

COPIE NON SIGNÉE - art 792 C.J.,
Exemption du droit d'expédition art. 280,
2 du code des droits d'enregistrement



Numéro de répertoire 2026/
Date du prononcé 30 JAN. 2026
Numéro de rôle RR/26/0003

expédition

Délivrée à	Délivrée à	Délivrée à
le €	le €	le €

☐

ne pas présenter à
l'inspecteur

Tribunal de l'entreprise francophone de Bruxelles

Ordonnance sur requête
unilatérale

présenté le
ne pas enregistrer

Vu la requête ci-annexée et les pièces jointes, déposées au greffe du tribunal de céans le 28 janvier 2026 par :

1. La s.a. **RTL BELGIUM**, inscrite à la B.C.E. sous le n° 0428.201.847, dont le siège social est à 1030 SCHAERBEEK, Avenue Jacques Georgin, 2 ;

Ci-après dénommée « *RTL* »,

2. L'établissement public **RADIO-TELEVISION BELGE DE LA COMMUNAUTE FRANCAISE**, inscrite à la B.C.E. sous le n° 0223.459.690, dont le siège social est à 1030 SCHAERBEEK, Boulevard Auguste Reyers 52 CIT,

Ci-après dénommé « *RTBF* »,

Dénommées ensemble, « *les requérantes* »,



Vu les dispositions de la loi du 15 juin 1935 sur l'emploi des langues en matière judiciaire ;

Vu les articles XVII.34/1 et suivants du Code de droit économique ;

Vu la requête et les pièces déposées le 28 janvier 2026 ;

1. CONTEXTE FACTUEL

1. Les requérantes se présentent comme les principaux radiodiffuseurs opérant en Fédération Wallonie-Bruxelles.

La première requérante, la RTBF, est une entreprise publique autonome à caractère culturel. Son offre télévisée de programmes s'effectue au travers La Une, Tipik, La Trois et Arte. Elle diffuse également son contenu via sa plateforme de streaming (Auvio), via des applications (App RTBF et App Auvio) et via la télévision interactive disponible dans les offres des fournisseurs d'accès à internet.

La deuxième requérante, RTL, est une société belge qui édite plusieurs chaînes de télévision généralistes commerciales privées relevant de la compétence du Conseil supérieur de l'Audiovisuel. Son offre de contenu s'effectue au travers des chaînes RTL tvi, RTL club, RTL plug et club RTL, ainsi que par internet, via sa plateforme de streaming appelée RTL play.

Les requérantes, en leur qualité de diffuseurs, indiquent bénéficier de droits voisins du droit d'auteur. Elles exposent subir une atteinte manifeste et considérable à leurs droits en raison de la réémission, la reproduction et la communication de leurs émissions via des services IPTV illégaux.

Suivant les requérantes, l'IPTV, acronyme de *Internet Protocol Television*, est un terme générique désignant les services et les applications qui permettent de regarder la télévision en utilisant la technologie internet. L'utilisation de l'IPTV requiert internet pour diffuser son contenu plutôt que les méthodes de transmission traditionnelle comme les ondes hertziennes, le satellite, ou le câble. Il est possible de regarder des chaînes linéaires en direct ou en différé, des replays ou des vidéos à la demande (VOD).

Des plateformes pirates, se revendiquant IPTV, sont apparues et offrent des services visant la diffusion de contenus pour lesquels elles ne possèdent aucun droit.

Par la présente procédure, les requérantes sollicitent le concours de diverses catégories d'intermédiaires afin de mettre fin aux atteintes.

Elles dirigent leurs demandes contre :

- PROXIMUS, sa filiale MOBILE VIKINGS, TELENET, ORANGE et DIGI COMMUNICATIONS BELGIUM sont des fournisseurs d'accès à internet (ci-après « FAI's ») qui, selon les requérantes, couvrent l'écrasante majorité des abonnés en Belgique.

Ces opérateurs – hormis MOBILE VIKINGS – disposent en outre de leur propre infrastructure réseau, ce qui signifie qu'ils contrôlent les infrastructures physiques ainsi que les services associés essentiels à l'accès à internet. Parmi ces services, figurent notamment leurs propres serveurs DNS (Domain Name System), qui sont utilisés par défaut par leurs abonnés et par les opérateurs virtuels (qui ne disposent donc pas d'infrastructures physiques propres) qui s'appuient sur leurs réseaux.

Leur concours à l'application des mesures de restriction d'accès aux contenus illégaux en ligne est dès lors nécessaire ;

- CLOUDFLARE, société de droit américain basée en Californie, offre un service de réseau de diffusion de contenu (CDN), c'est-à-dire un groupe de serveurs répartis géographiquement qui met en cache le contenu à proximité des utilisateurs finaux. Un service CDN permet le transfert rapide des ressources nécessaires au chargement du contenu internet, notamment les images et les vidéos.

Elle offre également un service d'hébergement de sites internet.

- GOOGLE, groupe américain basé en Californie.

GOOGLE LLC a notamment développé son moteur de recherche « Google Search », qui est le moteur de recherche le plus utilisé au monde avec près de 90% des parts de marché mondiale. GOOGLE offre aussi un service d'hébergement de sites internet (« Google Sites » et « Google Cloud Platform »), ainsi que « Google Play », une boutique en ligne dans laquelle les utilisateurs peuvent trouver des applications, films, séries TV et autres divertissements.

