sociaux Facebook, de pixels Facebook ou de moyens technologiques similaires sur des sites tiers, d'une manière excessive eu égard aux objectifs desdits cookies, étant entendu que :

a) la collecte systématique de cookies à des fins de sécurité lors de la visite de pages Web n'appartenant pas au domaine facebook.com est excessive si la personne concernée 1) ne dispose pas d'un compte Facebook ou n'est pas connectée et 2) ne tente pas d'utiliser les modules sociaux (par exemple, en cliquant dessus) ;

b) la collecte systématique de cookies à des fins publicitaires lors de la visite de pages Web n'appartenant pas au domaine facebook.com est excessive si la personne concernée a indiqué qu'elle ne souhaitait pas que des informations sur son comportement de navigation soient utilisées à des fins publicitaires ;

c) la collecte systématique de cookies utilisés pour vérifier l'identité d'un utilisateur de Facebook ou pour enregistrer s'il a choisi de rester connecté à des pages Web ne faisant pas partie du domaine

facebook.com est excessive lorsqu'il n'est pas connecté et ne tente pas d'utiliser les modules sociaux (par exemple, en cliquant dessus) ; **[Or. 17]** [OMISSIS] **[Or. 18]**

B. en ce qui concerne tout internaute sur le territoire belge, cesser la fourniture d'informations qui pourraient raisonnablement induire en erreur les personnes concernées quant à la portée réelle des mécanismes mis à disposition par Facebook pour gérer l'utilisation des cookies par Facebook ;

C. détruire, dans un délai de trois mois à compter de la signification du présent jugement, sous le contrôle d'un expert en TIC à désigner par les parties et aux frais des appelantes, toutes les données personnelles de chaque internaute sur le territoire belge qu'elles ont obtenues au moyen de cookies et de modules sociaux de la manière dont la cessation est demandée ci-dessus, et d'exiger des tiers auxquels elles ont fourni ces données qu'ils effectuent cette destruction dans ce même délai ;

D. publier, aux frais des appelantes, 1) du présent arrêt dans son intégralité sur le site Web www.facebook.com lorsqu'il est consulté par un internaute sur le territoire belge pendant une période de trois mois à compter de la date de signification du présent arrêt, et 2) du dispositif du présent arrêt dans les journaux belges De Standaard, De Morgen, Het Nieuwsblad et, après traduction en français par un traducteur juré, aux frais des appelantes également, dans les journaux francophones suivants : Le Soir, La Libre Belgique et La Dernière Heure, dans un délai de quinze jours civils à compter de la date de la signification du présent jugement ;

Condamner les appelantes, in solidum, à payer au concluant une astreinte de 250 000 euros par jour civil de retard entamé dans l'exécution de toute mesure imposée par le présent arrêt, sans dépasser 100 000 000 euros.

Condamner les appelantes in solidum aux dépens de la procédure, y compris les frais de citation, les frais de signification et l'indemnité de procédure, celle-ci s'élevant actuellement à 1 440 euros par appelante par instance ».

IV.3.

En tant que venant aux droits de la partie intervenante initiale, à savoir **la COMMISSION VIE PRIVÉE**, [OMISSIS] l'APD conclut [OMISSIS] qu'il plaise au hof :

« Sur l'appel consécutif ou incident de la concluante, déclarer son intervention recevable et, statuant à nouveau :

Se déclarer compétent sur le plan international pour prendre connaissance de l'action de la concluante à l'encontre de Facebook Inc., Facebook Ireland en Facebook Belgium ; **[Or. 19]**

Déclarer l'action de la concluante recevable, ou à tout le moins saisir la Cour de justice de la question préjudicielle suivante relative à la compétence :

[OMISSIS] [questions proposées au hof, voir également point 5.1 ci-après]

Si par impossible l'action de concluante était déclarée irrecevable, en raison du défaut de qualité de la concluante pour continuer à agir dans la présente procédure, déclarer l'appel des appelantes également irrecevable, en raison de ce défaut de qualité de la concluante ;

Déclarer fondée l'action de la concluante et, en conséquence :

Constater que Facebook Inc. et Facebook Ireland ont enfreint, en ce qui concerne les traitements de données à caractère personnel en cause, avant le 25 mai 2018, les articles 4, 5 et 9 WVP et l'article 129 WEC ;

Constater que Facebook Inc. et Facebook Ireland ont enfreint, en ce qui concerne les traitements de données à caractère personnel en cause, à compter du 25 mai 2018, les articles 5, 6, 7,12 et 14 RGPD et l'article 129 WEC ;

Ordonner à Facebook Inc., Facebook Ireland et Facebook Belgium les mesures suivantes :

A. en ce qui concerne tout internaute sur le territoire belge, cesser :

1) de placer le cookie « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent ayant des fonctionnalités et une utilisation similaires **[Or. 20]** *lors de l'accès à une page Web du domaine facebook.com ou à un site Web tiers, sans que l'internaute ait, au préalable :*

a) été informé complètement et précisément, de manière claire et compréhensible :

– *des circonstances dans lesquelles Facebook place ces cookies sur son disque dur et les recueille ensuite ;*

– *des finalités pour lesquelles Facebook applique ces cookies ;*

– *de la nature des données recueillies par Facebook lorsqu'il visite un site Web qui contient un module social de Facebook, comme l'adresse Internet (URL) de ce site Web ;*

– *des destinataires ou les catégories de destinataires des données recueillies,*

– *de l'existence de ses droits d'opposition, d'accès et de correction ;*

– *de la durée de conservation des données recueillies au moyen des cookies et modules sociaux ;*

b) consenti librement, spécifiquement et sans ambiguïté à l'installation et à l'utilisation de ces cookies dans la mesure où ils ne sont pas strictement nécessaires au service expressément demandé par lui ;

et, s'il s'est désabonné ou a désactivé son compte Facebook, consenti librement, spécifiquement et sans ambiguïté à ce que ces cookies continuent d'être utilisés ;

c) eu la possibilité de refuser l'installation de ces cookies, dans la mesure où ils ne sont pas strictement nécessaires pour un service qu'il a expressément demandé, sans que l'accès au domaine facebook.com soit restreint ou entravé ;

2) de recueillir les cookies « c_user », « xs », « datr », « sb », « fr » et « lu » et tout autre cookie équivalent ayant des fonctionnalités et une utilisation similaires, au moyen de modules sociaux Facebook, de pixels Facebook ou de moyens technologiques similaires sur des sites tiers, d'une manière excessive eu égard aux objectifs desdits cookies, étant entendu que :

a) la collecte systématique de cookies à des fins de sécurité lors de la visite de pages Web n'appartenant pas au domaine facebook.com est excessive si la personne concernée 1) ne dispose pas d'un compte Facebook ou n'est pas connectée et 2) ne tente pas d'utiliser les modules sociaux (par exemple, en cliquant dessus) ;

b) la collecte systématique de cookies à des fins publicitaires lors de la visite de pages Web n'appartenant pas au domaine facebook.com est excessive si la personne concernée a indiqué qu'elle ne souhaitait pas que des informations sur son comportement de navigation soient utilisées à des fins publicitaires ;

c) la collecte systématique de cookies utilisés pour vérifier l'identité d'un utilisateur de Facebook ou pour enregistrer s'il a choisi de rester connecté à des pages Web ne faisant pas partie du domaine facebook.com est excessive lorsqu'il n'est pas connecté et ne tente pas d'utiliser les modules sociaux (par exemple, en cliquant dessus) ; **[Or. 21]**

B. en ce qui concerne tout internaute sur le territoire belge, cesser la fourniture d'informations qui pourraient raisonnablement induire en erreur les personnes concernées quant à la portée réelle des mécanismes mis à disposition par Facebook pour gérer l'utilisation des cookies par Facebook ;

C. détruire, dans un délai de trois mois à compter de la signification du présent jugement, sous le contrôle d'un expert en TIC à désigner par les parties et aux frais des appelantes, toutes les données personnelles de chaque internaute sur le

territoire belge qu'elles ont obtenues au moyen de cookies et de modules sociaux de la manière dont la cessation est demandée ci-dessus, et d'exiger des tiers auxquels elles ont fourni ces données qu'ils effectuent cette destruction dans ce même délai ;

D. publier, aux frais des appelantes, 1) du présent arrêt dans son intégralité sur le site Web www.facebook.com lorsqu'il est consulté par un internaute sur le territoire belge pendant une période de trois mois à compter de la date de signification du présent arrêt, et 2) du dispositif du présent arrêt dans les journaux belges De Standaard, De Morgen, Het Nieuwsblad et, après traduction en français par un traducteur juré, aux frais des appelantes également, dans les journaux francophones suivants : Le Soir, La Libre Belgique et La Dernière Heure, dans un délai de quinze jours civils à compter de la date de la signification du présent jugement ;

Condamner les appelantes, in solidum, à payer au concluant une astreinte de 250 000 euros par jour civil de retard entamé dans l'exécution de toute mesure imposée par le présent arrêt, sans dépasser 100 000 000 euros.

Condamner les appelantes in solidum aux dépens de la procédure, y compris les frais de citation, les frais de signification et l'indemnité de procédure, celle-ci s'élevant actuellement à 1 440 euros par appelante par instance ».

[OMISSIS]

V. Les faits

La décision attaquée a correctement résumé les faits, la juridiction de céans adopte * ce résumé : **[Or. 22]**

2.

Le service en ligne Facebook est un site de réseau social mondial gratuit, qui tire une grande partie de ses revenus des annonces publicitaires, 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 M. Willem Debeuckelaere, en sa qualité de président de la [Commission vie privée]. La Commission vie privée est intervenue volontairement en la présente procédure. Pour faciliter la lecture, le rechtbank dénommera ci-après conjointement ces deux parties au procès la « Commission vie privée », sauf s'il s'avérait nécessaire de les nommer séparément

* Ndt : le hof reproduit ci-après l'exposé des faits du jugement de première instance.

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 en matière de protection 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 », « modules sociaux » (« modules sociaux ») et « pixels »

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

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 (ci-après la « DDR »). Elle se décrit également comme étant la seule partie contractuelle de tous les utilisateurs belges [de Facebook] et comme la seule responsable du traitement de toutes les données reçues de ressortissants de l'UE, y compris 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 bvba [société privée à responsabilité limitée, 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. **[Or. 23]**

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 citation signifiée le 10 juin 2015.

La Commission vie privée affirme qu'à la suite de l'entrée en vigueur de la nouvelle politique d'utilisation des données et des cookies de Facebook, le 30 janvier 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 chargé de la Protection de 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 protection 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 leurs travaux, avaient déjà mené des

recherches approfondies sur Facebook. Le 31 mars 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 dudit rapport [OMISSIS], qui décrivent comment Facebook enregistrait à l'époque, par une combinaison de modules sociaux et de cookies, les sites web consultés par les internautes et comment Facebook enregistrait également le comportement de recherche des utilisateurs de Facebook [*], 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 ci-après).

Le 13 mai 2015, la Commission vie privée a adopté la recommandation n° 04/2015 concernant le traitement des données à caractère personnel par le biais des modules sociaux de Facebook, visant *« 1) Facebook, 2) les utilisateurs d'Internet et/ou Facebook) et 3) les utilisateurs et les fournisseurs de services Facebook, notamment les modules sociaux »* [OMISSIS].

Il ressort 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 [OMISSIS]. Facebook reconnaissait exclusivement la compétence de la Commission vie privée irlandaise et estimait que seul le droit de la protection des données national irlandais s'appliquait à l'ensemble des utilisateurs européens de son réseau social. Facebook argumentait en outre que ce n'était pas Facebook, Inc., mais Facebook Ireland Limited qui devait 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 lui a notamment ordonné : **[Or. 24]**

– 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 modules sociaux, sauf si elle reçoit pour ce faire le consentement spécifique et indubitable, par

[*] Ndt : l'appel de note original dans le jugement [1] est conservé, mais la note est omise. Dans le jugement cité, la note était formulée comme suit : « Les utilisateurs de Facebook peuvent en outre être répartis en i) les détenteurs de compte Facebook et ii) les utilisateurs du service Facebook non-inscrits ; voir également ci-après ».

opt-in [*] de la personne concernée et dans la mesure où cela s'avère strictement nécessaire à des fins légitimes ;

– de renoncer à la collecte et l'utilisation des données des utilisateurs au moyen de cookies et de modules sociaux, 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 modules sociaux 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 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 Facebook Belgium bvba. Elle a également mis Facebook en demeure, par un courrier du 18 mai 2015, de mettre fin à la violation de la législation belge en matière de protection de la vie privée pour ce qui est des modules sociaux et des cookies [OMISSIS]. L'avocat de Facebook, Inc. et de Facebook bvba a répondu [OMISSIS] 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, [OMISSIS] le demandeur a cité les défenderesses à comparaître devant le président du rechtbank [OMISSIS] [**], siégeant en référé.

4.

Par une ordonnance rendue le 9 novembre 2015 [OMISSIS], le président du rechtbank [OMISSIS], siégeant en référé, a estimé qu'il était compétent (au niveau international) pour connaître du litige et que l'action du demandeur était recevable ; il a déclaré fondée à l'égard de toutes les défenderesses l'action en cessation intentée, en ce sens qu'elles ont été obligées de :

[*] Ndt : l'appel de note original [2] dans le jugement est conservé, mais la note est omise. Dans le jugement cité, la note était formulée comme suit : « 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 ».

[**] Ndt : à savoir, le rechtbank van eerste aanleg (président du tribunal de première instance) de Bruxelles, qui a statué en première instance.

« 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* **[Or. 25]** *place le cookie datr sur leur disque dur et de l'usage que Facebook fait de ce cookie datr au moyen de modules sociaux ;*

– *la collecte du cookie datr par le biais de modules sociaux placés sur les sites Web de tiers ».*

Par un arrêt du 29 juin 2016 [OMISSIS] le hof van Beroep te Brussel (cour d'appel de Bruxelles), 18e chambre néerlandaise, a réformé l'ordonnance susmentionnée. Le hof a jugé qu'il n'était pas compétent à l'égard des actions intentées à l'encontre de Facebook Ireland Limited et de Facebook Inc., qu'il était en revanche compétent pour connaître de l'action intentée par la Commission vie privée à l'encontre de Facebook Belgium bvba, mais que cette action était non fondée dans la mesure où elle reposait sur l'article 584 du code judiciaire, dès lors qu'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 son « cookie-banner » (bandeau cookies) [OMISSIS]. Le 31 août 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, y compris l'utilisation de tous les cookies et l'accès au contenu de ses pages publiques, étant entendu que le bandeau cookies avait été adapté, mais que l'usage de cookies serait étendu ([OMISSIS]).

