Texte intégral

Autre

RÉPUBLIQUE FRANÇAISE

AU NOM DU PEUPLE FRANÇAIS

Copies exécutoires RÉPUBLIQUE FRANÇAISE

délivrées aux parties le : AU NOM DU PEUPLE FRANÇAIS

COUR D'APPEL DE PARIS

Pôle 5 - Chambre 2

ARRÊT DU 13 JUIN 2025

(n°74, 16 pages)

Numéro d'inscription au répertoire général : n° RG 23/02588 - n° Portalis 35L7-V-B7H-CHCNJ

Décision déférée à la Cour : jugement du 25 octobre 2022 - Tribunal judiciaire de PARIS - 3ème chambre 3ème section - RG n°16/16346

APPELANTE

Société INTELLECTUAL VENTURES I LLC, société de droit américain, agissant en la personne de son 'manager' (gérant) domicilié en cette qualité au siège social situé

[Adresse 2]

[Adresse 6]

[Adresse 5]

[Adresse 4]

ÉTATS-UNIS D'AMÉRIQUE

Représentée par Me Julien FRENEAUX de la SAS BARDEHLE PAGENBERG, avocat au barreau de PARIS, toque P 390

INTIMÉE

S.A. SOCIETE FRANÇAISE DU RADIOTELEPHONE, prise en la personne de ses représentants légaux domiciliés en cette qualité au siège social situé

[Adresse 1]

[Localité 3]

Représentée par Me Michel ABELLO de la SELARL LOYER & ABELLO, avocat au barreau de PARIS, toque J 049

Assistée de Me Guillaume DUBOS plaidant pour la SELARL LOYER & ABELLO, avocat au barreau de PARIS, toque J 049

COMPOSITION DE LA COUR :

L'affaire a été débattue le 6 mars 2025, en audience publique, devant la Cour composée de :

Mme Véronique RENARD, Présidente de chambre, Présidente

Mme Marie SALORD, Présidente de chambre

M. Gilles BUFFET, Conseiller

qui en ont délibéré

Un rapport a été présenté à l'audience dans les conditions prévues par l'article 804 du code de procédure civile.

Greffière lors des débats : Mme Carole TREJAUT

ARRET :

Contradictoire

Par mise à disposition de l'arrêt au greffe de la Cour, les parties en ayant été préalablement avisées dans les conditions prévues au deuxième alinéa de l'article 450 du code de procédure civile

Signé par Mme Véronique RENARD, Présidente de chambre, Présidente, et par Mme Carole TREJAUT, Greffière, présente lors de la mise à disposition.

Vu le jugement rendu le 25 octobre 2022 par le tribunal judiciaire de Paris,

Vu l'appel interjeté par la société Intellectual Ventures I LLC le 27 janvier 2023,

Vu les dernières conclusions (« conclusions d'appelant n°4 ») notifiées par la société Intellectual Ventures I LLC le 14 janvier 2025,

Vu les dernières conclusions (« conclusions d'intimée n°3 ») notifiées par la société SFR le 19 décembre 2024,

Vu l'ordonnance de clôture du 16 janvier 2025.

SUR CE, LA COUR

La société de droit américain Intellectual Ventures I LLC fait partie du groupe des sociétés Intellectual Ventures et est spécialisée dans la création, le développement, l'acquisition et l'exploitation d'inventions.

La société Intellectual Ventures I est titulaire du brevet européen désignant la France EP 1 304 002 (EP'002) ayant pour titre « Organisation d'un chiffrement de données dans un système de communications sans fil ». Ce brevet, déposé le 28 juin 2001, est issu d'une demande internationale PCT WO 02/03730 déposée le 28 juin 2001, avec revendication de la priorité d'une demande de brevet

finlandais n°20001567 de la société Nokia Corporation du 30 juin 2000. La mention de la délivrance du brevet a été publiée le 23 janvier 2008.

Le 15 novembre 2019, la société Intellectual Ventures I a déposé auprès du directeur général de l'INPI une requête en limitation de la partie française du brevet EP'002, laquelle a été acceptée par décision du 8 janvier 2020, et inscrite au registre national des brevets le 9 janvier 2020.

Le brevet EP'002 a expiré le 28 juin 2021.

La Société Française de Radiotéléphone (SFR) est l'un des principaux opérateurs en matière de télécommunications en France. Elle offre à ses abonnés mobiles un service « Auto Connect Wifi » leur permettant de basculer automatiquement de leur connexion internet du réseau mobile vers le réseau SFR WiFi Mobile, la connexion se faisant par authentification de la carte SIM grâce à la technologie EAP-SIM (Extensible Authentification Protocol for Subscriber Identity Module).

La société Intellectual Ventures I considérant que le service « Auto Connect WiFi » proposé par la société SFR à ses abonnés mobiles au moyen de l'application « SFR WiFi » téléchargeable sur leurs terminaux mobiles utilisait le procédé objet de la revendication 1 du brevet EP'002, que les terminaux sans fil (notamment téléphones mobiles et tablettes) et les cartes SIM que la société SFR offrait de livrer et livrait à ses abonnés en France constituaient des moyens essentiels de mise en 'uvre d'un terminal sans fil reproduisant les caractéristiques de la revendication 11 du brevet EP'002 et que les « Hotspots WiFi » de la société SFR reproduisaient les caractéristiques du point d'accès pour un réseau local sans fil objet de la revendication 14 dudit brevet, a été autorisée, par ordonnance présidentielle du 4 octobre 2016, à faire pratiquer une saisie-contrefaçon dans les locaux de la société SFR, laquelle s'est déroulée les 13 et 14 octobre 2016.