2. OBJET DES DEMANDES

2. Les requérantes sollicitent du Président de :

« Dire pour droit que l'action de RTL et RTBF est recevable et fondée et, dès lors :

- constater que les noms de domaine identifiés en Annexe 1 (les Sites Cibles) donnent accès à des sites/offres Internet par lesquels il est porté atteinte aux droits voisins de radiodiffuseur (art. XI.215, §1er, CDE) appartenant aux Requérantes ;
- constater que les services des Intermédiaires sont utilisés ou susceptibles d'être utilisés par les opérateurs des Sites Cibles pour porter atteinte à des droits voisins appartenant aux Requérantes ; et par conséquent :
- ordonner à :
 - ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM et MOBILE VIKINGS en leur qualité de FAIs et partant fournisseurs de service de résolution de noms de domaine de mettre en œuvre, à leurs propres frais, des mesures de nature à empêcher l'accès, depuis le territoire belge aux :
 - CLOUDFLARE en sa qualité de fournisseur de service de réseau de diffusion de contenu (CDN) et/ou hébergeur de mettre en œuvre, à ses propres frais des mesures de nature à empêcher l'accès, depuis le territoire belge aux :
 - GOOGLE en sa qualité d'hébergeur (Google Sites et/ou Google Cloud Platform), de mettre en œuvre, à ses propres frais, des mesures de nature à empêcher l'accès aux :
 - GOOGLE en sa qualité de moteur de recherche (Google Search / Ads), de mettre en œuvre, à ses propres frais, des mesures de déréférencement et de désactivation des annonces associées aux :
 - Sites Cibles ;
 - mais également aux sites de redirection, sites miroir, noms de domaine passerelle ou, conformément aux conditions posées à l'Annexe 2, sites copycats,
 - qui leur seront ultérieurement notifiés par le Service, dans le cadre des mises à jour régulières de mesures de blocage,
 - et pour lesquels les Requérantes s'engagent à ne solliciter le blocage que de sites internet qui satisfont aux critères cumulatifs suivants:
 - i. ils sont, comme les Sites Cibles, structurellement dédiés à la contrefaçon de masse de contenu audiovisuel;
 - ii. ils offrent, notamment, du contenu sur lequel les Requérantes possèdent des droits exclusifs;
 - iii. ils sont accessibles en Belgique;
 - iv. aucune licence d'exploitation n'a été concédée aux opérateurs de ces sites par les Requérantes.
- ordonner à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM, MOBILE VIKINGS, GOOGLE et CLOUDFLARE de mettre en œuvre, à leurs propres frais, dans le cadre de leurs services respectifs, des mesures de nature à débloquent l'accès ou de nature à de nouveau référencer, depuis le territoire belge, tout nom de domaine qui a déjà été notifié aux Intermédiaires en vertu de l'ordonnance à intervenir, mais dont l'objectif unique ou prédominant n'est plus de donner accès à un Site Cible ou de répliquer celui-ci, qui leur seront notifiés ultérieurement par le Service;
- ordonner à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM, MOBILE VIKINGS, GOOGLE et CLOUDFLARE de mettre en œuvre les mesures de blocage et de déblocage précitées selon les modalités, la fréquence et le délai déterminé par le Service étant entendu que la requérante ou, le cas échéant le service s'il dispense la

requérante d'y procéder, procèdera annuellement, selon la même méthodologie que celle appliquée pour solliciter le blocage des sites visés dans la requête, à un screening de tous les sites bloqués et remettra au Service dans le mois dudit screening l'ensemble de ses recherches et tiendra ceux-ci à la disposition de toute partie à la procédure. Dans ce contexte la requérante communiquera au Service les éléments pertinents démontrant qu'un ou plusieurs des sites litigieux visés par les mesures auraient perdu leur caractère illégal. Le cas échéant, le Service enverra aux destinataires des mesures la notification que le ou les sites litigieux devront faire l'objet d'un déblocage ;

- ordonner à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM et à MOBILE VIKINGS de prendre des mesures de redirection, afin que leurs clients qui auront tenté d'accéder à un nom de domaine bloqué, soient redirigés vers une page internet dont le contenu sera déterminé par le Service en collaboration avec les Requérantes ;
- ordonner à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM et à MOBILE VIKINGS, en leur qualité d'intermédiaire au sens de l'article XVII.34 CDE, d'appliquer ces mesures techniques de blocage et de redirection à l'ensemble de leurs clients ayant souscrit à un service d'accès à Internet, et ce indépendamment du type d'abonnement concerné (privé, professionnel, mobile ou fixe) ;
- charger le Service de :
 - déterminer les modalités d'application des mesures ordonnées, en concertation avec les Requérantes et les Intermédiaires, notamment :
 - le calendrier exact de mise en œuvre par les Intermédiaires des mesures ordonnées,
 - le format des notifications dans le cadre des Mises à jour ;
 - le contenu de la page internet que les utilisateurs verront en lieu et place du site pirate auquel ils auront tenté d'accéder.
 - mettre en œuvre et coordonner la Mise à jour des mesures ordonnées et notamment :
 - identifier, avec l'aide des Requérantes pour autant que celle-ci soit nécessaire, les noms de domaine de contournement (redirections, sites miroirs, copycats) ainsi que les noms de domaine / URL passerelle ;
 - Identifier lesquels des Sites Cibles (y compris les redirections, sites miroirs et copycats) font appel aux services d'hébergement et/ou de CDN de Cloudflare ;
 - Identifier lesquels des Sites Cibles (y compris les redirections, sites miroirs et copycats) utilisent les services d'hébergement de Google (Google Sites ou Google Cloud Platform) ;
 - se positionner comme intermédiaire entre les Requérantes et les Intermédiaires, notamment en notifiant les Sites Cibles ainsi que les Mises à jour aux intermédiaires. Lorsque le Service notifie les Mises à jour aux Intermédiaires, sa notification est également adressée aux Requérantes ;
 - s'assurer de la mise en œuvre effective des mesures ordonnées par les Intermédiaires (y compris chaque Mise à jour), d'une part via des confirmations obtenues des Intermédiaires et, d'autre part, via des vérifications pratiques effectuées par le Service lui-même ;
 - surveiller l'impact des actions mises en place, notamment :
 - en récoltant les statistiques de consultation de la page internet que les utilisateurs verront en lieu et place du site pirate auquel ils auront tenté d'accéder, ainsi que l'évolution de celles-ci ;
 - en se concertant avec les Intermédiaires visés sur la manière la plus efficace d'évaluer, en collaboration, l'impact des mesures ;