Dans son « complément » à la recommandation nº 03/2017 du 12 avril 2017 qu'elle avait adoptée de sa propre initiative à la suite de la modification de la politique des cookies et des pratiques de Facebook (voir également ci-après), la Commission vie privée a exposé ce qui suit au sujet de ces modifications :

« [OMISSIS] *L'ordonnance du président du rechtbank van eerste aanleg (président du tribunal de première instance) de Bruxelles a été signifiée à Facebook le 2 décembre 2015. À la suite de cette signification, Facebook a décidé de refuser désormais l'accès aux internautes sur le territoire belge qui ne disposaient 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 telles que 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. <pour en savoir plus>''*

Le visiteur qui cliquait sur "pour en savoir plus" 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 **[Or. 26]** **[Or. 27]** *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 n'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 contribuer à la protection contre les actions nuisibles décrites ci-dessus. 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 effectivement 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.

(...) **[Or. 28]**

[OMISSIS] *Par courrier du 31 mars 2016, Facebook a fait savoir qu'elle adapterait de nouveau sa politique d'utilisation des cookies, son bandeau cookies et la procédure technique de ses cookies (entre autres, le moment auquel elle place des cookies).*

[OMISSIS] *Une des principales modifications de la politique d'utilisation des cookies de Facebook concerne les non-utilisateurs de Facebook. Facebook utiliserait désormais 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.*

[OMISSIS] *Dans son courrier du 31 mars 2016, Facebook a également fait comprendre qu'elle adapterait son "bandeau cookies" conformément aux changements apportés au contenu de sa politique d'utilisation des cookies Le bandeau cookies 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 ce 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>".

[OMISSIS] *En ce qui concerne le placement de cookies, Facebook indiquait 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*

[OMISSIS] *Facebook a introduit son nouveau bandeau cookies 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. Le nouveau bandeau cookies et la nouvelle politique étaient toutefois déjà introduites dans les autres pays européens ».*

5.

Dans l'intervalle, le demandeur actuel avait introduit la procédure au fond [OMISSIS] [devant le rechtbank van eerste aanleg (président du tribunal de première instance) de Bruxelles].

Dans ladite 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 du service Facebook que des non-utilisateurs, au moyen des « modules sociaux » (« modules d'extension sociaux »), cookies et pixels susmentionnés.

Selon la Commission vie privée, les défenderesses enfreignent encore la législation en matière de protection de la vie privée, à plusieurs égards et plus gravement encore qu'auparavant. **[Or. 29]**

La Commission vie privée souligne le fait que le référé susmentionné diffère en trois points de la procédure au fond [devant le rechtbank van eerste aanleg (président du tribunal de première instance) de Bruxelles] :

– 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 [procédure devant le rechtbank van eerste aanleg (président du tribunal de première instance) de Bruxelles] 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 « modules sociaux » et de cookies dits « datr », tandis que la procédure au fond [devant le rechtbank van eerste aanleg (président du tribunal de première instance) de Bruxelles] vise également l'enregistrement au moyen d'autres cookies (à savoir les cookies dits « 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 », c'est-à-dire « de premier niveau » ou « interne »), 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 », c'est-à-dire « tiers »).

Quand un utilisateur souhaite consulter une page Web (demande http), le navigateur envoie automatiquement certaines informations à chaque serveur « de premier niveau » et « tiers » 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 premier niveau, ainsi que tous les cookies préalablement placés par le site Web vers lequel le navigateur a envoyé une demande de contenu (qu'il s'agisse du « premier niveau » ou du « tiers »).

Le serveur de premier niveau envoie ensuite les informations de la page Web vers le navigateur. Ces informations sont notamment, outre le contenu de la page Web du premier niveau, les instructions pour que le navigateur charge le contenu du tiers 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 tiers 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 comportent généralement 1) une adresse IP ; 2) l'URL du site web de premier niveau ; 3) le système d'exploitation du navigateur ; 4) le type de navigateur, et 5) les cookies (précédemment) placés par le site Web tiers à partir duquel le navigateur demande le contenu tiers.

Les « **modules sociaux** » de Facebook sont des composants de site Web (des éléments de code logiciel) que Facebook met à disposition des concepteurs de sites Web externes. 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 module social 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 modules sociaux de Facebook, son navigateur établit automatiquement une connexion avec le serveur Facebook (à savoir, il envoie une demande https audit serveur), après quoi le navigateur de l'internaute charge directement la fonctionnalité du « module » (module d'extension) sur le serveur de **[Or. 30]** **[Or. 31]** Facebook. Selon le demandeur, en pratiquant de la sorte, Facebook reçoit ainsi 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 certaines 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, aux finalités suivantes, entre autres :

– pour 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 ») ;

– pour diffuser, mesurer et améliorer la pertinence des publicités (cookie « fr ») ;

– pour 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 [leur] avis cela ne soit pas nécessaire à strictement parler, elle obtient toujours l'autorisation pour ce faire (par le bandeau cookies) 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 à son compte. 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 sécurisé. 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 que ce cookie 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'authentification 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, entre autres, à la session « identificateur » et à la valeur d'authentification (attribuée par Facebook à une session spécifique **[Or. 32]** **[Or. 33]** ouverte par un détenteur de compte) offrant ainsi des possibilités de recherche et de protection supplémentaires. Selon Facebook, ces deux cookies sont seulement placés dans le navigateur des détenteurs de compte quand ceux-ci se connectent au service Facebook et ils sont supprimés au moment de la déconnexion ou de la désactivation de leurs comptes Facebook. Si ce n'est pas le cas, la durée de vie maximale de ces cookies est de quatre-vingt-dix 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'authentification 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 du service Facebook et les détenteurs de compte y donnent explicitement leur consentement au moment où ils décident de s'inscrire auprès du service 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 quatre-vingt-dix 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 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 quatre-vingt-dix jours.

Les défenderesses font valoir que le cookie « fr » est explicitement mentionné dans la politique d'utilisation des cookies du service Facebook et que les détenteurs de compte et les utilisateurs non-inscrits donnent également leur consentement explicite par l'intermédiaire du bandeau cookies (les détenteurs de compte également, lorsqu'ils décident de s'inscrire auprès du service Facebook). Selon Facebook, l'utilisation du cookie « fr » placé lors de la visite de sites Web 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'informations sur leur public. Contrairement aux « modules sociaux », 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 à des fins publicitaires les informations collectées à l'aide de pixels (par exemple, pour montrer ultérieurement, sur Facebook, aux visiteurs de leur site Web des publicités ciblées) ou pour **[Or. 34] [Or. 35]** obtenir des statistiques dites « 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. Leurs pixels 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 qu'il ressort du rapport de recherche de 2015 susmentionné 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 son 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 de module social de Facebook, son navigateur établissait généralement une connexion automatique avec le serveur de Facebook dans le but de récupérer le module. En raison de cette connexion, les informations contenues dans le cookie datr de Facebook (enregistrées sur le disque dur de l'utilisateur) étaient 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 février 2017, la Commission vie privée fait valoir 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 son service 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 d'identification persistant et unique sur le disque dur des 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 module social ayant les mêmes conséquences que celles décrites ci-dessus : les informations des cookies Facebook, enregistrées sur le disque dur de l'internaute, sont envoyées aux serveurs de Facebook, qui savent que cet internaute spécifique a navigué sur un site Web spécifique sur lequel se trouve le bouton de module social.

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 leur 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 ci-dessus, la Commission vie privée a adopté le 12 avril 2017 une recommandation d'initiative complémentaire nº 03/2017. **[Or. 36]**

VI. Les moyens [OMISSIS]

Le hof répond ci-après aux moyens des parties à la procédure [OMISSIS] [4] dans la mesure où ils aboutissent à une décision du hof, il ne motive pas argument par argument.

VI.1. Les moyens de FACEBOOK

Les parties FACEBOOK font valoir au préalable que :

> *1. Tout d'abord : la présente procédure en Belgique est entièrement dépassée et rendue obsolète par le RGPD, ce qui implique que les demandes des intimées sont irrecevables, à tout le moins inadmissibles et qu'il doit être mis fin immédiatement à la présente procédure. Cette constatation se base sur les éléments suivants :*
>
> – *Le hof ne peut plus traiter les demandes concernant les faits antérieurs au 25 mai 2018 [OMISSIS]. L'article 32, paragraphe 3, WVP a été abrogé par le RGPD et la nouvelle loi du 3 décembre 2017 portant création de l'APD. Si les intimées (ou même l'APD) ne peuvent plus engager une procédure sur la base de l'article 32, paragraphe 3, WVP contre une entité, alors il doit également être mis fin à la présente procédure.*
>
> *Si le hof devait confirmer les mesures ordonnées par le jugement, cela permettrait la mise en œuvre (et cela, pour une durée indéfinie) d'un ordre manifestement obsolète de cesser certaines activités, basé sur des faits anciens et imposé sous l'empire d'une loi qui a entre-temps été abolie. Le hof ne peut pas prendre le risque d'adopter une décision*

[4] [OMISSIS]

qui pourrait être contraire aux résultats des procédures formelles d'enquête relatives aux pratiques de Facebook Ireland, actuellement menées par le Data Protection Commissioner (commissaire à la protection des données) irlandais [5].

– *En ce qui concerne les faits postérieurs au 25 mai 2018* [OMISSIS], *il est indiscutable que les intimées ne sont pas compétentes pour enquêter sur les activités de traitement litigieuses, ni pour prendre des décisions les concernant. Le RGPD a abrogé les législations nationales en matière de protection de la vie privée dans l'ensemble de l'Union, y compris la WVP, et a mis en place un cadre de droit matériel et procédural tout à fait nouveau, que les autorités de surveillance de l'Union sont tenues de respecter. Ces règles, qui sont applicables à compter du 25 mai 2018, prévoient un mécanisme de « one-stop-shop » (guichet unique) auprès de l'autorité de contrôle chef de file de l'État membre dans lequel le responsable du traitement des données a son établissement principal. Ce principe de « guichet unique » a été confirmé explicitement dans les communiqués de presse des trois institutions principales de l'Union (à savoir, le Conseil, la Commission et le Parlement européen)* [6] *ainsi que* **[Or. 37]** *par les [prédécesseurs des] intimées dans leurs dernières conclusions devant le rechtbank van eerste aanleg (tribunal de première instance)* [7].

Facebook Ireland est l'établissement principal du responsable du traitement dans l'Union et son siège se situe à Dublin. C'est donc, conformément au RGPD, le Data Protection Commissioner (commissaire à la protection des données) irlandais qui est l'« autorité chef de file » pour enquêter sur les activités de Facebook Ireland. Comme indiqué précédemment, cela a également été reconnu publiquement par le [prédécesseur de la première intimée], comme l'ont fait d'autres autorités de contrôle également.

– *Même à supposer que les intimées soient considérées comme compétentes pour appliquer et faire respecter l'article 129 WE (quod non), elles ont elles-mêmes déjà reconnu que leur compétence est basée sur le lien entre ces dispositions et la législation en matière de protection de la vie privée. Si les intimées sont compétentes concernant l'article 129 WEC parce qu'elles étaient compétentes concernant la WVP* [8] *alors elles ne peuvent pas être compétentes concernant l'article 129 WEC lorsqu'elles ne le sont plus pour*

5 [OMISSIS]

6 [OMISSIS]

7 [OMISSIS]

8 Voir ci-après, section 3.6.

appliquer et imposer le respect de la législation e matière de protection de la vie privée, c'est-à-dire le RGPD. D'autres autorités de contrôle, comme la CNIL (Commission nationale de l'informatique et des libertés) française, ont déjà transmis au Data Protection Commissioner (commissaire à la protection des données) irlandais, en sa qualité d'« autorité de contrôle chef de file », des plaintes concernant les pratiques en matière de cookies du service Facebook (concernant tant le RGPD que la directive vie privée et communications électroniques) [OMISSIS].

2. Les appelantes ne considèrent pas qu'il serait utile au hof que les faits postérieurs au 25 mai 2018 soient examinés ici, étant donné qu'ils échappent manifestement à la présente procédure et qu'ils font déjà l'objet, sur la base du RGPD, d'un contrôle et d'un examen séparés par le Data Protection Commissioner (commissaire à la protection des données) irlandais ».

Elles développent ensuite les moyens suivants :

[OMISSIS] [premier moyen, concernant la compétence au niveau international : le hof tranche définitivement cette question et le sujet n'est pas abordé dans la question préjudicielle] **[Or. 38]**

3. Deuxième moyen : les demandes à l'encontre de Facebook Belgium sont irrecevables, étant donné que Facebook Belgium n'est pas le responsable du traitement des données litigieux ni le prestataire du service Facebook. Dès lors, elle ne peut être tenue responsable d'aucune des violations prétendues de la WVP ou de la WEC, et elle ne peut pas non plus exécuter les mesures demandées à cet égard, si ces lois devaient être considérées applicables (quod non). L'application par les intimées des affaires Google Espagne et pages fan [9] *est manifestement incorrecte* [10]*. Les demandes présentées par les intimées sont en outre inadmissibles ab initio, comme expliqué ci-après* [OMISSIS]. *Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes.*

4. Troisième moyen : la demande [du prédécesseur] de la première intimée est irrecevable étant donné que celui-ci n'avait pas qualité pour agir pour présenter des demandes en sa qualité de président de la [Commission vie privée], étant donné qu'il ressort du droit belge que seule la

9 Arrêt du 13 mai 2014, Google Spain et Google (C-131/12, EU:C:2014:317) (dans la procédure opposant *Google Spain SL et Google Inc. à Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*). [Ndt : en visant l'affaire "pages fan", l'auteur fait probablement référence également à l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388) (voir note de bas de page 7)]

10 [OMISSIS]

[Commission vie privée, à laquelle est venue aux droits la] seconde intimée (par l'intermédiaire de son président, agissant en son nom) pouvait engager des procédures sur la base de l'article 32, paragraphe 3, WVP (abrogé depuis). Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes, mais a toutefois jugé que l'action avait été engagée conformément aux dispositions de l'article 32, paragraphe 3, WVP. En tout état de cause, étant donné qu'il n'est plus, depuis le 25 mai 2018, membre [du prédécesseur] de la première intimée, il ne dispose plus de la compétence ni de la qualité pour engager cette action. La tentative des [prédécesseurs des] intimées, dans leurs conclusions d'appel, de se faire remplacer par l'APD et la poursuite prétendue de leurs demandes par cette dernière ne résout pas l'exception d'irrecevabilité invoquée par les appelantes dès le début du traitement de l'affaire au fond en première instance.