Par exploit d'huissier de justice du 14 novembre 2016, la société Intellectual Ventures I a fait assigner la société SFR devant le tribunal judiciaire de Paris en contrefaçon de la partie française du brevet EP'002.

Par jugement du 25 octobre 2022, ce tribunal a :

- rejeté les demandes de la société SFR aux fins d'annulation des preuves (procès-verbaux de saisie contrefaçon, de constat d'achat et des rapports d'expertise privée) ;

- dit que les revendications 1, 11 et 14 de la partie française du brevet EP 1 304 002 sont nulles pour extension de l'objet du brevet au-delà de la demande telle que déposée ;

- ordonné, à l'initiative de la partie la plus diligente, la transmission de la présente décision, une fois passée en force jugée, à l'INPI aux fins d'inscription au Registre National des Brevets ;

- rejeté par conséquent toutes les demandes fondées sur la contrefaçon de ce brevet ;

- condamné la société Intellectual Ventures I à payer à la société SFR la somme de 50 000 euros à titre de dommages-intérêts réparant le préjudice causé par le dénigrement commis ;

- condamné la société Intellectual Ventures I aux dépens,

- condamné la société Intellectual Ventures I à payer à la société SFR la somme de 450 000 euros par application des dispositions de l'article 700 du code de procédure civile ;

- ordonné l'exécution provisoire sauf en ce qui concerne la transcription du jugement au Registre National des Brevets.

Par déclaration matérialisée par la voie électronique le 27 janvier 2023, la société Intellectual Ventures I a interjeté appel de cette décision.

Aux termes de ses dernières conclusions notifiées par la voie électronique le 14 janvier 2025, la société Intellectual Ventures I demande à la cour de :

- infirmer le jugement en ce qu'il a :

- dit que les revendications 1, 11 et 14 de la partie française du brevet EP 1 304 002 sont nulles pour extension de l'objet du brevet au-delà de la demande telle que déposée ;

- ordonné, à l'initiative de la partie la plus diligente, la transmission de la présente décision, une fois passée en force jugée, à l'INPI aux fins d'inscription au Registre National des Brevets ;

- rejeté par conséquent toutes les demandes fondées sur la contrefaçon de ce brevet ;

- condamné la société Intellectual Ventures I à payer à la société SFR la somme de 50 000 euros à titre de dommages-intérêts réparant le préjudice causé par le dénigrement commis ;

- condamné la société Intellectual Ventures I aux dépens ;

- condamné la société Intellectual Ventures I à payer à la société SFR la somme de 450 000 euros par application des dispositions de l'article 700 du code de procédure civile ;

- ordonné l'exécution provisoire, sauf en ce qui concerne la transcription au Registre National des Brevets.

Statuant à nouveau :

- déclarer irrecevables, et en tout cas infondés, l'ensemble des moyens, fins, conclusions et demandes de la société SFR, y compris ses demandes en nullité des revendications 1, 11 et 14, de la partie française du brevet européen EP 1 304 002 ; l'en débouter ;

- dire et juger qu'en mettant en 'uvre sur le territoire français un service dénommé "Auto Connect WiFi" utilisant le protocole de communication réseau dénommé "EAP-SIM" (pour "Extensible Authentication Protocol ' Subscriber Identity Module") dans un réseau local sans fil de type WiFi, la société SFR a commis et commet des actes de contrefaçon par utilisation du procédé objet de la revendication 1 de la partie française du brevet EP 1 304 002, en violation de l'interdiction posée par l'article L.613-3 b) du code de la propriété intellectuelle ;

- dire et juger qu'en offrant et en mettant dans le commerce sur le territoire français des téléphones mobiles et tablettes (de marques autres que HUAWEI ou HONOR) aptes à mettre en 'uvre le protocole de communication réseau dénommé "EAP-SIM" (pour "Extensible Authentication Protocol ' Subscriber Identity Module") dans un réseau local sans fil de type WiFi, la société SFR a commis et commet des actes de contrefaçon de la revendication 11 de la partie française du brevet européen EP 1 304 002, par violation de l'interdiction posée par l'article L.613-3 a) du code de la propriété intellectuelle ;

- dire et juger qu'en offrant, en mettant dans le commerce et utilisant sur le territoire français des points d'accès pour un réseau local sans fil appelés "Hotspots WiFi", y compris les box des abonnés à son réseau de télécommunication fixe émettant un réseau WiFi public et aptes à mettre en 'uvre le protocole de communication réseau dénommé "EAP-SIM" (pour "Extensible Authentication Protocol ' Subscriber Identity Module"), la société SFR a commis et commet des actes de contrefaçon de la revendication 14 de la partie française du brevet européen EP 1 304 002, par violation de l'interdiction posée par l'article L.613-3 a) du code de la propriété intellectuelle ;

- dire et juger qu'en commettant les actes précités, la société SFR a engagé sa responsabilité civile envers la société Intellectual Ventures I, propriétaire dudit brevet, sur le fondement de l'article L.615-1 du code de la propriété intellectuelle ;