- *prendre acte du caractère confidentiel de l'Annexe 2 (a et b) et de la marquer comme telle dans l'ordonnance à intervenir si celle-ci devait y être reproduite ;*
- *délaisser à chaque partie la charge de ses dépens ;*
- *déclarer la décision exécutoire sur minute ».*

3. DISCUSSION

3. Les requérantes Nous saisissent d'une requête fondée sur les articles XVII.34/1 et suivants, CDE, insérés dans ce Code sous le titre I/1 de son livre XVII, ce titre étant intitulé « *Mesures provisoires en cas d'atteinte au droit d'auteur, à un droit voisin, au droit d'un producteur de bases de données commise en ligne ou en cas d'exploitation illégale d'un jeu de hasard en ligne* »¹.

a. Compétence et recevabilité de l'action

4. Suivant l'article XVII.34/1, § 1^{er}, CDE, le Président du tribunal de océans est territorialement et matériellement compétent aux fins de mettre fin aux atteintes manifestes et considérables au droit d'auteur, à un droit voisin ou au droit d'un producteur de base de données, commise en ligne.

5. L'action a, en outre, été introduite par le dépôt d'une requête unilatérale, ce qu'autorise expressément l'article XVII.34/1, § 3, CDE. L'absolue nécessité, au sens de l'article 584, al. 4 du Code judiciaire est également présumée et ne doit pas être démontrée (art. XVII.34/1, § 6, CDE).

Les requérantes, en leur qualité de diffuseurs, se prévalent de droits voisins du droit d'auteur. Dès lors qu'elles allèguent que leurs droits seraient méconnus par les services IPTV pirates, elles doivent être considérées comme des « intéressés » au sens de l'article XVII.34/1, § 2, CDE. Elles disposent d'un intérêt à agir pour solliciter les mesures provisoires.

La requête est dès lors recevable.

b. Conditions à l'obtention de mesures provisoires

6. L'objet de l'actuelle demande est l'obtention d'injonctions imposées à divers intermédiaires afin que ceux-ci mettent en œuvre des mesures visant à cesser toute exploitation non autorisée des séquences des émissions sur lesquelles les requérantes sont titulaires de droits voisins, que ce soit par reproduction, mise en ligne ou retransmission.

Ces intermédiaires sont les destinataires des mesures postulées par les requérantes.

7. Aux termes de l'article XVII.34/1, § 6, al. 1^{er}, du CDE, le président fait droit à la requête si :

- 1) le droit de propriété intellectuelle dont la protection est invoquée est, selon toutes apparences, valable ;
- 2) l'atteinte dénoncée semble manifeste et considérable ;
- 3) après avoir fait une pondération des intérêts, droits et libertés en présence, dont l'intérêt général, les faits et, le cas échéant, les pièces sur lesquelles le demandeur se fonde sont de nature à justifier raisonnablement les mesures provisoires demandées.

¹ Pour une vue d'ensemble : E. CORNU, « L'injonction dynamique Une nouvelle procédure judiciaire particulière (droit d'auteur, droits voisins et exploitation illégale des jeux de hasard en ligne) », *J.T.*, 2025, p. 145.

Cet article précise encore que le président « apprécie en particulier l'effet que pourraient avoir les mesures sollicitées sur l'accès du public à des informations ou tout autre contenu ne portant pas atteinte au droit invoqué par le demandeur ».

• **Quant à la validité *prima facie* des droits invoqués par les requérantes**

8. L'article XI.215, § 2, CDE prévoit qu'est présumé être organisme de radiodiffusion, sauf preuve du contraire, quiconque apparaît comme tel sur la prestation, sur une reproduction de la prestation, ou en relation avec une communication au public de celle-ci, du fait de la mention de son nom ou d'un sigle permettant de l'identifier.

Les requérants produisent à cet effet des extraits et des captures d'écran de plusieurs émissions diffusées sur leurs chaînes télévisées (l'émission « *Face au juge* » ou « *L'amour est dans le pré* » sur RTL tv ou le documentaire « *Merckx* » sur la plateforme Auvio). Ces émissions permettent de les identifier clairement, grâce notamment à la mention de leur nom et de leur logo.

Il suit dès lors des développements contenus dans la requête et se déduit des pièces déposées que les requérantes sont présumées revêtir cette qualité d'organisme de radiodiffusion au sens de l'article XI.215, § 2, CDE.

Comme le relèvent les requérantes, en vertu de l'article XI.215, § 1^{er} du CDE, les organismes de radiodiffusion ont seuls le droit d'autoriser :

- la réémission simultanée ou différée de ses émissions ;
- la reproduction de ses émissions par quelque procédé que ce soit ;
- la communication de ses émissions faite dans un endroit accessible au public moyennant un droit d'entrée ;
- la mise à disposition du public de la fixation de ses émissions de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement.

Dès lors que les requérantes sont présumées être des organismes de radiodiffusion des contenus diffusés, celles-ci bénéficient des droits exclusifs y afférents. A bon escient, elles indiquent que leurs droits leur permettent d'interdire toute retransmission non autorisée de leurs émissions, qu'il s'agisse d'une diffusion simultanée ou différée, d'une mise à disposition en ligne ou d'une communication au public dans un lieu accessible moyennant paiement.