5. Quatrième moyen : sur la base de l'article 109 de la wet van 3 december 2017 (loi du 3 décembre 2017) sur l'APD, la base juridique réelle de la demande des [prédécesseurs des] intimées, à savoir l'article 32, paragraphe 3, WVP, a été tout simplement abrogée avec l'ensemble du chapitre dont cet article faisait partie. Par conséquent, à compter du 25 mai 2018, il n'y a plus de base juridique pour une **[Or. 39]** *action intentée par les [prédécesseurs des] intimées, sur la base de faits antérieurs au 25 mai 2018. En outre, la procédure concernant les faits antérieurs au 25 mai 2018 est devenue sans objet. Les intimées demandent pour l'avenir des mesures valables, sans aucune date de fin. Si les intimées devaient poursuivre cette procédure manifestement obsolète (sur la base d'une loi abrogée et de faits obsolètes), cela entraînerait des conséquences inadmissibles et discriminantes à l'égard des appelantes – même si cela ne portait que sur des faits antérieurs au 25 mai 2018 – en les désavantageant à l'égard d'autres opérateurs du marché qui ne sont pas tenus de respecter une injonction juridique basée sur une loi désormais obsolète.*

a) Le hof ne peut pas exiger que le service Facebook ne place ou ne reçoive des données issues de cookies que sur la base d'un consentement reçu de la manière spécifique dictée par l'APD belge sur la base de l'analyse subjective de cette dernière, qui interprète la loi sur la vie privée (WVP). Dans le cadre du RGPD, il existe de nouvelles règles relatives à l'acceptation du consentement comme base légale [11] S'il était possible pour le hof de confirmer les mesures postérieures au 25 mai 2018, il réglementerait de facto un comportement du passé de Facebook Ireland, qui fait l'objet d'une loi abrogée, et cela au moyen d'une injonction orientée vers l'avenir qui négligerait la législation

11 Voir article 4, point 11, article 6 et article 7, RGPD et orientations relatives au consentement au titre du règlement nº 2016/679 [OMISSIS].

actuelle tant en ce qui concerne les règles de droit matériel que celles relatives à la compétence. Par exemple, il ne serait ainsi pas possible pour le service Facebook de respecter aucune des exigences de la nouvelle législation (le RGPD et le futur règlement relatif à la vie privée et aux communications électroniques) qui dérogent aux dispositions des mesures imposées.

b) *Cela s'opposerait en outre aux enquêtes actuellement en cours auprès du Data Protection Commissioner (commissaire à la protection des données) irlandais à la suite des plaintes RGPD mentionnées ci-dessus* [OMISSIS]. *La Commission vie privée (désormais l'APD) ne saurait se voir autorisée à contourner de cette manière le RGPD (et la future réglementation relative à la vie privée, telle que le règlement relatif à la vie privée et aux communications électroniques à venir) en poursuivant des procédures parallèles et indépendantes concernant l'application des législations nationales de protection des données.*

c) *En outre, si le hof devait poursuivre la présente procédure, plusieurs critères pour l'acceptation du « consentement » existeraient en parallèle dans un seul et unique cadre juridique : un pour le service Facebook et un autre pour tous les autres services de la société de l'information disponibles sur l'Internet. Le hof n'est pas en mesure de conseiller les règles (y compris les règles de politique) que les autorités de contrôle devraient appliquer dans le cadre de leur contrôle administratif concernant le service Facebook.*

d) *Les juridictions belges ne peuvent pas non plus allonger la durée de validité des mesures imposées dès lors que les nouvelles règles tant de droit matériel que de compétence prévues dans le RGPD doivent être respectées, en raison de l'interdépendance entre la WEC et le RGPD (comme les intimées l'ont à plusieurs reprises reconnu) et de la réforme prévue de la directive vie privée et communications électroniques 2002/58/CE par le futur règlement vie privée et communications électroniques (qui deviendra la lex specialis pour l'application des règles de protection des données sur les cookies et technologies similaires)* **[Or. 40]**

6. Cinquième moyen : depuis l'entrée en vigueur du RGPD et de la législation belge correspondante, les demandes relatives à des faits postérieurs au 25 mai 2018 sont irrecevables. Le RGPD consolide la règle du guichet unique qui s'applique à toutes les initiatives et interventions des autorités de contrôle dans l'exercice de leurs compétences. Les [prédécesseurs des] intimées [eux]-mêmes l'ont reconnu dans leurs

dernières conclusions de synthèse devant le rechtbank van eerste aanleg (tribunal de première instance). L'ensemble de la procédure, les conséquences du jugement et les sanctions et astreintes qu'il inflige ne pourront plus produire d'effets après le 25 mai 2018 (outre le fait qu'il convient en tout état de cause de les annuler).

7. *Sixième moyen : en outre, les demandes sont en soi irrecevables sur la base de l'article 129 WEC, et le président de la [Commission vie privée, à laquelle est venue aux droits la] seconde intimée ne dispose en tout cas d'aucune compétence pour, sur la base de l'article 32, paragraphe 3, WVP (entre-temps abrogé et remplacé, et qui se limitait à l'application de la WVP), introduire une action fondée sur la WEC. Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes et il a jugé que le législateur n'avait pas pu avoir l'intention d'accorder des compétences à la Commission vie privée de manière restrictive et que les compétences qui avaient été conférées à un autre régulateur, à savoir l'Institut belge des services postaux et des télécommunications (ci-après l'« IBPT »), ne faisaient pas obstacle à celles de la Commission vie privée. En tout état de cause, l'entrée en vigueur du RGPD le 25 mai 2018 rend irrecevable ou inadmissible et/ou non fondée, à compter de cette date, toute poursuite de la présente action.*

8. *Septième moyen : la nouvelle demande concernant l'utilisation de pixels (y compris pour recevoir des données de cookies) a été introduite tardivement dans la procédure et devait donc être déclarée irrecevable. Cette pratique de Facebook Ireland existait déjà au moment de la citation, qui date du 11 septembre 2015. [Le prédécesseur de] la première intimée n'a dénoncé l'utilisation de pixels pour la première fois que dans ses premières conclusions du 31 janvier 2017 et [il] a présenté dans ces conclusions une nouvelle demande concernant cette utilisation de pixels, sans que même une position administrative de la [Commission vie privée, à laquelle est venue aux droits la] seconde intimée existe sur ce point, encore moins qu'elle soit communiquée aux appelantes. La [Commission vie privée, à laquelle est venue aux droits la] seconde intimée a elle-même pris position pour la première fois à cet égard après avoir rédigé un rapport technique, daté du mois de février 2017, dans une recommandation du 12 avril 2017. Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes et a également déclaré recevable la demande relative aux pixels.*

9. *Huitième moyen : même à supposer que le hof soit compétent (quod non), le droit belge ne s'applique pas à la résolution du litige, qui est soumise au droit de l'État membre dans lequel le responsable du traitement est établi. Comme les juridictions de l'Union l'ont déjà jugé, il s'agit, en l'espèce, de Facebook Ireland (en tant que responsable du traitement des données) et celle-ci est établie en Irlande, État membre de l'Union.*

a. *Le critère juridique correct pour déterminer la législation applicable en vertu de l'article 4, point 1) sous a), de la directive 95/46/CE (qui a depuis lors été abrogé) (y compris la signification des termes « dans le cadre [des activités] », comme l'a précisé l'arrêt « pages fan » de la Cour [12]) aurait indiscutablement dû aboutir à l'applicabilité du droit irlandais. Facebook Ireland était la responsable au niveau européen pour le traitement de données en cause et elle offrait le service Facebook uniquement à des intéressés dans l'Union européenne. Facebook Ireland a déterminé l'objectif et les moyens pour le traitement de toutes les* **[Or. 41]** *données de cookies dans le litige en cause en l'espèce, ainsi que de toutes les données personnelles concernant les utilisateurs du service Facebook, et elle était donc le seul établissement du groupe Facebook dans le cadre duquel le traitement des données contesté avait lieu. En revanche, Facebook Belgium exerçait des activités qui n'avaient rien à voir avec le traitement de données litigieux.*

b. *Même si le droit belge était applicable* (*quod non*)*, l'arrêt « pages fan » permet de conclure que la seconde intimée ne disposait d'aucune compétence à l'égard de Facebook Ireland et de Facebook, Inc. Les intimées n'auraient pu être compétentes que pour intervenir à l'égard de « l'entité établie sur [leur] territoire », à savoir Facebook Belgium.*

c. *En tout état de cause, le RGPD formalise le mécanisme de guichet unique et ce principe assure, de manière univoque, que les activités transfrontalières de traitement des données dans l'Union, depuis le 25 mai 2018, relèvent de la compétence d'une seule et unique autorité de protection des données, qui intervient en tant qu'autorité de contrôle : l'autorité de l'État membre dans lequel le responsable du traitement des données a son établissement principal, en l'espèce Facebook Ireland*.

10. *Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes et a jugé que le droit belge était applicable en l'espèce.*

11. *Neuvième moyen : même à supposer que le hof soit compétent et que le droit belge en matière de protection de la vie privée soit applicable (quod non), Facebook Ireland disposait d'une base juridique légitime en vertu du droit belge pour les activités de traitement des données litigieuses, y compris l'obtention d'un consentement valable, lorsque celui-ci était exigé, des utilisateurs du service Facebook pour utiliser des cookies, au moyen de sa procédure d'enregistrement, de son bandeau cookies et de sa politique de*

12 Arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388).

cookies. En ce qui concerne les pixels proposés par Facebook Ireland à des sites Web tiers, Facebook Ireland les a mis à disposition sous la condition contractuelle expresse (renforcée par des rappels régulièrement transmis à cet effet dans les applications de service) que ces sites Web tiers doivent avoir une base juridique valide pour le traitement des données personnelles des visiteurs, y compris, le cas échéant, l'obtention du consentement approprié, le tout précisément conformément à la recommandation publiée par la [Commission vie privée, à laquelle est venue aux droits la] seconde intimée pour des milliers d'entreprises utilisant des pixels et modules sur des sites Web tiers. Cela est tout à fait conforme aux pratiques courantes de l'industrie. Facebook Ireland a également justifié le traitement pour d'autres motifs prévus à l'article 5 de l'ancienne WVP et à l'article 129 WEC et les données, obtenues au moyen de ces cookies, ont également été traitées conformément aux articles 4 et 9 WVP. Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes. Il a jugé, à tort, que chacune des dispositions susmentionnées de la WVP et de la WEC avait été enfreinte.

[OMISSIS] [moyen relatif à l'indépendance des défendeurs, sans aucun rapport avec les questions préjudicielles]

12. [OMISSIS] **[Or. 42]** [OMISSIS] [moyen relatif à la nature des mesures imposées par la première juridiction, sans aucun lien avec les questions préjudicielles]

13. [OMISSIS] [moyen relatif à la recevabilité de l'intervention volontaire de la Commission vie privée en première instance]

14. [OMISSIS].

15. [OMISSIS] »

VI.2. Les moyens de l'APD

L'APD invoque les moyens suivants :

1. « [OMISSIS] [13] [moyen concernant la compétence au niveau international : le hof tranche définitivement au fond cette question et le sujet n'est pas abordé dans la question préjudicielle]

[OMISSIS] **[Or. 43]** [14] [OMISSIS] **[Or. 44]** [OMISSIS] **[Or. 45]** [OMISSIS] **[Or. 46]** [OMISSIS] **[Or. 47]** [OMISSIS] **[Or. 48]**

En ce qui concerne la recevabilité :

13 [OMISSIS]

14 [OMISSIS]

2. Deuxième moyen : l'allégation de Facebook selon laquelle l'action contre Facebook Belgium serait irrecevable parce que cette dernière ne s'occupe que du marketing et de la vente d'espaces publicitaires et d'activités de lobbying et ne serait pas elle-même impliquée dans le traitement des données personnelles en cause, de sorte qu'elle ne serait pas le destinataire correct de l'action, est dénuée de fondement. En effet, la question de savoir si Facebook Belgium commet ou non des erreurs et si elle est donc (conjointement) responsable ou non des violations ne concerne pas la recevabilité mais le fond de l'action.

En outre, même à supposer que la question de savoir si Facebook Belgium est ou non le destinataire correct de l'action dans le cadre de la présente procédure, étant donné qu'elle ne s'occupe que du marketing et de la vente d'espaces publicitaires et d'activités de lobbying et qu'elle n'intervient pas elle-même dans le traitement des données personnelles en cause, concerne la recevabilité de la réclamation (quod non), Facebook Belgium est toujours un destinataire correct de l'action et l'action exercée à son encontre est bel et bien admissible. Si, sur la base de l'article 4 de la directive 95/46, le droit belge en matière de protection de la vie privée est applicable, l'autorité de contrôle belge en ce qui concerne le traitement des données à caractère personnel dont Facebook Inc. et/ou Facebook Ireland sont responsables peut en effet également agir contre la succursale Facebook Belgium basée en Belgique, et l'action contre Facebook Belgium est donc admissible. Cela ressort de l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), qui concerne le groupe Facebook et dans lequel la Cour a jugé qu'il ressortait des articles 4 et 18 de la directive 95/46 que « lorsqu'une entreprise établie en dehors de l'Union européenne dispose de plusieurs établissements dans différents États membres, l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre, alors même que, en vertu de la répartition des missions au sein du groupe, d'une part, cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire dudit État membre et, d'autre part, la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union européenne, à un établissement situé dans un autre État membre ». Étant donné qu'en l'espèce, jusqu'au 25 mai 2018, le droit belge en matière de protection de la vie privée était applicable, l'action engagée contre Facebook Belgium était bel et bien admissible.