- ordonner à la société SFR de communiquer à la société Intellectual Ventures I, sous astreinte de 50 000 euros par jour de retard à compter de la signification de l'arrêt à intervenir :

- le nombre de téléchargements de l'application SFR WiFi par les abonnés mobiles de la société SFR,

- le nombre, la durée et le volume des connexions de données aux "Hotspots WiFi" de la société SFR, y compris les box des abonnés à son réseau de télécommunication fixe, intervenues sur le territoire français par mise en 'uvre du service "Auto Connect WiFi" ou tout autre service utilisant le protocole de communication réseau dénommé "EAP-SIM" (pour "Extensible Authentication Protocol ' Subscriber Identity Module") dans un réseau local sans fil de type WiFi,

- les quantités, modèles, prix d'achat, prix de vente, et origine des téléphones mobiles et tablettes (de marques autres que HUAWEI ou HONOR) aptes à mettre en 'uvre le protocole de communication réseau dénommé "EAP-SIM" (pour "Extensible Authentication Protocol ' Subscriber Identity Module") dans un réseau local sans fil de type WiFi, qui ont été offerts et mis dans le commerce par la société SFR sur le territoire français,

- les quantités, modèles, prix d'achat, et origine des points d'accès pour un réseau local sans fil appelés "Hotspots WiFi", y compris les box des abonnés au réseau de télécommunication fixe SFR émettant un

réseau WiFi public et aptes à mettre en 'uvre le protocole de communication réseau dénommé "EAP-SIM" (pour "Extensible Authentication Protocol ' Subscriber Identity Module"), qui ont été offerts, mis dans le commerce et utilisés par la société SFR sur le territoire français,

et ce pour la période couvrant les cinq années précédant l'introduction de l'instance jusqu'à la date d'expiration du brevet EP'002, soit du 14 novembre 2011 au 28 juin 2021.

- avant dire droit sur les dommages et intérêts, commettre tel expert qu'il plaira à la cour de désigner, aux frais avancés de la société SFR, avec pour mission de vérifier l'exactitude et l'exhaustivité des informations communiquées par cette dernière en exécution de l'arrêt à intervenir, et de fournir à la cour tous les éléments lui permettant de statuer ultérieurement sur le montant des dommages et intérêts en fonction de la méthode de calcul dont la société Intellectual Ventures aura fait le choix au vu des informations communiquées par la société SFR et vérifiées par l'expert ;

- dans l'attente de l'issue des mesures de production de pièces et d'expertise, condamner d'ores et déjà la société SFR à payer à la société Intellectual Ventures I la somme de 5 000 000 euros à titre de provision à valoir sur les dommages et intérêts ;

- ordonner la publication du dispositif de l'arrêt à intervenir dans cinq journaux ou magazines au choix de la société Intellectual Ventures I, et aux frais de la société SFR, dans la limite de 15 000 euros HT par insertion ;

- ordonner à la société SFR d'afficher en page d'accueil du site internet www.sfr.fr un encart occupant au moins 10% de la surface de la page d'accueil au-dessus de la ligne de flottaison et contenant le lien hypertexte suivant : « Publication Judiciaire : condamnation de la société SFR pour contrefaçon du brevet EP 1 304 002 appartenant à la société Intellectual Ventures I LLC », lequel lien devra renvoyer vers une copie intégrale de la minute de l'arrêt à intervenir, et ce pendant une durée de deux mois sous astreinte de 50 000 euros par jour de retard à compter de la signification de l'arrêt à intervenir ;

- condamner la société SFR à payer à la société Intellectual Ventures I la somme de 800 000 euros sur le fondement de l'article 700 du code de procédure civile au titre de la procédure de première instance et la somme de 50 000 euros sur le même fondement au titre de la procédure d'appel ;

- Condamner la société SFR aux entiers dépens de première instance et d'appel, qui pourront être directement recouvrés par la SAS Bardehle Pagenberg, avocats, conformément à l'article 699 du code de procédure civile.

Aux termes de ses dernières conclusions notifiées par la voie électronique le 19 décembre 2024, la société SFR demande à la cour de :

à titre principal,

- confirmer le jugement en toutes ses dispositions,

A titre subsidiaire,

- juger nulles les revendications 1, 11 et 14 de la partie française du brevet EP 1 304 002 pour défaut de nouveauté et/ou d'activité inventive,

- confirmer le jugement par ajout ou substitution de motifs,

- ordonner l'inscription de la décision à intervenir sur le Registre National des Brevets dès qu'elle sera devenue définitive, sur réquisition du Greffe ou à la requête de la partie la plus diligente et aux frais de la société Intellectual Ventures I,

A titre très subsidiaire,

- rejeter l'action en contrefaçon des revendications 1, 11 et 14 de la partie française du brevet EP 1 304 002,

A titre plus subsidiaire,

- juger que la partie française du brevet EP 1 304 002 est inopposable pour fraude aux normes 3GPP TS 33.234 incorporant EAP-SIM et WIFI,

- en conséquence, juger irrecevable l'action de la société Intellectual Ventures I fondée sur un brevet inopposable,

A titre encore plus subsidiaire,

- juger irrecevables les demandes de la société Intellectual Ventures I relatives aux faits allégués de contrefaçon postérieurs à décembre 2016, date de suppression de la norme 3GPP TS 33.234,

- juger que le montant sollicité par la société Intellectual Ventures I, en cas de condamnation pour contrefaçon, à titre de provision, doit être ramené à plus juste proportion et ne peut dépasser la somme de 25 000 euros,

En tout état de cause

- débouter la société Intellectual Ventures I de ses entières demandes, fins et conclusions,

- condamner la société Intellectual Ventures I, pour l'instance d'appel, à verser à la société SFR la somme complémentaire de 50 000 euros en application de l'article 700 du code de procédure civile et aux entiers dépens.