9. Les droits invoqués par les requérantes semblent dès lors *prima facie* suffisamment établis.

• **Quant à l'atteinte manifeste et considérable aux droits invoqués par les requérantes**

10. L'article XVII.34/1, § 6, CDE exige qu'il soit démontré que l'atteinte invoquée « semble manifeste et considérable ».

En l'espèce, les requérantes montrent à suffisance que les activités des offres IPTV violent leurs droits voisins en leur qualité d'organismes de radiodiffusion. Elles allèguent à juste titre que les offres IPTV retransmettent, reproduisent et communiquent au public leurs propres émissions, sans avoir obtenu la moindre autorisation préalable.

Pour rappel, l'IPTV – *Internet Protocol Television* – désigne les services et les applications permettant de regarder la télévision au moyen de la technologie internet. La diffusion du contenu est réalisée par

internet plutôt que par des méthodes de transmission traditionnelle comme les ondes hertziennes, le satellite ou le câble. Cette technologie a été adoptée par des acteurs de la télévision et du numérique dans un cadre légal.

Les requérantes soulignent toutefois qu'une quantité grandissante de services qui se revendiquent IPTV sont en réalité des plateformes pirates, qui diffusent en toute illégalité des contenus sur lesquels elles ne possèdent aucun droit. Ces services illégaux proposent à des utilisateurs finaux d'accéder à une large gamme de contenus vidéo et de chaînes de télévision – dont celles des requérantes – de manière quasi illimitée et à des prix attractifs.

Aux termes de leurs écrits, les requérantes exposent concrètement le fonctionnement des services IPTV de la façon suivante :

- Capture du contenu : le contenu des émissions est capturé depuis une source de diffusion ;
- Encodage et compression : le flux est encodé dans un format numérique, ce qui permet de réduire la taille des fichiers en préservant la qualité et d'assurer un passage efficace du fichier sur la bande passante ;
- Stockage des contenus : les services IPTV proposent des contenus à la demande de sorte que les flux vidéo encodés sont stockés sur des serveurs dédiés ;
- Transmission via le protocole IP : le protocole IP est une méthode utilisée pour envoyer des données sur internet. Le contenu IPTV est envoyé après avoir été découpé en paquets, qui contient deux informations, à savoir l'adresse IP source (adresse du serveur qui envoie le contenu) et l'adresse de destination ;
- Accès utilisateur : les utilisateurs des services IPTV illégaux accèdent au contenu via des applications installées sur de multiples supports électroniques (smartphones, tablettes, ordinateurs, téléviseurs, ...).

Ces plateformes pirates, utilisant l'IPTV, fonctionnent sans licence ni autorisation des requérantes.

11. En l'occurrence, les requérantes visent cinq offres illégales IPTV, à savoir :
1. LEMEILLEURIPTV
 2. BESTIPTVABO
 3. ATLASPRO12
 4. OTT PREMIUM
 5. MIJNIPTV

A l'Annexe 1 de la requête, sont identifiés, les noms de domaine renvoyant actuellement aux pages d'accueil des services IPTV visés par les requérantes. Y sont également visés les noms de domaine passerelle (et les URLs associées) utilisés par ces services illégaux qui seront ultérieurement identifiés par le Service et/ou les requérantes.

A cet égard, les requérantes déposent des captures d'écran démontrant un accès à des contenus de chaînes télévisées et de films et séries, à la demande, en grande quantité et à des prix très inférieurs à ceux des services IPTV légaux. A l'appui de leur demande, les requérantes expliquent d'ailleurs que ces plateformes pirates autorisent des modes de paiement par cryptomonnaie, ce qui serait, selon elles, un indicateur de l'illégalité du service. Il ressort également de leurs écrits que lesdites plateformes guident les utilisateurs finaux pour contourner d'éventuelles mesures de blocage.

Le caractère contrefaisant des services IPTV ci-visés est, en outre, *prima facie* confirmé par la pièce C déposée par les requérantes, montrant que les chaînes des requérantes sont comprises dans les offres IPTV.

12. S'agissant du caractère **manifeste** de l'atteinte, les requérantes exposent, à bon escient, que les plateformes IPTV ci-visées se livrent à une diffusion non autorisée de leurs émissions, en proposant aux utilisateurs un accès illicite aux retransmissions de leur contenu audiovisuel, que ce soit en direct ou en différé.

L'atteinte manifeste aux droits voisins des requérantes est *prima facie* suffisamment manifeste.

13. Quant au caractère **considérable** des atteintes portées, les requérantes déposent des pièces attestant qu'elles le sont tant au niveau quantitatif que qualitatif.

Les atteintes sont quantitativement considérables dès lors que les services IPTV visés sont structurellement contrefaisants en donnant accès à une pléthore (des milliers) d'émissions sans autorisation. L'atteinte n'est en outre pas strictement limitée à l'un ou l'autre de leurs programmes, mais à l'ensemble de leurs émissions.

Elles sont également qualitativement considérables puisque les services IPTV permettent d'accéder à du contenu protégé à des moments critiques, notamment au moment où ce contenu est retransmis en direct. Ces services exploitent en outre le contenu audiovisuel des requérantes aux fins de réaliser des bénéfices. La valeur économique des droits des requérantes s'en trouve compromise puisque les atteintes ont pour effet de détourner leurs audiences vers des services IPTV illégaux.

14. Les atteintes aux droits invoqués par les requérantes sont *prima facie* manifestes et considérables.

• **Quant à la balance des intérêts en présence**

15. La troisième condition de l'article XVII.34/1, § 6, du CDE requiert une pondération des intérêts, droits et libertés, en ce compris l'intérêt général. Il incombe au Président d'évaluer l'impact potentiel des mesures sollicitées sur l'accès du public aux informations ou à tout autre contenu qui ne porterait pas atteinte aux droits invoqués.

La pondération des intérêts en présence penche en faveur des requérantes. Les faits de la cause et les pièces déposées sont en effet de nature à justifier raisonnablement les mesures postulées.