3. Troisième moyen : l'allégation de Facebook laquelle il découlerait des « principes fondamentaux du marché intérieur » et de l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388) que l'APD ne pouvait agir que contre Facebook Belgium et non contre Facebook Inc. et Facebook Ireland et que, par conséquent, l'action à l'encontre de Facebook Inc. et de Facebook Ireland serait irrecevable est inexacte. En effet, la directive 95/46 n'impose en aucun cas que le droit à la vie privée d'un seul État membre soit applicable dans l'ensemble de l'Union ni qu'une seule autorité de contrôle soit

compétente. Par ailleurs, la question préjudicielle posée dans l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388) ne portait pas sur la possibilité de poursuivre un responsable du traitement établi dans un autre État membre, mais sur la possibilité de poursuivre également un simple établissement de vente et de marketing qui n'a aucune responsabilité dans le traitement. L'allégation de Facebook équivaut à considérer qu'aucune autorité de contrôle d'un État membre de l'Union ne pourrait agir à l'encontre de ce responsable et que seul cet établissement de vente et de marketing pourrait être poursuivi.

En outre, l'allégation de Facebook (tout à fait incorrecte) selon laquelle la Cour aurait **[Or. 49]** *jugé dans cet arrêt que l'autorité de contrôle de l'État membre dans lequel le responsable du traitement a un établissement ne pourrait agir que contre cet établissement et non contre le responsable qui est établi dans un autre État membre, implique encore autre chose. En effet, cela signifie que la Commission vie privée ou l'APD peut, en l'espèce et en tout état de cause, agir à l'encontre de Facebook Inc. Il s'agit en effet d'un responsable qui n'est pas établi dans un État membre de l'Union.*

[OMISSIS] [moyen concernant la recevabilité de l'intervention volontaire de la Commission vie privée en première instance]

5. Cinquième moyen : Facebook prétend que l'action concernant des faits antérieurs au 25 mai 2018 serait devenue irrecevable parce que 1) le 24 mai 2018, conformément à l'article 114 de la loi APD, le mandat du président de la Commission vie privée aurait pris fin, et 2) l'intérêt et la qualité de l'[APD] pour poursuivre cette procédure concernant des faits antérieurs au 25 mai 2018 auraient été «éteints », du fait que l'article 32, paragraphe 3, WVP a été abrogé à compter du 25 mai 2018 en vertu des articles 109 et 110 de la loi APD. Il n'en est rien.

Premièrement, le fait que le mandat du président de la Commission vie privée a pris fin le 24 mai 2018 parce que la Commission vie privée a cessé d'exister est en effet dépourvu de pertinence car, lors de l'introduction de cette procédure, la partie effective au procès était la Commission vie privée et non son président. Conformément à l'article 3, premier et deuxième alinéas, de la loi APD, l'APD succède à la Commission de la protection de la vie privée à compter du 25 mai 2018. L'APD vient donc aux droits de la Commission de la protection de la vie privée dans la présente procédure, et reprend l'instance à toutes fins utiles.

Deuxièmement, l'abrogation de l'article 32, paragraphe 3 WVP n'entraîne en aucune manière l'irrecevabilité de l'action en ce qui concerne des faits antérieurs au 25 mai 2018. Sur la base de l'article 6 de la loi APD, qui succède à compter du 25 mai 2018 à l'article 32, paragraphe 3, WVP, l'APD conserve en effet la possibilité d'intenter une action en justice.

La qualité et l'intérêt de la Commission vie privée dans la présente procédure ont donc été tout simplement transmis à son successeur, l'APD. Il n'est pas question d'une « extinction » de la qualité et de l'intérêt du fait de l'abrogation de l'article 32, paragraphe 3, WVP.

En outre, même si par impossible le hof devait juger que, sur la base des considérations qui précèdent, l'APD n'aurait plus qualité pour agir, alors le recours en appel de Facebook serait irrecevable étant donné que les conséquences seraient valables pour toutes les parties à la procédure, conformément à la jurisprudence constante de la Cour de cassation. En effet, il n'y aurait plus dans ce cas de partie adverse disposant de la qualité à cet effet à l'encontre de laquelle Facebook pourrait encore exercer son recours en appel.

6. Sixième moyen : Facebook prétend à tort que l'APD ne pourrait pas **[Or. 50]** *poursuivre la procédure et ne pourrait pas engager d'action concernant des faits postérieurs au 25 mai 2018, parce que l'APD ne serait pas l'autorité de contrôle chef de file concernant les traitements transfrontaliers de Facebook en cause. Cette allégation est cependant tout à fait erronée.*

Premièrement, il est inexact que l'autorité de contrôle chef de file disposerait de toutes les compétences s'agissant des traitements transfrontaliers. Le mécanisme de guichet unique implique qu'un responsable du traitement ayant plusieurs établissements ou un établissement unique dans l'Union se voit attribuer une autorité de contrôle déterminée comme unique interlocuteur pour un traitement transfrontalier. Il s'agit de l'autorité de contrôle de l'État membre dans lequel le responsable du traitement a son établissement principal dans l'Union, qui devient alors l'autorité de contrôle « chef de file ». Le mécanisme de guichet unique, tel qu'établi par l'article 56, paragraphe 1, RGPD, reste cependant une règle d'exception. La règle fondamentale demeure que toute autorité de contrôle peut exercer sur son territoire les compétences dont elle est investie par le RGPD, comme le prévoit expressément l'article 55, paragraphe 1, RGPD.

Deuxièmement, le mécanisme de guichet unique ne fait pas du tout obstacle à la qualité d'une autorité de contrôle pour agir en justice. Le RGPD fait une distinction claire, en ce qui concerne les pouvoirs d'exécution d'une autorité de contrôle, entre un parcours administratif et un parcours judiciaire. Le parcours administratif, dans le cadre duquel une autorité de contrôle prend elle-même des mesures d'application, est régi par les articles 58, paragraphes 1, 2 et 3, RGPD et relève du mécanisme de guichet unique. En revanche, le parcours judiciaire, dans le cadre duquel une autorité de contrôle engage une procédure judiciaire, ne relève pas du mécanisme de guichet unique. En effet, cela ressort clairement de l'objectif du mécanisme de guichet unique, qui vise uniquement à garantir la cohérence dans l'interprétation et l'application du droit de protection de la vie privée par les autorités de contrôle. Pour l'application et l'interprétation par les instances judiciaires, un autre système existe déjà, à savoir la possibilité d'adresser une demande de décision préjudicielle à la Cour. En outre, l'article 81 RGPD prévoit un mécanisme séparé et optionnel de consultation, de

suspension et de désaisissement pour les juridictions. Par ailleurs, le rôle de l'autorité de contrôle chef de file dans le cadre du mécanisme de guichet unique ne saurait être interprété trop largement. Enfin, le libellé de l'article 58, paragraphes 5 et 6, RGPD, la genèse du RGPD et la mise en œuvre du RGPD en Belgique amènent à conclure que le mécanisme de guichet unique ne concerne pas le parcours judiciaire prévue à l'article 58, paragraphe 5, RGPD. Le législateur belge a d'ailleurs souligné dans le cadre des travaux parlementaires en ce qui concerne l'article 6 de la loi APD que l'APD conserve la possibilité de porter toute affaire à l'attention des autorités judiciaires.

Troisièmement, l'application du mécanisme de guichet unique aurait des conséquences absurdes sur la qualité pour saisir le parquet, un juge d'instruction ou un tribunal. En effet, cela aboutirait, entre autres, à ce que l'APD ne pourrait pas porter à la connaissance du parquet ou d'un juge d'instruction des infractions concernant le traitement transfrontalier sur le territoire belge, même si elles sont passibles de sanctions pénales.

Quatrièmement, même si par impossible le hof devait juger que la qualité d'une autorité de contrôle pour engager une procédure judiciaire sur son territoire relève du mécanisme de guichet unique (quod certe non), aucune disposition du RGPD ne prévoit que celui-ci a pour effet de mettre fin à toutes les procédures déjà engagées au 25 mai 2018, même si elles portent sur des infraction au RGPD postérieures au 25 mai 2018. **[Or. 51]**

Cinquièmement, l'APD demande qu'en aucun cas le présent moyen ne soit rejeté sans qu'une question préjudicielle ait été au préalable posée à la Cour de justice [OMISSIS]. *Il s'agit en effet de questions très importantes relatives à l'interprétation du droit de l'Union en cause, droit qui est nouveau, et la problématique dépasse également le présent litige et affecte la compétence d'autres autorités de contrôle dans d'autres États membres quant aux traitements transfrontaliers.*

En outre, même si par impossible le hof devait juger que, sur la base des considérations qui précèdent, l'APD n'aurait plus qualité pour agir, alors le recours en appel de Facebook serait irrecevable étant donné que les conséquences seraient valables pour toutes les parties à la procédure, conformément à la jurisprudence constante de la Cour de cassation. En effet, il n'y aurait plus dans ce cas de partie adverse disposant de la qualité à cet effet à l'encontre de laquelle Facebook pourrait encore exercer son recours en appel.

[OMISSIS] [moyen de droit national de la procédure, sans aucun lien avec les questions préjudicielles]

8. Huitième moyen : il convient de rejeter car dénuée de fondement l'allégation de Facebook selon laquelle l'action serait irrecevable parce qu'elle est basée sur l'article 129 WEC. **[Or. 52]**

Premièrement, l'article 32, paragraphe 3, WVP constitue effectivement une base permettant à la Commission vie privée d'engager une action en raison de la violation de l'article 129 WEC. En effet, l'article 129 WEC « spécifie et complète » la WVP, car l'article 129 WEC est la transposition de l'article 5, paragraphe 3, de la directive 2002/58 et l'article 1er, paragraphe 2, de la directive 2002/58 dispose que « [l]es dispositions de la présente directive précisent et complètent la directive 95/46/CE ». En outre, la WVP était incorporée dans l'article 129 WEC, car tant les « informations » visées par l'article 129, premier alinéa, 1°, WEC que le « consentement » visé à l'article 129, premier alinéa, 2°, WEC, sont ceux définis dans la WVP, et l'article 129 WEC dispose que le responsable, outre les obligations relatives aux informations et au consentement, est tenu de respecter toutes les autres obligations imposées par la WVP. Par conséquent, en cas de traitement de données personnelles, par exemple par la collecte de cookies, l'article 129 WEC implique que les règles de la WVP sont également appliquées. Il s'ensuit nécessairement que la Commission vie privée était également compétente pour le contrôle de celui-ci. Par conséquent, il convient de rejeter car dénuée de fondement la demande de Facebook visant à déclarer l'action irrecevable au motif qu'elle est basée sur l'article 129 WEC.

Deuxièmement, l'allégation de Facebook selon laquelle seul l'IBPT et non la Commission vie privée pourrait engager une action en raison de la violation de l'article 129 WEC est incorrecte. L'article 129 WEC, qui transpose l'article 5, paragraphe 3, de la directive 2002/58 en droit belge, porte également sur les « services de la société de l'information », comme les réseaux sociaux en ligne (par exemple, celui de Facebook) car, parmi les exceptions à l'exigence de consentement, l'article 5, paragraphe 3, de la directive 2002/58 prévoit la situation dans laquelle un cookie est strictement nécessaire pour la fourniture d'un « service de la société de l'information demandé par l'abonné ». Si cet article 5, paragraphe 3, n'était pas applicable à des services de la société de l'information, il ne serait pas nécessaire de prévoir une exception pour certains de ces services. Étant donné que le champ d'application de la WEC est limité, conformément à l'article 1er, paragraphe 1, à l'article 2, sous c), de la directive-cadre 2002/21 et à l'article 2, 5° WEC, aux « service de communications électroniques », et que les « services de la société de l'information » sont exclus de la notion de « services de communications électroniques », l'IBPT n'est compétent qu'en ce qui concerne les « service de communications électroniques » et non pour les « services de la société de l'information ». Par conséquent, il n'est pas non plus compétent en ce qui concerne le traitement de données personnelles lors de l'utilisation de cookies dans le cadre de services de la société de l'information ; concernant ces derniers, la Commission vie privé est exclusivement compétente.

Troisièmement, même à supposer que l'IBPT fût compétente pour le traitement de données personnelles lors de l'utilisation de cookies dans le cadre de services de la société de l'information (quod non), la Commission vie privée restait en tout état de cause compétente, ne serait-ce que concurremment. Dans tous les cas où la WEC régit, par des dispositions spécifiques, le traitement de données

personnelles dans le secteur des communications électroniques, non seulement l'organisme de surveillance sectoriel IBPT est compétent, mais également la Commission vie privée (en qualité d'organisme de surveillance général).

En ce qui concerne le bien-fondé :

9. Neuvième moyen : le traitement, par Facebook, de données personnelles des utilisateurs au moyen des cookies, modules sociaux et pixels enfreignait, jusqu'au 25 mai 2018, la WVP et l'article 129 WEC, et enfreignent depuis le 25 mai 2018, le RGPD et l'article 129 WEC, en ce que :

10. Premièrement, Facebook n'obtient aucun consentement valable, alors que celui-ci est exigé sur la base de l'article 5 WVP, de l'article 6 RGPD et de l'article 129 WEC. Pour être valable, le consentement de l'intéressé doit être 1) univoque, 2) libre, 3) éclairé (reposant sur des informations), et 4) spécifique. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples (article 7, paragraphe 2, RGPD). En outre, il doit être aussi simple de retirer que de donner son consentement (article 7, paragraphe 3, RGPD). Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat (article 7, paragraphe 4, RGPD).