La clôture de l'instruction a été prononcée par ordonnance du 16 janvier 2025.

MOTIFS :

Dans le dispositif de ses conclusions, la société Intellectual Ventures I demande à la cour de « déclarer irrecevables, l'ensemble des moyens, fins, conclusions et demandes de la société SFR, y compris ses demandes en nullité des revendications 1, 11 et 14, de la partie française du brevet européen EP 1 304 002 » mais n'explicite aucun moyen au soutien de la fin de non-recevoir invoquée. La fin de non-recevoir ne peut donc prospérer.

Sur la contrefaçon du brevet EP'002 :

Présentation du brevet :

Selon la description du brevet, l'invention concerne l'agencement d'un chiffrement de données dans des systèmes de télécommunication sans fil, en particulier dans des réseaux locaux sans fil (WLAN) [0001].

Le paragraphe [0002] enseigne que l'utilisation de différents réseaux locaux sans fil est devenue courante, lesquels incluent ceux basés sur la norme IEEE802.11 (WiFi) et qu'une attention particulière a été portée sur la sécurité des réseaux relevant de cette norme par la production d'une fonction à confidentialité équivalente au filaire, fonction appelée WEP (« Wired Equivalent Privacy »), qui décrit le chiffrement du trafic sur la couche MAC (« Media Access Control », servant d'interface entre la partie logicielle de la couche 2 dite « couche Liaison » et la couche physique du modèle en 7 couches OSI), entre un terminal et un point d'accès prenant en charge la norme IEEE802.11, la description soulignant que le chiffrement WEP est un algorithme symétrique, dans lequel la même clé de chiffrement est utilisée pour le chiffrement et le déchiffrement de données.

La description indique qu'un problème rencontré sur certains réseaux de télécommunication sans fil, comme les réseaux sans fil (WLAN) de norme IEEE802.11 est que les clés de chiffrement utilisées pour chiffrer le trafic doivent être stockées à l'avance dans le terminal et le point d'accès, que si le réseau ne présente pas la même clé que le terminal, alors les données entre le réseau et le terminal ne peuvent être chiffrées et qu'il est difficile d'ajouter différentes clés de chiffrement et ainsi d'assurer une transmission de données sécurisée aux terminaux mobiles itinérants dans différents réseaux [0003].

L'invention objet du brevet EP'002 vise à proposer un nouveau moyen en vue de créer et d'utiliser des clés de chiffrement au moyen d'un procédé, d'un système, d'un terminal et d'un point d'accès [0006].

L'invention est basée sur l'idée qu'une seconde clé de chiffrement est calculée dans le terminal et dans le réseau mobile public terrestre sur la base d'au moins une première clé de chiffrement selon le réseau mobile public terrestre. La seconde clé de chiffrement est transmise du réseau mobile au réseau local sans fil. Les données entre le terminal et le réseau sont chiffrées et déchiffrées dans le terminal et dans le réseau local sans fil utilisant la seconde clé de chiffrement [0007]. Cette solution présente l'avantage que, dans le réseau local sans fil, le réseau mobile et le module d'identification peuvent être utilisés pour le

calcul de la clé de chiffrement à utiliser, une clé de chiffrement pouvant être délivrée dynamiquement au réseau local sans fil pour des terminaux mobiles lorsque le terminal établit une connexion. Dans un tel cas, la clé de chiffrement ne doit pas être stockée dans le réseau local sans fil à l'avance [0008].

Les paragraphes [0012] et suivants présentent une description détaillée de l'invention qui peut être appliquée à un quelconque système de télécommunication sans fil comportant un réseau local sans fil et un réseau mobile public terrestre. Selon un mode de réalisation préféré de l'invention, le système comporte un terminal mobile (MT), un réseau local sans fil (WLAN) selon la norme IEEE802.11 et un réseau mobile public terrestre [0012]. Un opérateur de réseau local sans fil (WLAN), WISP (fournisseur de services Internet sans fil) offre des services basés sur IP sans fil de sorte que les terminaux mobiles (MT) sont capables d'être en itinérance dans les différents points d'accès sans fil généralement hautement chargés comme les hôtels, aéroports, etc. Le réseau local sans fil (WLAN) comporte des points d'accès au réseau local sans fil (AP) offrant une connexion sans fil pour une multitude de terminaux mobiles (MT). La norme IEEE802.11 détermine les protocoles de couche physique et de couche de contrôle d'accès au support (MAC) pour la transmission des données sur l'interface radio [0013].

Le brevet mentionne que le module d'identification de l'abonné (SIM) fourni par l'opérateur de réseau de système mondial de communication avec les mobiles (GSMNW) est connecté à l'équipement terminal (TE) du terminal mobile (MT). Il est généralement stocké sur une carte IC (circuit intégré). Ce module fonctionne comme un identificateur du terminal mobile (MT). Le module d'identification de l'abonné (SIM) comporte une clé secrète Ki, un algorithme A8 pour la formation d'une clé de chiffrement Kc et un algorithme A3 pour la formation d'une réponse d'authentification SRES (réponse signée) [0014].