Les requérantes avancent les justifications suivantes, que Nous faisons nôtres :

- la démonstration de l'atteinte grave portée à leurs droits exclusifs est suffisamment rapportée ;
- l'intérêt général plaide en faveur de l'octroi des mesures ;
- le droit à la liberté d'information des internautes demeure intact puisque les mesures sollicitées portent exclusivement sur des services IPTV illicites, dont les liens internet ont été précisément désignés par les requérantes, et dont les contenus sont structurellement contrefaisants ;
- les mesures sollicitées ne sont pas illimitées dans le temps puisqu'elles sont soumises à un mécanisme de déblocage dans l'hypothèse où le nom de domaine visé ne renverrait plus vers du contenu structurellement contrefaisant ;
- les mesures sollicitées n'affectent pas le droit à la vie privée des internautes puisqu'elles n'impliquent pas la collecte de données les concernant ;
- les mesures sollicitées n'affectent *prima facie* pas l'essence de la liberté d'entreprise des intermédiaires visés dès lors que :

- des garanties procédurales sont mises à leur disposition, via le Service, sous l'égide duquel des discussions auront lieu pour assurer la mise en œuvre des mesures ;
- aucune astreinte n'est, à ce jour, prononcée, de sorte qu'ils ne risquent pas de subir le moindre préjudice financier ;
- suivant les requérantes, les FAI's, Google et Cloudflare mettent déjà en œuvre des mesures de blocage au niveau du CDN et/ou de l'hébergement, ainsi que des mesures de déréférencement.

Les mesures de blocage sont efficaces et limitent leur impact à l'objectif poursuivi, de sorte que la réponse est proportionnée face aux violations constatées.

Le critère de proportionnalité est dès lors rencontré en l'espèce.

c. Destinataires des mesures

16. Afin de mettre fin aux atteintes aux droits voisins du droit d'auteur identifiées par les requérantes, celles-ci sollicitent de la part des intermédiaires destinataires de la présente ordonnance des mesures de blocage dynamique.

Elles dirigent à cet effet ces demandes à l'encontre des fournisseurs d'accès à internet (les « FAIs ») et également à l'encontre de Google et Cloudflare.

17. Les travaux préparatoires et la doctrine enseignent que la notion d'« intermédiaire » s'entend largement². Elle couvre celui qui fournit un service susceptible d'être employé par une ou plusieurs autres personnes pour permettre l'exploitation illégale d'un jeu de hasard en ligne, sans qu'il soit nécessaire qu'il entretienne une relation particulière avec cette ou ces personnes. Sont visés par exemple les fournisseurs d'accès à internet et les hébergeurs, mais aussi les intermédiaires de paiements, les exploitants de moteurs de recherche, les gestionnaires de noms de domaine³.

18. En l'espèce, les « intermédiaires » visés par les requérantes sont des fournisseurs d'accès à internet et couvrent une majeure partie de la population belge. Il s'agit en effet de :

- La SA PROXIMUS ;
- La SPRL TELENET,
- La SA ORANGE BELGIUM NV,
- La SA DIGI COMMUNICATIONS BELGIUM,
- La SA MOBILE VIKINGS.

Les FAI's sont, selon les requérantes, des acteurs incontournables pour la mise en œuvre des mesures de restriction d'accès aux contenus illégaux dès lors que, parmi les services qu'ils proposent, figurent leurs propres serveurs DNS (*Domain Name System*) qui sont utilisés par défaut par leurs abonnés et par les opérateurs virtuels (qui ne disposent donc pas d'infrastructures physiques propres) qui s'appuient sur leurs réseaux.

Les mesures sont également dirigées contre **CLOUDFLARE**, en sa qualité de fournisseur de service de réseau de diffusion de contenu (CDN) et/ou hébergeur. Elle fournit des services susceptibles d'être utilisés par une ou plusieurs personnes pour porter atteinte aux droits des requérantes. En effet, via

² E. CORNU, « L'injonction dynamique Une nouvelle procédure judiciaire particulière (droit d'auteur, droits voisins et exploitation illégale des jeux de hasard en ligne) », *J.T.*, 2025, p. 148 ; Exposé des motifs, p. 126.

³ *Ibid.*, p. 148.

son service CDN, CLOUDFLARE offre un ensemble de serveurs répartis géographiquement qui mettent en cache le contenu à proximité des utilisateurs finaux. Un tel service permet le transfert rapide des ressources nécessaires au chargement d'un site Internet, notamment les vidéos ou fichiers multimédias volumineux. Elle est dès lors, selon les requérantes, un maillon essentiel de l'infrastructure technique utilisée par des sites pirates pour diffuser rapidement, efficacement et anonymement des contenus contrefaisants.

Enfin, les requérantes désignent également **GOOGLE** en sa qualité d'hébergeur (*Google Sites* et/ou *Google Cloud Platform*) et en sa qualité de moteur de recherche (*Google Search / Ads*), comme intermédiaire. Selon les requérantes, son moteur de recherche indexe, référence et met à disposition des internautes des liens menant vers les sites contrefaisants, augmentant leur visibilité et facilitant leur accès par le public. En outre, elle fournit des services d'hébergement de sites internet pouvant être utilisés par des sites pirates.

Il s'observe que la mission du Service, telle que libellée par les requérantes, tient spécialement compte de l'offre de services, ainsi décrite, de Cloudflare et de Google (*cfi: infra*).

Les intermédiaires visés par les requérantes proposent des services susceptibles *prima facie* d'être utilisés directement ou indirectement pour accéder aux sites litigieux, de sorte qu'ils peuvent être valablement visés par les mesures provisoires.