Malgré les modification (limitées) qu'elle a apportées depuis le jugement de première instance, Facebook n'obtient pas encore de consentement valable, parce que : 1) les actes dont elle estime déduire un « consentement » ne sont pas univoques, 2) les intéressés ne **[Or. 53]** *disposent pas de la possibilité de refuser leur consentement ou de le retirer sans subir de conséquences défavorables, 3) il n'a pas été remédié aux lacunes dans les informations fournies par Facebook aux intéressés, 4) les intéressés ne disposent pas de la possibilité d'accepter certains cookies ou l'ensemble de ceux-ci, ou de refuser certains cookies ou l'ensemble de ceux-ci, 5) les lacunes dans les possibilités de choix offertes par Facebook sont toujours présentes, 6) il n'est pas aussi simple de retirer que de donner son consentement, et 7) Facebook ne peut pas aussi simplement répercuter sa responsabilité en ce qui concerne le placement et la collecte de cookies au moyen de pixels sur les exploitants de sites Web tiers.*

11. Deuxièmement, en plaçant et collectant ses cookies au moyen de ses modules sociaux et pixels, Facebook a enfreint systématiquement et à grande échelle, jusqu'au 25 mai 2018 les exigences de qualité énoncées à l'article 4 WVP et à compter du 25 mai 2018 les exigences de qualité énoncées à l'article 5, paragraphe 1, RGPD. 1) Premièrement, Facebook a enfreint le principe de loyauté énoncé à l'article 4, paragraphe 1, 1°, WVP, ce qu'elle continue à faire

depuis que ce principe figure à l'article 5, paragraphe 1, sous a), RGPD, en fournissant des informations vagues et équivoques, non adaptées au groupe cible et qui de surcroît induisent en erreur. 2) Deuxièmement, Facebook a enfreint le principe de finalité énoncé à l'article 4, paragraphe 1, 2°, WVP, ce qu'elle continue à faire depuis que ce principe figure à l'article 5 paragraphe 1, sous b), RGPD, en ignorant les attentes raisonnables des intéressés et les dispositions légales applicables.(3) Troisièmement, Facebook a enfreint le principe de proportionnalité énoncé à l'article 4, paragraphe 1, 3°, WVP, ce qu'elle continue à faire depuis que ce principe figure à l'article 5 paragraphe 1, sous c) RGPD, tant pour les cookies publicitaires que pour les cookies de sécurité, du fait que les traitements sont dans tous les cas identifiés excessifs, et en ce qui concerne les cookies de sécurité, du fait qu'ils ne sont pas pertinents ni suffisants.

12. Troisièmement, Facebook a déjà enfreint l'obligation de transparence visée à l'article 9 WVP avec son bandeau cookies et ses politiques antérieures de cookies et en matière de données. Depuis l'entrée en vigueur du RGPD le 25 mai 2018, Facebook ne respecte pas non plus les obligations plus larges de transparence, définies par les articles 12 et 14 RGPD, malgré les adaptations de sa politique de cookies et de sa politique en matière de données.

*13. Quatrièmement, Facebook enfreint, depuis le 25 mai 2018, les obligations relatives à la protection des données dès la conception et de protection des données par défaut, définies à l'article 25 * RGPD, du fait qu'elle n'a pas pris de mesures techniques et organisationnelles pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.*

14. À cet égard, il convient d'observer que Facebook ne peut (toujours) pas invoquer les autres fondements de compatibilité, définis à l'article 5 WVP et à l'article 6 RGPD, parce que l'article 129 WEC prescrit expressément le consentement. De surcroît, les conditions pour ces autres fondements de compatibilité, fixées à l'article 5, sous b) et sous f) WVP et à l'article 6, paragraphe 1, sous b) et sous f) RGPD ne sont pas remplies. Le traitement de données personnelles issues de cookies collectés par Facebook au moyen de modules sociaux et pixels sur des sites Web tiers n'est, en effet, pas nécessaire pour l'exécution de l'accord avec l'intéressé ni pour la sauvegarde des intérêts invoqués par Facebook.

15. Il convient d'observer également à cet égard que Facebook ne saurait se prévaloir de l'exception figurant à l'article 129, deuxième alinéa, WEC, car la collecte de cookies au moyen de pixels et de modules sociaux sur des sites Web tiers n'est pas strictement nécessaire pour fournir un service expressément demandé par l'utilisateur. **[Or. 54]**

* Ndt : il s'agit, semble-t-il, de l'article 27.

16. Dixième moyen : l'action peut être déclarée fondée à l'égard des trois sociétés Facebook, et non pas seulement à l'égard de Facebook Ireland.

L'allégation de Facebook selon laquelle l'action pourrait être déclarée non fondée à l'égard de Facebook Inc. parce que seule Facebook Ireland serait responsable du traitement et que Facebook Inc. serait simplement un sous-traitant agissant seulement sous l'autorité et selon les instructions de Facebook Ireland, est tout à fait inexacte. En effet Facebook Inc. détermine, avec Facebook Ireland, l'objectif et les moyens des traitements de données personnelles litigieux, de sorte qu'elle est, avec Facebook Ireland, la « responsable » des traitements au sens de l'article 2, sous d), de la directive 95/46, de l'article 1er, paragraphe 4, WVP et de l'article 4, paragraphe 7, RGPD. En tout cas, Facebook affirme elle-même que Facebook Inc. traite les données personnelles litigieuses, de sorte qu'elle est à tout le moins co-responsable des infractions.

L'allégation de Facebook selon laquelle l'action devrait être déclarée non fondée à l'égard de Facebook Belgium parce que celle-ci n'est pas elle-même la responsable et qu'elle n'est même pas concernée par les traitements de données personnelles litigieux, est tout à fait inexacte. Lorsque le droit belge en matière de protection de la vie privé est applicable, conformément à l'article 4 de la directive 95/46, l'autorité de contrôle belge peut en effet agir également contre l'établissement établi en Belgique, à savoir Facebook Belgium, en ce qui concerne les traitements de données personnelles dont Facebook Inc. et/ou Facebook Ireland sont les responsables et l'action engagée contre Facebook Belgium est donc fondée. Cela ressort de l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388). Cet arrêt concerne le groupe Facebook et la Cour y a jugé (point 64) qu'il ressortait des articles 4 et [28] de la directive 95/46 que « lorsqu'une entreprise établie en dehors de l'Union dispose de plusieurs établissements dans différents États membres, l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre alors même que, en vertu de la répartition des missions au sein du groupe, d'une part, cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire dudit État membre et, d'autre part, la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union, à un établissement situé dans un autre État membre ». En l'espèce, jusqu'au 25 mai 2018, le droit belge de la protection de la vie privée était applicable, de sorte que l'action peut être déclarée fondée à l'égard de Facebook Belgium.

[OMISSIS] [moyen relatif à la sanction à appliquer, sans aucun lien avec les questions préjudicielles]

[OMISSIS] [moyen relatif à l'indépendance de la Commission vie privée/de l'APD, sans aucun lien avec les questions préjudicielles] **[Or. 55]**

19. Treizième moyen : Facebook prétend pour diverses raisons que les mesures en cause ne pourraient plus être demandées. Il n'en est rien.

Ainsi, Facebook prétend à tort que la Commission vie privée ne pourrait pas demander les mesures en cause parce que l'article 32, paragraphe 3, WVP ne mentionnait pas littéralement qu'elle pouvait demander ces mesures au tribunal, et qu'elle pouvait seulement lui demander des «éclaircissements» sur les dispositions de la WVP. En effet, il ressort clairement des travaux parlementaires de la WVP et de la genèse de l'article 32, paragraphe 3, WVP qu'il était dans l'intention du législateur que le tribunal puisse prononcer, sur la demande de la Commission vie privée, un jugement exécutoire pour mettre fin à un certain traitement de données personnelles.

De même, l'allégation de Facebook selon laquelle les mesures en cause ne pourraient plus être demandées depuis le 25 mai 2018, parce qu'elles ne concernent pas seulement Facebook Belgium ou parce qu'elles auraient perdu toute pertinence, est inexacte, pour les raisons déjà exposées ci-dessus.

L'allégation de Facebook selon laquelle les mesures en cause seraient vagues, disproportionnées, illimitées dans le temps et dans l'espace, et en outre impossibles à exécuter, est inexacte. De surcroît, elle n'indique pas pourquoi ce serait le cas, de sorte qu'elle ne fournit pas la preuve qu'il lui incombe d'apporter. Par ailleurs, Facebook alléguait la même chose en ce qui concerne les mesures similaires demandées par la Commission vie privée en référé. Après que le juge des référés a jugé, en première instance, qu'il n'accordait aucun crédit à ces allégations, et qu'il a ordonné les mesures demandées, Facebook les a exécutées. Elle a de ce fait elle-même démenti ses propres allégations ».

VII. Discussion

La juridiction de céans examinera les éléments de l'affaire dans l'ordre suivant :

1. La compétence des juridictions belges.

[OMISSIS] **[Or. 56]**

2. La recevabilité des demandes en ce qu'elles sont dirigées contre Facebook Belgium bvba au moment de leur introduction

3. L'intervention de la Commission vie privée, à laquelle a succédé l'APD, et cette succession.

4. La qualité et l'intérêt de l'APD pour (encore) agir contre Facebook Belgium bvba.

5. Les questions préjudicielles posées à la Cour de justice.

6. L'intérêt et la qualité de l'APD pour agir sur la base de la WEC.

1. La compétence des juridictions belges.

[La juridiction de renvoi estime ne pas disposer de la compétence internationale pour connaître des demandes dirigées contre Facebook Ireland Ltd. et Facebook Inc., mais bien pour ce qui concerne les demandes dirigées contre Facebook [Belgium] bvba]

[OMISSIS] **[Or. 57]** [OMISSIS] **[Or. 58]** [OMISSIS] **[Or. 59]** [OMISSIS] **[Or. 60]** [OMISSIS] **[Or. 61]** [OMISSIS] **[Or. 62]** [OMISSIS] **[Or. 63]** [15][OMISSIS] **[Or. 64]** [OMISSIS] **[Or. 65]** [OMISSIS] **[Or. 66]** [OMISSIS] **[Or. 67]** [OMISSIS] **[Or. 68]** [OMISSIS] **[Or. 69]** [OMISSIS] **[Or. 70]** [OMISSIS] **[Or. 71]** [OMISSIS] **[Or. 72]** [OMISSIS] **[Or. 73]** [OMISSIS] **[Or. 74]** [OMISSIS] **[Or. 75]** [OMISSIS] **[Or. 76]** [16] [OMISSIS] **[Or. 77]** [OMISSIS] **[Or. 78]** [OMISSIS] **[Or. 79]** [OMISSIS] **[Or. 80]** [1718] [OMISSIS] **[Or. 81]** [OMISSIS] **[Or. 82]** [19][OMISSIS] **[Or. 83]** [20] [OMISSIS] **[Or. 84]** [2122] [OMISSIS] **[Or. 85]** [2324] [OMISSIS] **[Or. 86]** [OMISSIS] **[Or. 87]** [OMISSIS] **[Or. 88]** [OMISSIS] **[Or. 89]** [OMISSIS] **[Or. 90]** [25] [OMISSIS] **[Or. 91]** [OMISSIS] **[Or. 92]** [OMISSIS] [2627282930] [OMISSIS] **[Or. 93]** [31] [OMISSIS]

15 [omissis]

16 [omissis]

17 [omissis]

18 [omissis]

19 [omissis]

20 [omissis]

21 [omissis]

22 [omissis]

23 [omissis]

24 [omissis]

25 [omissis]

26 [omissis]

27 [omissis]

28 [omissis]

29 [omissis]

30 [omissis]

31 [omissis]

[Or. 94] [32] [OMISSIS] **[Or. 95]** [OMISSIS] **[Or. 96]** [33] [OMISSIS] **[Or. 97]** [34] [OMISSIS] **[Or. 98]** [OMISSIS]

2. La recevabilité des demandes en ce qu'elles sont dirigées contre Facebook Belgium bvba au moment de leur introduction

[OMISSIS] **[Or. 99]** [OMISSIS]

Dès lors que la juridiction de céans est compétente pour statuer sur la demande dirigée contre Facebook Belgium bvba, elle constate que la demande pouvait en principe être recevable [35] (voir aussi infra).

3. L'intervention de la Commission de protection de la vie privée, aux droits de laquelle est venue l'APD, et cette succession.

[La juridiction de renvoi statue sur la recevabilité de l'intervention volontaire d'une partie en première instance, sans aucun rapport avec les questions préjudicielles]

[OMISSIS] **[Or. 100]** [OMISSIS] **[Or. 101]** [OMISSIS]

4. La qualité et l'intérêt de l'APD pour (encore) agir contre Facebook Belgium

[La juridiction de renvoi juge que la demande de l'APD relative aux faits antérieurs au 25 mai 2018 est sans objet en raison du défaut de l'intérêt requis]

[OMISSIS] [3637] **[Or. 102]** [3839404142] [OMISSIS] **[Or. 103]** [OMISSIS]

32 [omissis]

33 [omissis]

34 [omissis]

35 En constatant que « *la demande est recevable en principe* », la juridiction de céans indique qu'il faudra encore vérifier « concrètement » si l'APD dispose effectivement, hic et nunc, de la qualité et de l'intérêt pour agir. La juridiction de renvoi constate seulement ici qu'une « *telle* » demande peut « *en principe* » être recevable.

36 [omissis]

37 [omissis]

38 [omissis]

39 [omissis]

40 [omissis]

41 [omissis]

4.3.

Pour la période postérieure au 25 mai 2018, les entités Facebook font valoir ce qui suit :

> « *Les demandes qui sont basées sur des faits postérieurs au 25 mai 2018 sont irrecevables, à tout le moins inadmissibles, et doivent faire l'objet d'une tout autre voie de droit, qui est prévue, en particulier, aux articles 56 et 60 du RGPD et qui est désignée, en langage courant, comme le "guichet unique"* ».