Figure 1 du brevet :

Le brevet décrit une passerelle d'authentification au moyen d'un ou plusieurs triplets de réseau de communication constitués de la clé secrète Ki selon l'identification de l'abonné mobile international (ISMI) utilisant un algorithme A3, un nombre aléatoire RAND fourni par le centre d'authentification,

permettant, grâce à la clé secrète Ki utilisant l'algorithme A3, de générer une réponse d'authentification SRES et une première clé de chiffrement Kc [0025].

Les seconds moyens de calcul inclus dans le terminal mobile (MT), de préférence les moyens de commande, calculent une seconde clé de chiffrement K en utilisant une ou plusieurs premières clés de chiffrement Kc, selon un mode de réalisation préféré comme suit : K=HMAC (n*Kc,n*RAND/IMSI/MT-RAND) [0028].

La passerelle d'authentification informe le contrôleur d'accès public (PAC) que l'authentification est acceptée, le message comportant au moins la seconde clé de chiffrement K. Le contrôleur d'accès public (PAC) indique au terminal mobile (MT) que l'authentification est acceptée. L'authentification est ensuite exécutée et le terminal mobile (MT) et le contrôleur d'accès public (PAC) comportent une seconde clé de chiffrement K similaire qui peut être transmise aux moyens de chiffrement exécutant le chiffrement en vue de chiffrer le trafic [0033].

Après association du terminal mobile (MT) à un point d'accès au réseau local sans fil (AP), le terminal mobile calcule la seconde clé de chiffrement K. Si l'authentification est acceptable, le contrôleur d'accès public (PAC) reçoit la seconde clé de chiffrement K calculée par la passerelle d'authentification et de facturation GSM/GPRS (GAGW). Le contrôleur PAC transmet au point d'accès au réseau local sans fil (AP) la seconde clé de chiffrement K et indique l'authentification réussie, auquel cas, le point d'accès au réseau local sans fil (AP) associe la clé K à l'adresse de contrôle d'accès au support (MAC) du terminal mobile (MT). Le contrôleur d'accès public (PAC) indique de préférence au terminal mobile (MT) le succès de l'authentification (PAT - MT - AUTHANSWER - REST-OK) via le point d'accès au réseau local sans fil (AP) utilisant le même message [0038].

Après avoir reçu la seconde clé de chiffrement K, le point d'accès au réseau local sans fil (AP) transmet une demande au terminal mobile (MT) concernant l'utilisation de l'algorithme à confidentialité équivalente au filaire (WEP) en vue du chiffrement de données, ce dont le terminal mobile accuse réception, de sorte que le point de départ de chiffrement de données est correctement synchronisé. La

seconde clé de chiffrement K est alors appliquée dans la couche MAC du terminal mobile (MT) lequel chiffre les données à transmettre et déchiffre les données chiffrées reçues en utilisant l'algorithme à confidentialité équivalente au filaire (WEP) et la clé K. Le point d'accès au réseau local sans fil (AP) commence également à utiliser la clé de chiffrement K et l'algorithme de chiffrement à confidentialité équivalente au filaire (WEP) en vue de chiffrer des données adressées au terminal mobile (MT) et de déchiffrer les données reçues du terminal mobile (MT) [0039].

Sont opposées les revendications 1, 11 et 14 limitées du brevet EP'002 :

Revendication 1 :

Procédé destiné à agencer un chiffrement des données dans un système de télécommunication comportant au moins un terminal sans fil, un réseau local sans fil et un réseau mobile terrestre public, le procédé comportant les étapes consistant à fournir un identificateur pour le terminal et une clé secrète spécifique pour l'identificateur, la clé secrète étant également stockée dans le réseau mobile, transmettre (204) l'identificateur de terminal du terminal au réseau mobile, calculer (207) dans le réseau mobile plus d'une première clé de chiffrement selon le réseau mobile en utilisant la clé secrète spécifique pour l'identificateur et plus d'un code d'identification sélectionnés pour les premières clés de chiffrement, transmettre (210) plus d'un code d'identification au terminal, calculer (213) dans le terminal plus d'une première clé de chiffrement selon le réseau mobile en utilisant la clé secrète et plus d'un code d'identification,

caractérisé par les étapes consistant à exécuter une transmission de données entre le réseau mobile et le terminal par l'intermédiaire du réseau local sans fil,calculer (217 ; 221) une seconde clé de chiffrement dans le terminal et dans le réseau mobile en utilisant plus d'une première clef de chiffrement, transmettre (222) ladite seconde clé de chiffrement du réseau mobile au réseau local sans fil, chiffrer (311 ; 312), dans la couche MAC du terminal et du réseau local sans fil, les données transmises entre le terminal et le réseau local sans fil en utilisant ladite seconde clé de chiffrement.