19. Les conditions visées à l'article XVII.34/1, § 6, al. 1^{er}, du CDE, sont dès lors remplies. Il convient de mettre fin aux atteintes vantées par les requérantes.

d. Quant aux mesures postulées

20. Afin d'obtenir la cessation des atteintes à leurs droits voisins du droit d'auteur, les requérantes sollicitent de la part des destinataires des mesures de blocage dynamique à l'encontre des sites internet actuellement disponibles via les noms de domaine énumérés en Annexe 1 de la requête jointe à la présente ordonnance.

21. Il s'agit d'un blocage « dynamique ». L'article XVII.34/1, § 8, du CDE précise en effet que le président peut : « (...) *fixer les mesures spécifiques qui doivent être prises par le(s) destinataire(s) de son ordonnance pour mettre fin à l'atteinte dénoncée ou limiter les conséquences de celle-ci. Le président du tribunal de l'entreprise peut notamment décider d'étendre les mesures provisoires à tout ou partie d'un site web répliquant le site web identifié dans l'ordonnance et faisant l'objet des mesures provisoires, ou à toute adresse donnant directement accès à celui-ci* ».

Il s'agit donc de viser non seulement les noms de domaine identifiés dans la requête, mais également les noms de domaine contournant les mesures de blocage, via des redirections et/ou des sites miroirs et/ou des « cpycats » (traduction libre : sites copies). Les mesures de blocage feront dès lors régulièrement l'objet de mises à jour.

22. Les requérantes détaillent dans leur requête les différentes mesures qu'elles sollicitent, auxquelles Nous nous rallions.

Outre la liste des « sites cibles » qu'elles fournissent à l'annexe 1 de leur requête, les requérantes déposent également une annexe 2.a., qualifiée de confidentielle, et dans laquelle les requérantes expliquent le phénomène des marques pirates, avant de fournir, en annexe 2.b, une liste de 5 noms de

marques pirates (les services IPTV ci-visés). Ces noms sont utilisés par les pirates comme moyen d'identification de l'offre de contenu audiovisuel (films et séries) de façon illégale.

23. Dans ces circonstances, il s'impose de bloquer non seulement les noms de domaine identifiés dans l'annexe 1 mais aussi les noms de domaine qui contourneront les mesures d'interdiction. A bon escient, la demande de blocage vise dès lors :

- les noms de domaine actuellement identifiés et énumérés dans l'annexe 1 de la requête, annexée à la présente ordonnance, étant les « sites cibles » ;
- les noms de domaine donnant accès aux « sites cibles », par le biais de sites miroirs et de redirections qui seront ultérieurement identifiés par les requérantes et/ou par le Service et notifiés aux intermédiaires par le Service sur une base régulière ;
- les noms de domaine donnant accès à des répliques (ou copycats) des « sites cibles », qui seront ultérieurement identifiés par les requérantes et/ou le Service et notifiés aux intermédiaires par le Service sur une base régulière.

Il en découle que les mesures de blocage seront régulièrement mises à jour sur la base de nouveaux noms de domaine qui auraient été identifiés par les requérantes et, le cas échéant, en collaboration avec le Service, pour être ensuite notifiés pour blocage aux intermédiaires visés par la présente ordonnance.

24. D'autre part, s'agissant spécialement du risque de bloquer un site qui, bien qu'utilisant une « marque pirate » n'offrirait pas de contenu contrefaisant, les requérantes s'engagent, dans le cadre des mises à jour qu'elles prévoient, à demander exclusivement le blocage de sites internet qui satisfont aux critères cumulatifs suivants :

1. ils satisfont aux critères confidentiels exposés dans l'Annexe 2.b. ;
2. ils sont, tout comme les Sites Cibles, structurellement dédiés à la contrefaçon de masse de contenu audio-visuel ;
3. ils offrent, notamment, du contenu sur lequel les requérantes possèdent des droits exclusifs ;
4. ils sont accessibles en Belgique
5. aucune licence d'exploitation n'a été concédée aux opérateurs de ces sites par les requérantes.

Ces garanties apparaissent suffisantes et proportionnées à la lumière des atteintes subies par les requérantes.

A juste titre, l'annexe 2, tenue pour confidentielle par les requérantes, ne sera pas divulguée avec la présente ordonnance pour éviter que les contrefacteurs n'adaptent leurs noms de façon à éviter de tomber sous l'application de la présente ordonnance. Il appartiendra cependant bien aux requérantes de communiquer l'annexe 2 à qui de droit, une fois l'ordonnance prononcée.

e. Quant au rôle du Service

25. Les requérantes sollicitent que le Service visé à l'article XVII.34/3, du CDE soit impliqué dans la mise en œuvre des mesures sollicitées. Celui-ci peut en effet être chargé par le Président de tout ce qui relève des modalités d'application des mesures provisoires ordonnées.

Les requérantes précisent le périmètre d'intervention du Service, dont la mission est conforme aux articles XVII.34/1 et suivants CDE. Le libellé de ces mesures et du rôle du Service apparaît en outre

clair et sans ambiguïté de sorte que la requérante a légitimement pu solliciter les mesures par voie unilatérale.

En effet, s'il est vrai que l'article XVII.34/1, §6, du CDE dispose que le président peut, avant d'ordonner des mesures, entendre les destinataires de celles-ci, il apparaît en l'espèce que les mesures à ordonner sont particulièrement claires, dès lors qu'elles se résument en réalité à ordonner le blocage des sites internet visés. En revanche, il pourrait s'avérer que les modalités pratiques de mise en œuvre et d'exécution des mesures de blocage puissent soulever des difficultés.