Elles exposent le moyen suivant :

> [« S*ur la base de l'article 109 de la loi APD, la base juridique réelle de la demande des [prédécesseurs des] intimées, à savoir l'article 32, paragraphe 3, WVP, a été tout simplement abrogée avec l'ensemble du chapitre dont cet article faisait partie. Par conséquent, à compter du 25 mai 2018, il n'y a plus de base juridique pour une action intentée par les [prédécesseurs des] intimées, sur la base de faits antérieurs au 25 mai 2018. En outre, la procédure concernant les faits antérieurs au 25 mai 2018 est devenue sans objet. Les intimées demandent pour l'avenir des mesures valables, sans aucune date de fin. Si les intimées devaient poursuivre cette procédure manifestement obsolète (sur la base d'une loi abrogée et de faits obsolètes), cela entraînerait des conséquences inadmissibles et discriminantes à l'égard des appelantes – même si cela ne portait que sur des faits antérieurs au 25 mai 2018 – en les désavantageant à l'égard d'autres opérateurs du marché qui ne sont pas tenus de respecter une injonction juridique basée sur une loi désormais obsolète* .] **[Or. 104]**
>
> *a) Le hof ne peut pas exiger que le service Facebook ne place ou ne reçoive des données issues de cookies que sur la base d'un consentement reçu de la manière spécifique dictée par l'APD belge sur la base de l'analyse subjective de cette dernière, qui interprète la loi sur la vie privée (WVP). Dans le cadre du RGPD, il existe de nouvelles règles relatives à l'acceptation du consentement comme base légale. S'il était possible pour le hof de confirmer les mesures postérieures au 25 mai 2018, il réglementerait de facto un comportement du passé de Facebook Ireland, qui fait l'objet d'une loi abrogée, et cela au moyen d'une injonction orientée vers l'avenir qui négligerait la législation actuelle, tant en ce qui concerne les règles de droit matériel que celles relatives à la compétence. Par exemple, il ne serait ainsi pas possible pour le service Facebook de respecter aucune des exigences de la nouvelle législation (le RGPD et le futur règlement relatif à la vie privée et aux communications électroniques) qui dérogent aux dispositions des mesures imposées.*

42 [omissis]

b) Cela s'opposerait en outre aux enquêtes actuellement en cours auprès du Data Protection Commissioner (commissaire à la protection des données) irlandais à la suite des plaintes RGPD [mentionnées ci-dessus]. *La Commission vie privée (désormais l'APD) ne saurait se voir autorisée à contourner de cette manière le RGPD (et la future réglementation relative à la vie privée, telle que le règlement relatif à la vie privée et aux communications électroniques à venir) en poursuivant des procédures parallèles et indépendantes concernant l'application des législations nationales de protection des données.*

c) En outre, si le hof devait poursuivre la présente procédure, plusieurs critères pour l'acceptation du "consentement" existeraient en parallèle dans un seul et unique cadre juridique : un pour le service Facebook et un autre pour tous les autres services de la société de l'information disponibles sur l'Internet. Le hof n'est pas en mesure de conseiller les règles (y compris les règles de politique) que les autorités de contrôle devraient appliquer dans le cadre de leur contrôle administratif concernant le service Facebook.

d) Les juridictions belges ne peuvent pas non plus allonger la durée de validité des mesures imposées dès lors que les nouvelles règles tant de droit matériel que de compétence prévues dans le RGPD doivent être respectées, en raison de l'interdépendance entre la WEC et le RGPD (comme les intimées l'ont à plusieurs reprises reconnu), et de la réforme prévue de la directive vie privée et communications électroniques 2002/58/CE par le futur règlement vie privée et communications électroniques (qui deviendra la lex specialis pour l'application des règles de protection des données sur les cookies et technologies similaires) ».

4.4.

Pour les faits qui se sont produits à partir de l'entrée en vigueur de la loi APD, à savoir le 25 mai 2018, une tout autre procédure s'applique.

Les plaintes peuvent donner lieu à une enquête des services d'inspection de l'APD.

Lorsque l'enquête est terminée, l'affaire peut être portée devant la chambre contentieuse.

Celle-ci peut, le cas échéant (à côté de nombreuses autres mesures qui sont énumérées à l'article 100), décider de « *transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier* » (point 15**) [Or. 105]**.

Les décisions de la chambre contentieuse peuvent faire l'objet d'un recours devant la Cour des marchés (voir article 108 [43]).

La procédure qui consiste à agir contre une partie – comme, en l'espèce, la procédure qui a été introduite par la Commission vie privée – n'est en principe plus possible.

Par contre, dans le cadre européen du suivi et de la lutte contre les infractions à la réglementation relative à la vie privée sensu lato (le RGPD), une nouvelle règle s'applique (le « guichet unique »).

Au vu de ces deux éléments – pour les faits « postérieurs » au 25 mai 2018 – la question se pose de savoir si l'APD peut encore agir contre Facebook Belgium bvba. En effet, d'une part, Facebook Ireland Limited est l'entité qui effectue le traitement des données ; d'autre part, puisque depuis cette date et en vertu du principe du « guichet unique », une action ne peut être introduite qu'en Irlande, par les autorités qui y sont habilitées – à tout le moins aux termes de l'article 56 du RGPD – seules les juridictions de cet État sont compétentes (ce qui devrait avoir pour conséquence que l'autorité nationale chargée de la protection des données ne devrait plus disposer de la qualité ni de l'intérêt pour agir dans d'autres États membres où l'activité de traitement des données n'est pas effectuée).

4.5.

À l'appui du bien-fondé de ses demandes contre Facebook Belgium bvba (lire : la question de savoir si elle dispose de la qualité et de l'intérêt pour agir devant les juridictions belges contre l'entité belge Facebook Belgium bvba), l'APD fait valoir que, dans l'arrêt du 5 juin 2018 [44], la Cour a jugé que l'autorité nationale de protection des données (en Allemagne) était compétente pour agir contre Facebook Germany.

4.6. **[Or. 106]**

Dans cet arrêt, la Cour a répondu comme suit aux questions préjudicielles qui lui étaient soumises :

[43] Article 108 : « *§ 1er La chambre contentieuse informe les parties de sa décision et de la possibilité de recours dans un délai de trente jours, à compter de la notification à la Cour des marchés. Sauf les exceptions prévues par la loi ou sauf si la chambre contentieuse en décide autrement par décision spécialement motivée, la décision est exécutoire par provision, nonobstant recours. La décision d'effacement des données conformément à l'article 100, § 1er, 10°, n'est pas exécutoire par provision. § 2 Un recours peut être introduit contre les décisions de la chambre contentieuse en vertu des articles 71 et 90 devant la Cour des marchés qui traite l'affaire selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire.* »

[44] Arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388).

« *1. L'article 2, sous d), de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doit être interprété en ce sens que la notion de "responsable du traitement", au sens de cette disposition, englobe l'administrateur d'une page fan hébergée sur un réseau social.*

2. Les articles 4 et 28 de la directive 95/46 doivent être interprétés en ce sens que, lorsqu'une entreprise établie en dehors de l'Union européenne dispose de plusieurs établissements dans différents États membres, l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre, alors même que, en vertu de la répartition des missions au sein du groupe, d'une part, cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire dudit État membre et, d'autre part, la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union européenne, à un établissement situé dans un autre État membre.

3. L'article 4, paragraphe 1, sous a), et l'article 28, paragraphes 3 et 6, de la directive 95/46 doivent être interprétés en ce sens que, lorsque l'autorité de contrôle d'un État membre entend exercer à l'égard d'un organisme établi sur le territoire de cet État membre les pouvoirs d'intervention visés à l'article 28, paragraphe 3, de cette directive en raison d'atteintes aux règles relatives à la protection des données à caractère personnel, commises par un tiers responsable du traitement de ces données et ayant son siège dans un autre État membre, cette autorité de contrôle est compétente pour apprécier, de manière autonome par rapport à l'autorité de contrôle de ce dernier État membre, la légalité d'un tel traitement de données et peut exercer ses pouvoirs d'intervention à l'égard de l'organisme établi sur son territoire sans préalablement appeler l'autorité de contrôle de l'autre État membre à intervenir. »

La directive 95/46 a été abrogée par l'article 94, paragraphe 1, du RGPD avec effet au 25 mai 2018.

La directive sur laquelle portait la demande de décision préjudicielle soumise à la Cour ayant été abrogée, il y a lieu de s'interroger sur la pertinence de la réponse donnée par la Cour pour ce qui concerne la réglementation actuelle.

4.7.

Facebook Belgium bvba fait valoir ce qui suit concernant cet arrêt : **[Or. 107]**

« [omissis] *Tout d'abord, les intimées se basent sur l'arrêt de la Cour de justice dans l'affaire Fan Pages pour affirmer que les appelantes, Facebook*

Inc. ou Facebook Ireland, sont responsables du traitement des données de cookies conjointement avec les sites Web tiers. Toutefois, dans leurs conclusions, les intimées ne tiennent pas compte des conséquences qu'aurait la reconnaissance d'une telle responsabilité conjointe. En effet, aux termes des constatations de la Cour de justice concernant Facebook Ireland (le fournisseur du service Facebook) et Wirtschaftsakademie (un fournisseur de services d'éducation au moyen d'une page fan hébergée sur le site du réseau social Facebook), "l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce".

[OMISSIS] *La Cour de justice précise, en substance, que le rôle de chaque responsable du traitement des données pour ce qui concerne la conformité des pratiques avec la législation en matière de protection de la vie privée doit être déterminé suivant le caractère approprié de l'entité la mieux placée à cette fin. Dans la présente affaire, Facebook Ireland n'était pas techniquement en mesure d'interpréter des informations ou d'obtenir le consentement pour placer le cookie fr (ou tout autre cookie) sur des sites qui sont administrés par des tiers. Le service Facebook ne pouvait tout simplement pas prendre le contrôle d'un site tiers et y afficher des informations ou obtenir un consentement (par exemple en affichant un bandeau cookies) pour placer des cookies au moyen de pixels. Cela était vrai tant du service Facebook que de tout autre réseau publicitaire dans le monde. En conséquence, les faits démontrent qu'il s'agit ici d'une chose qui revient au propriétaire du site tiers et pour laquelle il est tenu d'obtenir un consentement valable.*

[OMISSIS] *De plus, il apparaît en fait que certains sites tiers qui contiennent aussi des pixels et des modules sociaux du service Facebook mettent effectivement en place et appliquent des mécanismes pour informer les utilisateurs pour éviter que des données de cookies soient placées ou obtenues avant que les utilisateurs y aient consenti.*

[OMISSIS] *Enfin, il ressort clairement de la jurisprudence de la Cour de justice qu'un responsable du traitement peut invoquer un consentement obtenu par un tiers pour traiter lui aussi (légalement) des données personnelles : "*[D]*ès lors qu'un abonné a été informé* […] *de la possibilité de la transmission des données à caractère personnel le concernant à une entreprise tierce* […] *en vue* [d'une finalité], *et que celui-ci* [y] *a consenti* […], *la transmission de ces mêmes données à une autre entreprise* […] *ne doit pas faire de nouveau l'objet d'un consentement par l'abonné* […]". »

4.8.

Aux termes de l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C210/16, EU:C:2018:388, point 43) :

> « *Cela étant, il y a lieu de préciser, ainsi que l'a relevé M. l'avocat général aux points 75 et 76 de ses conclusions, que l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de* **[Or. 108]** *responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce* ».

4.9.

Il ressort des éléments disponibles que la position de Facebook Belgium bvba peut se résumer comme suit :

> « [omissis] *Contrairement à Facebook Ireland, Facebook Belgium n'a aucun rapport avec le traitement des données litigieuses. Au contraire, Facebook Belgium est une entité qui a été créée principalement pour se concentrer sur les relations avec les institutions de l'Union européenne et, accessoirement, pour soutenir les activités publicitaires de Facebook Ireland qui se déroulent en Belgique. Ces activités n'ont cependant pas le moindre rapport avec le traitement des données qui font l'objet de la présente instance et elles ne sont pas exercées dans le cadre des activités de Facebook Ireland.*
>
> [OMISSIS] *Facebook Belgium n'est en effet pas responsable de la prestation du service Facebook aux habitants de la Belgique ou d'un autre État ; elle ne collecte absolument aucune donnée (de connexion) relative aux utilisateurs (par exemple des données de cookies) ; elle ne joue aucun rôle dans le placement de cookies ou dans le traitement des données provenant des navigateurs des titulaires de comptes, des utilisateurs enregistrés ou des non-utilisateurs au moyen des cookies lu-, xs-, c_user-, fr-, sb-, datr- ou de quelque autre cookie, pixel ou module social. Les salariés de Facebook Belgium ne se voient pas confier d'informations sur le fonctionnement technique des pixels, des modules sociaux ou des cookies et ils ne jouent aucun rôle en rapport avec la prestation du service Facebook ou avec les données litigieuses.*
>
> *c) Conclusion*
>
> [OMISSIS] *Facebook Belgium n'est pas un établissement important de Facebook Ireland ; c'est dans le cadre des activités de cette dernière qu'ont lieu les activités pertinentes de traitement de données. En conséquence, seul*

le droit irlandais s'applique à ces opérations de traitement de données, qui sont exercées et contrôlées en Irlande. »

4.10.

Facebook Belgique bvba ajoute encore ce qui suit :

« [omissis] *Comme nous l'avons indiqué ci-dessus, le RGPD a été adopté le 27 avril 2016 et est pleinement applicable depuis le 25 mai 2018. Le RGPD abroge la directive 95/46, étant donné qu'il vise à remplacer l'ancien cadre de la législation de l'Union et de la législation nationale en matière de protection des données par un règlement unique et plus ample. Comme tous les règlements de l'Union, le RGPD est d'application directe dans les États membres et il prévaut sur les législations nationales qui sont contraires à ses dispositions. La législation de l'Union est contraignante pour toutes les entités et tous les organes de l'administration qui l'interprètent et l'appliquent, y compris les juridictions.*

[OMISSIS] *Ainsi que nous l'indiquons au cinquième moyen (section 3.5 ci-dessous), aux termes de l'article 56 du RGPD, "l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par* **[Or. 109]** *ce responsable du traitement ou ce sous-traitant". De plus, "*[l]*'autorité de contrôle chef de file est le seul interlocuteur du responsable du traitement ou du sous-traitant pour le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant". Les dispositions du RGPD ne se prêtent pas à l'interprétation : les autorités de l'État membre de l'établissement principal du responsable du traitement sont le seul interlocuteur du responsable du traitement pour ce qui concerne le RGPD. Dans le cas du service Facebook, Facebook Ireland est l'établissement principal et le "seul interlocuteur" (à l'exclusion de tous les autres) est le Data Protection Commissioner (commissaire à la protection des données) irlandais. De plus, le RGPD prévoit les mécanismes de coopération et de cohérence que doivent respecter l'autorité de contrôle chef de file et les autres autorités de contrôle concernées (articles 60 et suiv.).*

[OMISSIS] *Il découle de ce qui précède que, même si l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C210/16, EU:C:2018:388) devait être interprété dans le sens indiqué par les intimées, l'enseignement de cet arrêt pour ce qui concerne l'article 4, paragraphe 1, sous c), de la directive 95/46 est désormais dépourvu de pertinence et le dispositif a perdu sa pertinence à la lumière du nouveau cadre prévu par le RGPD (voir quatrième et cinquième moyens, sections 3.4 et 3.5 ci-dessus).* »

4.11.

La juridiction de céans constate que l'APD ne démontre pas [45] que Facebook Belgium bvba pourrait avoir le moindre rapport avec le traitement effectif des données.

Cependant, il y a lieu de s'interroger sur la pertinence du renvoi à l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C210/16, EU:C:2018:388) (voir ci-dessus), même si, en l'espèce, l'existence d'une interaction entre Facebook Ireland et Facebook Belgium bvba pour ce qui concerne le traitement des données n'est pas démontrée.