Revendication 11 :

Terminal sans fil comportant un émetteur-récepteur en vue d'établir une connexion sans fil avec un point d'accès dans un réseau local sans fil et un module d'identification afin de calculer (213) plus d'une première clé de chiffrement selon un réseau mobile terrestre public en utilisant une clé secrète stockée dans le module d'identification et plus d'un code d'identification transmis par le réseau mobile,

caractérisé en ce que

le terminal comporte un second moyen de calcul en vue de calculer (217) une seconde clé de chiffrement en utilisant lesdites plus d'une première clé de chiffrement, et le terminal comporte un moyen de chiffrement dans la couche MAC en vue de chiffrer /déchiffrer (311) les données transmises entre le terminal et le point d'accès en utilisant ladite seconde clé de chiffrement.

Revendication 14 :

Point d'accès pour un réseau local sans fil comportant un moyen de chiffrement en vue de chiffrer / déchiffrer des données entre un terminal sans fil et le point d'accès,

caractérisé en ce que

le moyen de chiffrement est agencé dans la couche MAC en vue de chiffrer (312) les données à transmettre et en vue de déchiffrer les données reçues en utilisant une seconde clé de chiffrement spécifique au terminal calculée par un réseau mobile terrestre public et envoyée à partir du réseau mobile au réseau local sans fil, la seconde clé de chiffrement étant calculée au moyen de plus d'une première clé de chiffrement calculées dans le réseau mobile en utilisant une clé secrète spécifique au terminal et plus d'un code d'identification sélectionnés pour les premières clés de chiffrement.

Sur la personne du métier :

La personne du métier est celle du domaine technique où se pose le problème que l'invention, objet de ce brevet, se propose de résoudre. Elle possède les connaissances normales de la technique en cause et est capable à l'aide de ses seules connaissances professionnelles de concevoir la solution du problème que propose de résoudre l'invention.

Les parties s'opposent sur la détermination de la personne du métier : la société Intellectual Ventures I fait valoir qu'il s'agit d'un ingénieur spécialisé des technologies mises en 'uvre dans les réseaux locaux sans fil, doté de connaissances et compétences moyennes ou ordinaires, tandis que la société SFR soutient que la personne du métier doit s'entendre comme un ingénieur spécialisé dans la sécurité, notamment un spécialiste des technologies de communication mises en 'uvre dans les réseaux locaux et les réseaux de téléphonie mobile, ayant connaissance des normes ainsi que des travaux de normalisation.

Il est relevé que le domaine technique du brevet litigieux concerne à la fois les réseaux sans fil et les réseaux de téléphonie mobile, les normes Wifi (IEEE802.11) et GSM étant décrites dans le brevet comme relevant de l'état de la technique, les technologies de réseau local sans fil et de téléphonie mobile étant liées à la date de priorité du brevet.

Par conséquent, la personne du métier doit s'entendre comme un ingénieur spécialiste des technologies de communication mises en 'uvre dans les réseaux locaux sans fil et les réseaux de téléphonie mobile, ayant des connaissances générales dans ces domaines et maîtrisant les normes correspondantes.

Sur la demande reconventionnelle en nullité pour extension de l'objet au-delà de la demande :

La société SFR rappelle que constitue une généralisation intermédiaire le fait de revendiquer une caractéristique extraite d'un mode de réalisation particulier de l'invention, en l'isolant des autres caractéristiques de ce mode de réalisation et que, pour déterminer si l'extraction d'une caractéristique d'un mode de réalisation particulier est licite au regard de l'article 123(2) de la CBE, une double condition cumulative doit être remplie : la demande ne doit pas présenter la caractéristique comme apparentée ou inextricablement liée aux autres caractéristiques de ce mode de réalisation et la divulgation générale de la demande (hors du mode de réalisation particulier) doit justifier l'isolement de la caractéristique et sa généralisation.

La société SFR fait valoir que, dans sa requête en limitation, la société Intellectual Ventures I citait un unique passage de la description de la demande initiale comme support de cette modification qui est relatif à un mode particulier illustré par la figure 3, dans lequel le réseau local sans fil suit la norme

IEEE802.11 dans sa version en vigueur de 1999 ; que ce passage enseigne que le chiffrement dans la couche MAC a lieu en utilisant l'algorithme à confidentialité équivalente au filaire (WEP) ; que, cependant, la société Intellectual Ventures I n'a pas revendiqué l'utilisation de l'algorithme WEP dans sa limitation, alors que l'utilisation de cet algorithme est cohérente avec les revendications 4, 5, 10, 13 et 15 qui y font référence ; que l'extraction de la caractéristique selon laquelle le chiffrement a lieu dans la couche MAC, sans pour autant revendiquer l'algorithme WEP, constitue donc une généralisation intermédiaire d'un mode de réalisation particulier ; que la caractéristique MAC est inextricablement liée à la caractéristique WEP ; que le mode de réalisation particulier utilisé par la société Intellectual Ventures I pour soutenir sa limitation enseigne que le WEP est nécessaire au chiffrement sur la couche MAC ; que les connaissances générales de l'homme du métier, à savoir la norme IEEE802.11, confirment que le WEP est indispensable au chiffrement sur la couche MAC ; que le WEP est également obligatoire dans la seule alternative présentée par la demande ; qu'il s'en déduit que la possibilité d'appliquer le chiffrement dans la couche MAC sans utiliser le WEP est une information nouvelle au regard de la demande initiale, et à ce titre inadmissible ; que, par conséquent, les revendications telles que limitées constituent une généralisation intermédiaire étendant l'objet du brevet au-delà de la demande telle que déposée ; qu'à titre surabondant, le reste de la description de la demande ne pouvait permettre à la personne du métier de déduire que le chiffrement sur la couche MAC pouvait être généralisé au contexte plus général de l'invention ; qu'à cet égard, tous les passages de la demande relatifs à la couche MAC la décrivent soit directement en lien avec le WEP, soit dans le cadre de la norme IEEE802-11-1999, dans laquelle la seule méthode de chiffrement était le WEP ; qu'il est impossible à la personne du métier, à la date de priorité, de déduire directement et sans ambiguïté de la demande et de ses connaissances générales constituées par la norme IEEE802.11 dans sa version de 1999 que le chiffrement et le déchiffrement des données pouvait avoir lieu dans la couche MAC du terminal et du réseau sans fil, sans pour autant recourir à l'algorithme WEP ; que la société Intellectual Ventures I ne peut isoler la caractéristique « MAC » sans revendiquer en même temps des messages permettant la synchronisation du chiffrement ; qu'il est inopérant de savoir si la caractéristique « WEP » est ou non utile à la résolution