Le président observe que le législateur a précisément entendu rencontrer ces préoccupations en instituant le Service au sein du SPF Economie. Comme l'écrit la doctrine : *« Afin d'assurer l'efficacité des mesures provisoires qui pourraient être accordées dans le cadre de cette nouvelle procédure et de résoudre les difficultés pratiques qui interviennent souvent dans l'exécution de mesures de cessation, cette réforme institue également le Service de lutte contre les atteintes au droit d'auteur et aux droits voisins commises en ligne et contre l'exploitation de jeux de hasard en ligne. »*⁴

L'option choisie par le législateur se reflète dans la structure du Titre 1/1 du Livre XVII du Code de droit économique. Le législateur a en effet pris le soin de distinguer la phase judiciaire d'une procédure en injonction dynamique (octroi des mesures - articles XVII.34/1 et XVII.34/2), de la phase de mise en œuvre de l'injonction dynamique (détermination des modalités d'application des mesures - article XVII.34/3).

En conséquence, la présente ordonnance habilitera le Service pour préciser toutes les modalités d'application et d'exécution des mesures techniques de blocage. Elle lui confiera également le soin du suivi de la mise en œuvre des mesures de blocage.

Il apparaît dès lors que ce sera sous la supervision du Service que les intermédiaires pourront utilement faire valoir les spécificités techniques les concernant en rapport avec l'exécution des mesures de blocage. Le cas échéant, il sera fait application par le Service de l'article XVII.34/3, § 2, al. 2, du CDE.

26. En l'espèce, et dans le respect des principes ci-rappelés, le Service sera chargé d'adapter les modalités d'application des mesures dynamiques ordonnées, de superviser, coordonner et d'assurer une mise en œuvre rigoureuse des mesures provisoires ordonnées, afin de garantir une application conforme aux objectifs d'efficacité poursuivis, et d'examiner l'impact effectif des mesures ordonnées.

A cet égard, il incombera au Service de :

- déterminer les modalités d'application des mesures ordonnées, en concertation avec les requérantes et les intermédiaires, notamment :
 - o le calendrier exact de mise en œuvre par les intermédiaires des mesures ordonnées,
 - o le format et le canal de communication des notifications dans le cadre des Mises à jour ;
 - o le contenu de la page internet que les utilisateurs verront en lieu et place du site pirate auquel ils auront tenté d'accéder.
- mettre en œuvre et coordonner la Mise à jour des mesures ordonnées: le Service identifie, avec l'aide des Requérantes pour autant que celle-ci soit nécessaire, les noms de domaine de

⁴ E. CORNU, *op. cit.* p. 145.

contournement (redirections, sites miroirs, copycats), ainsi que les noms de domaine passerelle (et URL associés), encadre le processus de Mise à jour, agissant comme intermédiaire entre les Requérantes et les Intermédiaires. Lorsque le Service notifie les Mises à jour aux Intermédiaires, sa notification est également adressée aux requérantes ;

- identifier lesquels des Sites Cibles (y compris les redirections, sites miroirs et copycats) font appel aux services d'hébergement et/ou de CDN de Cloudflare ;
- identifier lesquels des Sites Cibles (y compris les redirections, sites miroirs et copycats) utilisent les services d'hébergement de Google (Google Sites ou Google Cloud Platform) ;
- s'assurer de la mise en œuvre effective des mesures par les Intermédiaires: le Service veille à ce que les Intermédiaires appliquent les mesures ordonnées de manière conforme aux prescriptions de l'ordonnance et aux modalités d'application déterminées. Il assure également un suivi attentif afin de détecter d'éventuelles défaillances dans cette mise en œuvre et d'y remédier rapidement, évitant ainsi tout retard ou inadéquation susceptible de compromettre l'efficacité des mesures prises.
- surveiller l'impact des actions mises en place, le cas échéant en collaboration avec les Intermédiaires et les Requérantes.

Cette mission du Service tient spécialement compte de (i.) l'offre de Cloudflare, qui propose un service de réseau de diffusion de contenu (CDN) et un service d'hébergement, et de (ii.) l'offre de Google qui met à la disposition des utilisateurs un moteur de recherche (« Google Search ») ainsi qu'un service d'hébergement (« Google Sites » et « Google Cloud »).

Pareille mission, strictement cantonnée aux offres respectives de Cloudflare et Google, telles que décrites par les requérantes, n'emporte *prima facie* pas d'atteinte disproportionnée aux intérêts de ces intermédiaires.

Cette implication du Service garantira une application efficiente et proportionnée des mesures ordonnées, assurant que les mesures soient adaptées aux réalités des violations aux droits d'auteur commises.

PAR CES MOTIFS,

Statuant sur pièces ;

Disons la requête recevable et fondée, et par conséquent :

- constatons que les noms de domaine identifiés en Annexe 1 (les Sites Cibles) donnent accès à des sites/offres Internet par lesquels il est porté atteinte aux droits voisins de radiodiffuseur (art. XI.215, §1er, CDE) appartenant aux requérantes ;
- constatons que les services des Intermédiaires sont utilisés ou susceptibles d'être utilisés par les opérateurs des Sites Cibles pour porter atteinte à des droits voisins appartenant aux requérantes ; et par conséquent :
- ordonnons à :
 - ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM et MOBILE VIKINGS en leur qualité de FAIs et partant fournisseurs de service de résolution de noms de domaine de mettre en œuvre, à leurs propres frais, des mesures de nature à empêcher l'accès, depuis le territoire belge aux :
 - CLOUDFLARE en sa qualité de fournisseur de service de réseau de diffusion de contenu (CDN) et/ou hébergeur de mettre en œuvre, à ses propres frais des mesures de nature à empêcher l'accès, depuis le territoire belge aux :
 - GOOGLE en sa qualité d'hébergeur (Google Sites et/ou Google Cloud Platform), de mettre en œuvre, à ses propres frais, des mesures de nature à empêcher l'accès aux :
 - GOOGLE en sa qualité de moteur de recherche (Google Search / Ads), de mettre en œuvre, à ses propres frais, des mesures de déréférencement et de désactivation des annonces associées aux :
 - Sites Cibles ;
 - mais également aux sites de redirection, sites miroir, noms de domaine passerelle ou, conformément aux conditions posées à l'Annexe 2, sites copycats,
 - qui leur seront ultérieurement notifiés par le Service, dans le cadre des mises à jour régulières de mesures de blocage,
 - et pour lesquels les requérantes s'engagent à ne solliciter le blocage que de sites internet qui satisfont aux critères cumulatifs suivants:
 - v. ils sont, comme les Sites Cibles, structurellement dédiés à la contrefaçon de masse de contenu audiovisuel;
 - vi. ils offrent, notamment, du contenu sur lequel les Requérantes possèdent des droits exclusifs;
 - vii. ils sont accessibles en Belgique;
 - viii. aucune licence d'exploitation n'a été concédée aux opérateurs de ces sites par les Requérantes.