En outre, la juridiction de céans constate que l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C210/16, EU:C:2018:388) concernait la directive 95/46, entre temps abrogée, mais que, d'autre part, dans l'intervalle, le Bundeskartellamt (autorité fédérale de la concurrence, Allemagne) a adopté, le 6 février 2019, la décision dite « Facebook », dans laquelle cette autorité estime que Facebook abuse de sa position dominante en concentrant des données provenant de différentes sources, ce qui, dorénavant, ne devrait plus pouvoir se faire qu'avec le consentement exprès des utilisateurs (il s'agit de rassembler des données provenant aussi bien de Facebook que d'autres sites, par le biais des applications Whatsapp et Instagram), étant entendu que l'utilisateur qui n'y consent pas ne peut pas être exclu des services de Facebook.

La juridiction de céans n'a, certes, pas à se prononcer sur ces développements dans d'autres États membres, et les décisions adoptées dans d'autres États membres n'ont aucune incidence sur la compétence des juridictions belges. La juridiction de céans se demande seulement si la position de la Cour dans l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C210/16, EU:C:2018:388), comparée avec celle du Bundeskartellamt (autorité fédérale de la concurrence, Allemagne) (qui estime, malgré le principe du « guichet unique », disposer d'une compétence à **[Or. 110]** l'égard de Facebook Germany) ne doivent pas être soumises à la Cour de justice au moyen d'une demande de décision préjudicielle.

5. Les questions préjudicielles à poser à la Cour de justice

5.1.

Par voie de conclusions, les parties suggèrent à la juridiction de céans de poser, le cas échéant, les questions préjudicielles suivantes à la Cour de justice :

Pour ce qui concerne les entités Facebook :

[45] À l'égard de Facebook Belgium bvba, l'APD s'appuie seulement sur le fait que, dans l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), la Cour a jugé que l'action « pouvait » « aussi » être exercée contre un établissement national.

« *1) À la lumière des mécanismes de cohérence et de coopération qui sont prévus, entre autres, aux articles 56 et 60 du RGPD, l'article 58, paragraphe 5 du RGPD permet-il à l'autorité de contrôle d'un État membre autre que celui dans lequel le responsable du traitement a son établissement principal d'ester en justice concernant des activités transfrontalières de traitement de données dans son propre État membre contre ce responsable du traitement, au lieu de mettre en œuvre la procédure prévue à l'article 60 du RGPD ?*

2) En cas de réponse affirmative à la question précédente, l'article 58, paragraphe 5, du RGPD est-il d'effet direct, de sorte qu'une autorité de contrôle nationale peut s'appuyer sur cette disposition pour intenter ou reprendre une instance contre des particuliers, même si l'article 58, paragraphe 5 du RGPD n'est pas transposé spécifiquement dans la législation des États membres, malgré l'obligation de le faire ?

3) En cas de réponse affirmative aux questions précédentes, l'issue de telles procédures pourrait-elle faire obstacle à une constatation en sens contraire de l'autorité de contrôle chef de file dans le cas où celle-ci enquête sur les mêmes activités de traitement transfrontalières ou sur des activités similaires conformément au mécanisme prévu aux articles 56 et 60 du RGPD ? »

5.2.

Pour ce qui concerne l'APD :

« *1) L'article 55, paragraphe 1, les articles 56 à 58 et les articles 60 à 66 du RGPD, lus en combinaison avec les articles 7, 8 et 47 de la Charte, doivent-ils être interprétés en ce sens qu'une autorité de contrôle qui, en vertu d'une législation nationale adoptée en exécution de l'article 58, paragraphe 5, de ce règlement, est compétente pour ester en justice devant une juridiction de son État membre contre des infractions à ce règlement, ne peut pas exercer cette compétence pour ce qui concerne un traitement de données transfrontalier si elle n'est pas l'autorité de contrôle chef de file pour ce qui concerne ce traitement de données transfrontalier ?*

2) La réponse à la question qui précède est-elle différente si le responsable de ce traitement transfrontalier n'a pas son établissement principal cet État membre mais y a un autre établissement ?

3) La réponse à cette question est-elle différente si l'autorité de contrôle nationale dirige son action contre l'établissement principal du responsable du traitement plutôt que contre l'établissement qui se trouve dans son propre État membre ? **[Or. 111]**

4) La réponse à cette question est-elle différente si l'autorité de contrôle nationale a déjà intenté l'action en justice avant la date à laquelle ce règlement est entré en vigueur (le 25 mai 2018 ? »

5.3.

Pour ce qui concerne l'application de l'article 58, paragraphe 5, du RGPD, Facebook Belgium bvba fait valoir ce qui suit :

« *L'accès aux juridictions est subordonné à l'adoption préalable par la Belgique d'une loi qui conférerait à l'APD la qualité pour ester en justice – cette compétence n'est pas prévue par la loi belge.*

[OMISSIS] *En tout état de cause, et même si les arguments des intimées étaient fondés quant au fait que les autorités de contrôle devraient pouvoir librement intenter une instance en justice qui relèverait de la directive 95/46, ce qui n'est pas le cas, ce raisonnement ne mène pas à la conclusion que l'APD peut reprendre cette instance (ou pourrait ester en justice contre les appelantes) en Belgique.*

[OMISSIS] *Qu'il s'agisse du RGPD ou de l'ancienne directive 95/46, la voie de recours autonome prévue en Belgique par l'article 32, paragraphe 3, de la WVP n'existe plus, puisque cette disposition a été abrogée. En outre,* [la procédure prévue par] *cette disposition n'a pas été remplacée par une procédure comparable ou analogue lors de la dernière refonte de la législation belge en matière de protection de la vie privée. La législation belge actuelle en matière de protection de la vie privée prévoit seulement une procédure administrative à l'article 95 de la loi APD, qui dispose que l'APD belge peut ouvrir la procédure, communiquer des griefs et infliger une amende à un responsable du traitement ou à un sous-traitant lorsque l'autorité est compétente pour agir. Comme nous l'avons exposé ci-dessus, l'APD belge n'est en tout état de cause pas compétente pour agir à l'égard d'un quelconque responsable du traitement de données du service Facebook, qui relève exclusivement du Data Protection Commissioner (commissaire à la protection des données) irlandais.*

[OMISSIS] *Comme nous l'avons indiqué ci-dessus, l'article 58, paragraphe 5, du RGPD impose explicitement aux États membres de veiller à ce que les autorités de contrôle soient en mesure d'ester en justice avec la qualité nécessaire ("*[c]*haque État membre prévoit, par la loi" et "le cas échéant"). Il apparaît du libellé de cette disposition que celle-ci n'a pas d'effet direct à l'égard des particuliers, puisqu'elle n'est pas suffisamment complète, claire, inconditionnelle et précise. L'article 58, paragraphe 5, du RGPD indique que "*[l']*État membre prévoit, par la loi" la compétence de saisir le juge d'une procédure d'infraction et que, comme nous l'avons indiqué, cette procédure peut varier suivant les traditions juridiques des États membres. Les États membres doivent apprécier, à cet égard, s'il*

convient de conférer à leurs autorités de contrôle la qualité pour ester en justice. Il serait contraire au principe de légalité que les autorités de contrôle des États membres puissent simplement invoquer l'article 58, paragraphe 5, du RGPD pour ester en justice devant le juge compétent contre des particuliers, qui seraient ainsi privés de protection contre les interventions discrétionnaires des États membres. La législation et la jurisprudence de l'Union interdisent aux États membres d'invoquer une législation de l'Union qui n'a pas été transposée au niveau national (alors qu'elle devrait l'être) pour agir contre des particuliers.

[OMISSIS] [Le Hof van beroep te Brussel (cour d'appel de Bruxelles)] *l'a confirmé dans les termes suivants, qui se réfèrent à la transposition et à la mise en œuvre de la directive 95/46, mais qui s'appliquent aussi pleinement à l'article 58, paragraphe 5, du RGPD :* **[Or. 112]**

> *"une règle de droit international ou supranational a un effet direct si elle peut être appliquée dans l'ordre juridique dans lequel elle est en vigueur sans aucune mesure d'exécution interne substantielle".*

[OMISSIS] *Étant donné que la Belgique a abrogé une disposition et n'en a adopté aucune autre qui permettrait à l'APD d'intenter une procédure contre des particuliers, l'APD n'a pas la qualité pour reprendre cette procédure (ni pour intenter aucune procédure). Telle était la volonté du législateur belge lorsqu'il a adopté la refonte de la législation belge en matière de protection des données.*

(v) Conclusion

[OMISSIS] P*our les motifs exposés ci-dessus, plaise au* [Hof van beroep te Brussel (cour d'appel de Bruxelles)] *déclarer la demande irrecevable en ce qu'elle est basée sur des faits qui se sont produits après le 25 mai 2018, ou à tout le moins décliner sa compétence et déclarer les demandes des intimées en matière de protection de la vie privée irrecevables, ou à tout le moins inadmissibles, et dans tous les cas non fondées.* »

5.4.

L'APD réplique ce qui suit :

« [OMISSIS] *Le processus d'élaboration du RGPD montre qu'il incombe au législateur national de faciliter les voies de recours judiciaires comme solution de rechange à l'action administrative d'une autorité de contrôle. Le législateur belge a exécuté l'obligation qui lui est imposée par l'article 58, paragraphe 5, du RGPD : la possibilité pour l'APD de porter des infractions à l'attention des autorités judiciaires et d'ester en justice est prévue à l'article 6 de la loi APD :*

> *"L'autorité de protection des données a le pouvoir de porter toute infraction aux principes fondamentaux de la protection des données à caractère personnel, dans le cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel, à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice en vue de voir appliquer ces principes fondamentaux."*

Rien dans cette disposition n'indique que l'APD ne pourrait ester en justice que dans le cas où elle serait la seule autorité compétente ou l'autorité de contrôle chef de file. Ainsi que nous l'avons déjà indiqué plus haut, le RGPD n'impose pas non plus une telle interprétation de l'article 6 de la loi APD. Le seul principe qui résulte clairement et incontestablement de l'article 6 de la loi APD est que l'APD peut porter des infractions aux principes fondamentaux de la protection des données personnelles à la connaissance des autorités judiciaires et ester en justice à ce sujet sur le territoire belge. Peu importe à cet égard que ces principes fondamentaux soient prévus par le RGPD ou par d'autres lois qui touchent à la matière de la protection des données personnelles, telles que l'article 129 du WEC. On ne comprend pas que Facebook soutienne que l'article 58, paragraphe 5, du RGPD n'aurait pas été mis en œuvre en droit belge. Le législateur belge n'aurait pas pu mettre cette disposition en œuvre de manière plus littérale qu'il l'a fait à l'article 6 de la loi APD. Il s'agit en effet d'une réitération presque mot pour mot de l'article 58, paragraphe 5, du RGPD. Il ne saurait être sérieusement mis en doute que l'APD peut saisir le [Hof van beroep te Brussel (cour d'appel de Bruxelles)] *de la présente procédure aussi bien pour des faits antérieurs au 25 mai 2018 que pour des faits postérieurs à cette date.*

[OMISSIS] *Le libellé de l'article 6 de la loi APD illustre en outre à quel point Facebook fait fausse route dans l'interprétation qu'elle tente de donner des termes "le cas échéant" qui figurent à l'article 58, paragraphe 5, du RGPD. Elle soutient à cet égard que le caractère "approprié" * ou non de l'exercice d'une action en justice par l'Autorité de protection des données dépendrait de la présence d'une autorité de contrôle chef de file. Or, cela n'est naturellement pas ce que ces mots signifient.* **[Or. 113]**

Si cette interprétation était correcte (ce qui n'est certainement pas le cas), la version initiale de l'article 58, paragraphe 5, établie par la Commission européenne aurait alors dû être maintenue et tout ce qui concerne l'exercice d'actions en justice par les autorités de contrôle aurait été prévu directement par le RGPD. Cependant, le choix a finalement été de s'en

* Ndt : les termes néerlandais du règlement correspondant au français « le cas échéant » sont « *waar passend* », c'est-à-dire, littéralement « là où [cela est] approprié » (« *passend* » pris isolément signifie approprié, adéquat).

remettre aux États membres pour qu'ils prévoient dans leur législation nationale la faculté pour l'autorité de contrôle d'ester en justice ou non. Il s'agit donc ici d'une faculté que l'APD tire directement du droit belge. Les références aux autorités de contrôle chefs de file et au mécanisme de cohérence prévu par le RGPD ne sont pas pertinentes en l'espèce. Pour le dire avec les mots du législateur lui-même :

> *"L'article 6 donne à l'Autorité de protection des données un accès général au juge, y compris le juge européen"*[*].

Les termes "le cas échéant" indiquent seulement que l'APD peut apprécier de manière discrétionnaire quelles affaires elle souhaite traiter elle-même et quelles affaires elle préfère soumettre au pouvoir judiciaire. L'article 6 de la loi APD succède à l'article 32 de la WVP et reconnaît donc à l'APD une marge d'appréciation similaire pour décider quelles affaires elle entend soumettre au pouvoir judiciaire, ainsi que le législateur l'a expressément précisé :

> *"Comme le prévoit l'article 58 § 8 du RGPD, l'Autorité de protection des données conserve la possibilité de renvoyer n'importe quelle affaire devant l'ordre judiciaire"*[**].

On ne comprend pas non plus sur quelle base Facebook affirme que l'article 32 de la WVP n'aurait pas été remplacé depuis l'entrée en vigueur du RGPD, étant donné que les travaux préparatoires indiquent expressément qu'il s'agit de maintenir la compétence. Les choses deviennent cependant totalement absurdes lorsque Facebook affirme que l'APD ne peut pas ester en justice contre elle depuis le 25 mai 2018 parce qu'il y aurait une autorité de contrôle chef de file en Irlande, alors que l'APD se voit précisément conférer cette faculté expressément pour "n'importe quelle affaire". Comprenne qui pourra… »

5.5.

Il semble à la juridiction de céans que le renvoi à l'article 6 de la loi APD est insuffisant. Certes, l'APD est compétente pour porter des infractions aux principes fondamentaux de la protection des données à l'attention des autorités judiciaires et, le cas échéant, ester en justice en vue de voir appliquer ces principes fondamentaux, mais cela n'établit pas dans la législation nationale un principe selon lequel l'APD devrait en tout état de cause et dans tous les cas pouvoir ester devant les juridictions belges, alors que la règle générale du « guichet unique » prévoit seulement une action devant le juge du lieu où a lieu le traitement des données.