du problème technique, la société Intellectual Ventures I ne pouvant alléguer que le protocole WEP serait inutile selon le brevet pour assurer une transmission des données sécurisée entre le terminal et le WLAN alors qu'il est expressément enseigné dans le paragraphe cité par l'appelante comme support à la limitation que l'activation du WEP est nécessaire pour que le point de départ de chiffrement de données soit correctement synchronisé sur la couche MAC.

La société Ventures I réplique que si différents passages de la description du brevet mentionnent que les données transmises entre le terminal et le réseau local sans fil sont chiffrées dans la couche MAC et que le chiffrement de données est réalisé au moyen d'un algorithme WEP, ces deux caractéristiques ne sont pas inextricablement liées sur le plan technique, l'homme du métier n'ayant aucune raison de les comprendre comme telles à la lecture de l'ensemble de la demande telle que déposée ; que le mode de réalisation spécifique illustré par la figure 3 correspond au cas particulier où le réseau local sans fil est un réseau selon la norme IEEE802.11 (WiFi) dans laquelle le chiffrement des données dans la couche MAC peut utiliser l'algorithme WEP optionnel prévu par cette norme ; que la demande telle que déposée indique expressément à la personne du métier que l'invention n'est pas limitée à ce cas particulier, pouvant être appliquée dans tout système de télécommunications sans fil comprenant un réseau local sans fil et un réseau mobile public terrestre ; que si les normes WiFi et Hiperlan prévoient toutes deux le chiffrement des données dans la couche MAC, la norme Hiperlan a en revanche recours à son propre système de chiffrement, qui n'est pas l'algorithme WEP ; que, par conséquent, la personne du métier comprend directement et sans ambiguïté du contenu global de la demande telle que déposée que lorsque le réseau local sans fil est conforme à la norme IEEE802.11(WiFi), le chiffrement des données dans la couche MAC peut utiliser l'algorithme WEP optionnel prévu par cette norme, mais que tel n'est pas nécessairement le cas, en particulier lorsque le réseau local sans fil relève d'une autre norme, comme par exemple un réseau basé sur la norme Hiperlan ; que, de plus, le choix d'une méthode particulière de chiffrement des données plutôt qu'une autre dans le réseau local sans fil ne participe aucunement à la résolution du problème technique posé ; que c'est le chiffrement des données dans la couche MAC indépendamment de la méthode de chiffrement des données utilisée qui permet d'assurer une

transmission de données sécurisée entre le terminal et le point d'accès au réseau local sans fil WLAN ; qu'il n'était donc nullement nécessaire, lorsque la caractéristique relative au chiffrement des données dans la couche MAC a été introduite dans les revendications 1, 11 et 14 pour les limiter, d'y introduire également la caractéristique tenant à l'utilisation d'un algorithme de chiffrement WEP pour chiffrer les données, de sorte que la limitation des revendications 1, 11 et 14 du brevet EP'002 acceptée par le directeur général de l'INPI le 8 janvier 2020 n'a pas étendu l'objet de ces revendications au-delà du contenu de la demande telle que déposée.

Réponse de la cour :

En vertu de l'article L.614-12 du code de la propriété intellectuelle, la nullité du brevet européen est prononcée en ce qui concerne la France par décision de justice pour l'un quelconque des motifs visés à l'article 138, paragraphe 1, de la Convention de Munich.

Conformément à l'article 138 c) de la Convention sur la délivrance de brevets européens (CBE), sous réserve de l'article 139, le brevet européen ne peut être déclaré nul, avec effet pour un Etat contractant, que si (') l'objet du brevet européen s'étend au-delà du contenu de la demande telle qu'elle a été déposée ou, lorsque le brevet a été délivré sur la base d'une demande divisionnaire ou d'une nouvelle demande déposée en vertu de l'article 61, si l'objet du brevet s'étend au-delà du contenu de la demande antérieure telle qu'elle a été déposée.

Enfin, l'article 123 de la CBE dispose que la demande de brevet européen ou le brevet européen ne peut être modifié de manière que son objet s'étende au-delà du contenu de la demande telle qu'elle a été déposée.