- ordonnons à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM, MOBILE VIKINGS, GOOGLE et CLOUDFLARE de mettre en œuvre, à leurs propres frais, dans le cadre de leurs services respectifs, des mesures de nature à débloquent l'accès ou de nature à de nouveau référencer, depuis le territoire belge, tout nom de domaine qui a déjà été notifié aux Intermédiaires en vertu de la présente ordonnance, mais dont l'objectif unique ou prédominant n'est plus de donner accès à un Site Cible ou de répliquer celui-ci, qui leur seront notifiés ultérieurement par le Service ;
- ordonnons à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM, MOBILE VIKINGS, GOOGLE et CLOUDFLARE de mettre en œuvre les mesures de blocage et de déblocage précitées selon les modalités, la fréquence et le délai déterminé par le Service étant entendu que la requérante ou, le cas échéant le service s'il dispense la requérante d'y procéder, procédera annuellement, selon la même méthodologie que celle appliquée pour solliciter le blocage des sites visés dans la requête, à un screening de tous les sites bloqués et remettra au Service dans le mois dudit screening l'ensemble de ses recherches et tiendra ceux-ci à la disposition de toute partie à la procédure. Dans ce contexte la requérante communiquera au Service les éléments pertinents démontrant qu'un ou plusieurs des sites litigieux visés par les mesures auraient perdu leur caractère illégal. Le cas échéant, le Service enverra aux destinataires des mesures la notification que le ou les sites litigieux devront faire l'objet d'un déblocage ;
- ordonnons à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM et et MOBILE VIKINGS de prendre des mesures de redirection, afin que leurs clients qui auront tenté d'accéder à un nom de domaine bloqué, soient redirigés vers une page internet dont le contenu sera déterminé par le Service en collaboration avec les requérantes ;
- ordonnons à ORANGE BELGIUM, PROXIMUS, TELENET, DIGI COMMUNICATIONS BELGIUM et et MOBILE VIKINGS, en leur qualité d'intermédiaire au sens de l'article XVII.34 CDE, d'appliquer ces mesures techniques de blocage et de redirection à l'ensemble de leurs clients ayant souscrit à un service d'accès à Internet, et ce indépendamment du type d'abonnement concerné (privé, professionnel, mobile ou fixe) ;
- chargeons le Service de :
 - déterminer les modalités d'application des mesures ordonnées, en concertation avec les Requérantes et les Intermédiaires, notamment :
 - le calendrier exact de mise en œuvre par les Intermédiaires des mesures ordonnées,
 - le format des notifications dans le cadre des Mises à jour ;
 - le contenu de la page internet que les utilisateurs verront en lieu et place du site pirate auquel ils auront tenté d'accéder.
 - mettre en œuvre et coordonner la Mise à jour des mesures ordonnées et notamment :
 - identifier, avec l'aide des Requérantes pour autant que celle-ci soit nécessaire, les noms de domaine de contournement (redirections, sites miroirs, copycats) ainsi que les noms de domain / URL passerelle ;
 - Identifier lesquels des Sites Cibles (y compris les redirections, sites miroirs et copycats) font appel aux services d'hébergement et/ou de CDN de Cloudflare ;
 - Identifier lesquels des Sites Cibles (y compris les redirections, sites miroirs et copycats) utilisent les services d'hébergement de Google (Google Sites ou Google Cloud Platform) ;

- se positionner comme intermédiaire entre les Requérantes et les Intermédiaires, notamment en notifiant les Sites Cibles ainsi que les Mises à Jour aux intermédiaires. Lorsque le Service notifie les Mises à jour aux Intermédiaires, sa notification est également adressée aux Requérantes ;
- s'assurer de la mise en œuvre effective des mesures ordonnées par les Intermédiaires (y compris chaque Mise à jour), d'une part via des confirmations obtenues des Intermédiaires et, d'autre part, via des vérifications pratiques effectuées par le Service lui-même ;
- surveiller l'impact des actions mises en place, notamment:
 - en récoltant les statistiques de consultation de la page internet que les utilisateurs verront en lieu et place du site pirate auquel ils auront tenté d'accéder, ainsi que l'évolution de celles-ci ;
 - en se concertant avec les Intermédiaires visés sur la manière la plus efficace d'évaluer, en collaboration, l'impact des mesures;
- Prenons acte du caractère confidentiel de l'Annexe 2 (a et b). En conséquence, ne l'annexons pas à la présente ordonnance mais laissons le soin aux requérantes de la diffuser à qui de droit ;
- Délaissons solidairement aux requérantes la charge de leurs dépens, dont les frais de mise au rôle de 165 € ;
- Déclarons la présente ordonnance exécutoire sur minute.

Fait en notre cabinet au tribunal de l'entreprise francophone de Bruxelles, boulevard de Waterloo 70 à 1000 Bruxelles, le 30 janvier 2026.

Le greffier

Le président,