[*] Ndt : exposé des motifs, Doc. Parl. 54 2648/001, p. 15.

[**] Ndt : ibidem, p. 14.

Il y a lieu de distinguer la faculté d'intenter « une » action en justice et celle de « toujours intenter cette action devant les juridictions belges sans limitations ni conditions ».

5.6.

En vertu de l'article 288 TFUE, la juridiction de céans est tenue de veiller à une interprétation conforme au droit de l'Union. **[Or. 114]**

L'obligation d'interprétation conforme ne se limite pas aux cas dans lesquels il existe des divergences entre le droit national et le droit de l'Union. Même lorsqu'elle correspond par son libellé au droit de l'Union, le juge doit interpréter sa législation nationale à la lumière du droit de l'Union. Il doit donc interpréter les notions conformément à leur signification autonome en droit de l'Union. De même, lorsqu'il applique le droit de l'Union, le juge national doit le faire, le cas échéant, conformément à l'interprétation de ces notions donnée par la [Cour de justice]. Ainsi, l'interprétation conforme ne garantit pas seulement l'effectivité du droit de l'Union, mais aussi, dans une large mesure, son application uniforme.

5.7.

Par conséquent, il y a lieu de saisir la Cour de justice des questions préjudicielles suivantes :

[omissis] **[Or. 115]** [omissis] [questions reproduites dans le dispositif]

5.8

Sur la base de l'interprétation avancée par Facebook Belgium bvba, la juridiction de céans serait encline à juger que le « guichet unique » constitue une voie de recours exclusive. Cependant, considérant que, dans l'arrêt du 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), la Cour a jugé : « *lorsqu'une entreprise établie en dehors de l'Union européenne dispose de plusieurs établissements dans différents États membres, l'autorité de contrôle d'un État membre est habilitée à exercer les pouvoirs que lui confère l'article 28, paragraphe 3, de cette directive à l'égard d'un établissement de cette entreprise situé sur le territoire de cet État membre, alors même que, en vertu de la répartition des missions au sein du groupe, d'une part, cet établissement est chargé uniquement de la vente d'espaces publicitaires et d'autres activités de marketing sur le territoire dudit État membre et, d'autre part, la responsabilité exclusive de la collecte et du traitement des données à caractère personnel incombe, pour l'ensemble du territoire de l'Union européenne, à un établissement situé dans un autre État membre* », la juridiction de céans se demande si cette interprétation est encore valable à l'égard du RGPD actuellement en vigueur (et, en droit interne, la loi APD).

5.9.

L'article 58, paragraphe 5, du RGPD dispose expressément :

> « *Chaque État membre prévoit, par la loi, que son autorité de contrôle a le pouvoir de porter toute violation du présent règlement à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement* ».

Selon la juridiction de céans, cette règle exige que les États membres prévoient, par une disposition expresse, les conditions concrètes dans lesquelles leur autorité locale peut ester en justice devant leurs juridictions et cela en passant « au-dessus » des principes du « guichet unique » prévus aux articles 55 et 56 du RGPD.

Il semble donc à la juridiction de céans que chaque autorité de contrôle (autre que l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement) n'est compétente pour traiter une plainte qui lui est soumise ou une violation éventuelle de ce règlement que dans le cas où l'objet de l'affaire n'a de lien qu'avec un établissement sis dans son État membre ou n'a de conséquences effectives pour les intéressés que dans son État membre. **[Or. 116]**

6. L'intérêt et la qualité de l'APD pour agir sur la base de la WEC

6.1.

Les entités Facebook font valoir ce qui suit :

> « 49. *Sixième moyen : en outre, les demandes sont en soi irrecevables sur la base de l'article 129 WEC, et le président de la [Commission vie privée, à laquelle est venue aux droits la] seconde intimée ne dispose en tout cas d'aucune compétence pour, sur la base de l'article 32, paragraphe 3, WVP (entre-temps abrogé et remplacé, et qui se limitait à l'application de la WVP), introduire une action fondée sur la WEC. Le rechtbank van eerste aanleg (tribunal de première instance) n'a pas suivi, à tort, ce moyen de défense des appelantes et il a jugé que le législateur n'avait pas pu avoir l'intention d'accorder des compétences à la Commission vie privée de manière restrictive et que les compétences qui avaient été conférées à un autre régulateur, à savoir l'Institut belge des services postaux et des télécommunications (ci-après l'"IBPT"), ne faisaient pas obstacle à celles de la Commission vie privée. En tout état de cause, l'entrée en vigueur du RGPD le 25 mai 2018 rend irrecevable ou inadmissible et/ou non fondée, à compter de cette date, toute poursuite de la présente action.* »

6.2.

L'article 129 de la WEC dispose :

« *Le stockage d'informations ou l'obtention de l'accès à des informations déjà stockées dans les équipements terminaux d'un abonné ou d'un utilisateur est autorisée uniquement à condition que :*

1° l'abonné ou l'utilisateur concerné reçoive conformément aux conditions fixées dans la loi du 8 décembre 1992 relative à la protection de la vie privée et à l'égard des traitements de données à caractère personnel, des informations claires et précises concernant les objectifs du traitement et ses droits sur la base de la loi du 8 décembre 1992 ;

2° l'abonné ou l'utilisateur final ait donné son consentement après avoir été informé conformément aux dispositions visées au point 1°

L'alinéa 1er n'est pas d'application pour l'enregistrement technique des informations ou de l'accès aux informations stockées dans les équipements terminaux d'un abonné ou d'un utilisateur final ayant pour seul but de réaliser l'envoi d'une communication via un réseau de communications électroniques ou de fournir un service demandé expressément par l'abonné ou l'utilisateur final lorsque c'est strictement nécessaire à cet effet.

Le consentement au sens de l'alinéa 1er ou l'application de l'alinéa 2, n'exempte pas le responsable du traitement des obligations de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui ne sont pas imposées par le présent article.

Le responsable du traitement donne gratuitement la possibilité aux abonnés ou utilisateurs finals de retirer le consentement de manière simple. » **[Or. 117]**

Pour ce qui concerne le renvoi à la WVP qui est encore opéré par la WEC, ce renvoi ne peut en tout cas pas porter sur l'article 32, paragraphe 3, de la WVP, puisque cette disposition a été irrévocablement abrogée (voir supra).

Le libellé de l'article 129 de la WEC ne peut donc pas constituer une base valable pour le ou les prédécesseurs de l'APD, ni pour l'APD elle-même, pour reprendre ou pour introduire une demande.

6.3.

La position de l'APD est la suivante :

« *Huitième moyen : il convient de rejeter car dénuée de fondement l'allégation de Facebook selon laquelle l'action serait irrecevable parce qu'elle est basée sur l'article 129 WEC.*

Premièrement, l'article 32, paragraphe 3, WVP constitue effectivement une base permettant à la Commission vie privée d'engager une action en raison de la violation de l'article 129 WEC. En effet, l'article 129 WEC "spécifie et complète" la WVP, car l'article 129 WEC est la transposition de l'article 5, paragraphe 3, de la directive 2002/58 et l'article 1er, paragraphe 2, de la directive 2002/58 dispose que "[l]es dispositions de la présente directive précisent et complètent la directive 95/46/CE". En outre, la WVP était incorporée dans l'article 129 WEC, car tant les "informations" visées par l'article 129, premier alinéa, 1°, WEC que le "consentement" visé à l'article 129, premier alinéa, 2°, WEC, sont ceux définis dans la WVP, et l'article 129 WEC dispose que le responsable, outre les obligations relatives aux informations et au consentement, est tenu de respecter toutes les autres obligations imposées par la WVP. Par conséquent, en cas de traitement de données personnelles, par exemple par la collecte de cookies, l'article 129 WEC implique que les règles de la WVP sont également appliquées. Il s'ensuit nécessairement que la Commission vie privée était également compétente pour le contrôle de celui-ci. Par conséquent, il convient de rejeter car dénuée de fondement la demande de Facebook visant à déclarer l'action irrecevable au motif qu'elle est basée sur l'article 129 WEC.

Deuxièmement, l'allégation de Facebook selon laquelle seul l'IBPT et non la Commission vie privée pourrait engager une action en raison de la violation de l'article 129 WEC est incorrecte. L'article 129 WEC, qui transpose l'article 5, paragraphe 3, de la directive 2002/58 en droit belge, porte également sur les "services de la société de l'information", comme les réseaux sociaux en ligne (par exemple, celui de Facebook) car, parmi les exceptions à l'exigence de consentement, l'article 5, paragraphe 3, de la directive 2002/58 prévoit la situation dans laquelle un cookie est strictement nécessaire pour la fourniture d'un "service de la société de l'information demandé par l'abonné". Si cet article 5, paragraphe 3, n'était pas applicable à des services de la société de l'information, il ne serait pas nécessaire de prévoir une exception pour certains de ces services. Étant donné que le champ d'application de la WEC est limité, conformément à l'article 1er, paragraphe 1, à l'article 2, sous c, de la directive-cadre 2002/21 et à l'article 2, 5° WEC, aux "service de communications électroniques", et que les "services de la société de l'information" sont exclus de la notion de "services de communications électroniques", l'IBPT n'est compétent qu'en ce qui concerne les "services de communications électroniques" et non pour les "services de la société de l'information". Par conséquent, il n'est pas non plus compétent en ce qui concerne le traitement de données personnelles lors de l'utilisation de cookies dans le cadre de services de la société de l'information ; concernant ces derniers, la Commission vie privé est exclusivement compétente.

Troisièmement, même à supposer que l'IBPT était compétente pour le traitement de données personnelles lors de l'utilisation de cookies dans le

cadre de services de la société de l'information (quod non), la Commission vie privée restait en tout état de cause compétente, ne serait-ce que concurremment. Dans tous les cas où la WEC régit, par des dispositions spécifiques, le traitement de données personnelles dans le secteur des communications électroniques, non **[Or. 118]** *seulement l'organisme de surveillance sectoriel IBPT est compétent, mais également la Commission vie privée (en qualité d'organisme de surveillance général).* »

6.4.

[Le bien-fondé de] la position de l'APD, selon laquelle la Commission vie privée « concurremment avec l'IBPT », serait (encore) compétente pour agir contre des violations alléguées de l'article 129 de la WEC, dépend lui-même de la question de savoir si l'APD, après le 25 mai 2018, dispose encore d'une voie de recours devant les juridictions belges, puisque les articles 55 et suivants du RGPD semblent en disposer autrement.

La question de savoir si l'APD peut agir sur la base de l'article 129 de la WEC dépend donc de la réponse qui sera donnée aux questions préjudicielles.

VIII. Décision

[omissis] [voir dispositif]

IX. Les dépens

[OMISSIS]

Par ces motifs, [Or. 119]

Le Hof van beroep te Brussel (cour d'appel de Bruxelles, Belgique),

[OMISSIS]

Déclare l'appel de Facebook Ireland Limited et Facebook Inc. recevable et en grande partie fondé ;

Donne acte à l'Autorité de protection des données de sa succession à M. Willem Debeuckelaere agissant en sa qualité de président de la « Commission de la protection de la vie privée » ;

Dit pour droit que la succession de l'Autorité de protection des données [à] l'entité sans personnalité juridique « Commission de la protection de la vie privée » est irrecevable ;

Déclare l'appel incident de l'Autorité de protection des données recevable mais non fondé ;

Réforme le jugement attaqué, sauf dans la mesure où celui-ci déclare irrecevable l'intervention volontaire de la « Commission de la protection de la vie privée » et déclare recevable la demande dirigée contre Facebook Belgium bvba ;

Statuant à nouveau pour le surplus :

- se déclare sans compétence internationale à l'égard de Facebook Ireland Limited et de Facebook Inc. ;

- se déclare compétente pour statuer à l'égard de Facebook Belgium bvba ;

- dit la demande, en ce qu'elle est dirigée contre Facebook Belgium bvba, recevable en principe ;

- avant de statuer au fond sur la qualité et l'intérêt de l'APD pour agir contre Facebook Belgium bvba pour des faits qui se sont produits après le 25 mai 2018, saisit la Cour de justice de l'Union européenne des questions préjudicielles suivantes :

  « 1) *L'article 55, paragraphe 1, les articles 56 à 58 et les articles 60 à 66 du 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 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, lus en combinaison* **[Or. 120]** *avec les articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne, doivent-ils être interprétés en ce sens qu'une autorité de contrôle qui, en vertu d'une législation nationale adoptée en exécution de l'article 58, paragraphe 5, de ce règlement, est compétente pour ester en justice devant une juridiction de son État membre contre des infractions à ce règlement, ne peut pas exercer cette compétence pour ce qui concerne un traitement de données transfrontalier si elle n'est pas l'autorité de contrôle chef de file pour ce qui concerne ce traitement de données transfrontalier ?*

  2) La réponse à la question qui précède est-elle différente si le responsable de ce traitement transfrontalier n'a pas son établissement principal dans cet État membre mais y a un autre établissement ?

  3) La réponse à cette question est-elle différente si l'autorité de contrôle nationale dirige son action en justice contre l'établissement principal du responsable du traitement plutôt que contre l'établissement qui se trouve dans son propre État membre ?

4) La réponse à cette question est-elle différente si l'autorité de contrôle nationale a déjà intenté l'action en justice avant la date à laquelle ce règlement est entré en vigueur (le 25 mai 2018) ? »

5) En cas de réponse affirmative à la question précédente, l'article 58, paragraphe 5, du règlement 2016/679 est-il d'effet direct, de sorte qu'une autorité de contrôle nationale peut s'appuyer sur cette disposition pour intenter ou reprendre une instance contre des particuliers, même si l'article 58, paragraphe 5, du règlement 2016/679 n'est pas transposé spécifiquement dans la législation des États membres, malgré l'obligation de le faire ?

6) En cas de réponse affirmative aux questions précédentes, l'issue de telles procédures pourrait-elle faire obstacle à une constatation en sens contraire de l'autorité de contrôle chef de file dans le cas où celle-ci enquête sur les mêmes activités de traitement transfrontalières ou sur des activités similaires conformément au mécanisme prévu aux articles 56 et 60 du règlement 2016/679 ?

[OMISSIS] **[Or. 121]**

[OMISSIS] Prononcé en audience publique le **8 mai 2019** [OMISSIS]