La pratique dite de la « généralisation intermédiaire » qui consiste à extraire une caractéristique isolée de son contexte spécifique, n'est justifiée qu'en l'absence de toute relation fonctionnelle ou structurelle clairement reconnaissable entre les caractéristiques de la combinaison spécifique ou si la caractéristique extraite n'est pas inextricablement liée à ces caractéristiques. En d'autres termes, une généralisation intermédiaire n'est autorisée en vertu de l'article 123(2) de la CBE que si la personne du métier reconnaît

sans aucun doute, d'après la demande telle qu'elle a été déposée, que les caractéristiques tirées d'un mode de réalisation détaillé ne sont pas étroitement liées aux autres caractéristiques de ce mode de réalisation et qu'elles s'appliquent directement et sans ambiguïté au contexte plus général (V. chambre recours OEB, décision T 2489/13 du 18 avril 2018).

La généralisation intermédiaire, pour être admissible, doit résulter clairement d'informations déductibles directement et sans ambiguïté par la personne du métier de la demande telle que déposée.

Au cas d'espèce, la requête en limitation était fondée sur un passage de la demande initiale.

A cet égard, dans sa requête du 15 novembre 2019 au directeur général de l'INPI, le mandataire de la société Intellectual Ventures 1 écrit : « La revendication 1 relative à un procédé destiné à agencer un chiffrement des données dans un système de télécommunication, a été modifiée en apportant les limitations suivantes (') Les données transmises entre le terminal et le réseau local sans fil sont chiffrées dans la couche MAC du terminal et du réseau local sans fil. Ceci se fonde sur la description telle que déposée : voir page 11, lignes 3 à 12 de la demande initiale (PCT/FI01/00617) telle que publiée (WO 02/03730) » (pièce Intellectual Ventures I n°51).

Ce passage (page 11, lignes 3 à 12 de la demande PCT) est rédigé comme suit, selon la traduction non contestée produite en langue française par la société Intellectual Ventures I (pièce n°5 bis) :

« Après cela, la seconde clé de chiffrement K est appliquée dans la couche MAC du terminal mobile (MT), et le terminal mobile (MT) chiffre les données à transmettre et déchiffre les données chiffrées reçues 311 (chiffrement des données avec K et WEP) en utilisant l'algorithme à confidentialité équivalente au filaire (WEP) et la clé K. Le point d'accès au réseau local sans fil (AP) commence également à utiliser 312 (chiffrement des données avec K et WEP), la clé de chiffrement K et l'algorithme de chiffrement à confidentialité équivalente au filaire (WEP) en vue de chiffrer des données adressées au terminal mobile (MT) et de déchiffrer des données reçues du terminal mobile (MT). Le point d'accès au réseau local sans fil (AP) vérifie les adresses de contrôle d'accès au support (MAC) du terminal mobile (MT) des données reçues et effectue le déchiffrement des données en provenance de l'adresse de contrôle

d'accès au support (MAC) et corrélativement déchiffre les données de terminal mobile (MT) adressées à l'adresse de contrôle d'accès au support (MAC). Dans ce cas, la clé de chiffrement K est rapidement initiée et le chiffrement de données peut commencer ».

La demande PCT décrit, dans le même paragraphe, l'étape antérieure :

« Après avoir reçu la seconde clé de chiffrement K, le point d'accès au réseau local sans fil (AP) transmet 309 (Put-WEP-on (activation de WEP)) une demande au terminal mobile (MT) concernant l'utilisation de l'algorithme à confidentialité équivalente au filaire (WEP) en vue du chiffrement de données. Le terminal mobile (MT) accuse réception 310 (Put-WEP-on-ack (accusé de réception d'activation de WEP)) de la demande, de sorte que le point de départ de chiffrement de données est correctement synchronisé.

La personne du métier déduit donc sans ambiguïté de la lecture de la demande que la synchronisation et le chiffrement subséquent de données dans la couche MAC reposent sur l'utilisation de l'algorithme WEP, ainsi que le conforte d'ailleurs la figure 3 qui montre que cet algorithme est utilisé pour le chiffrement de données :

Elle retiendra en conséquence que la caractéristique relative à la mise en 'uvre du chiffrement dans la couche MAC est inextricablement liée à l'utilisation de l'algorithme à confidentialité équivalente au filaire (WEP), dans le cadre du mode de réalisation particulier de l'invention utilisant la norme IEEE802.11 (WiFi) qui ne connait, à la date de priorité, que le protocole WEP.

Si la société Intellectual Ventures I soutient que l'invention s'applique à d'autres réseaux sans fil utilisant d'autres normes, comme la norme HIPERLAN, comprenant un propre mécanisme de chiffrement ne reposant pas sur l'algorithme WEP, de sorte que la personne du métier comprendra, au regard de ses connaissances générales des différentes normes, que le chiffrement s'opérera selon un algorithme compatible avec la norme du réseau local concerné, il est cependant relevé que la demande ne décrit que la norme WiFi, de sorte que la personne du métier ne peut envisager que le brevet envisage des modes de réalisation possibles excluant l'utilisation de l'algorithme WEP pour le chiffrement des données dans

la couche MAP après synchronisation, le tribunal soulignant pertinemment à cet égard que les revendications non opposées 4, 5, 10, 13 et 15 du brevet EP'002 font expressément référence au protocole WEP de la norme WiFi, étant ajouté que le brevet enseigne que l'activation de l'algorithme WEP est nécessaire pour que le point de départ du chiffrement de données soit correctement synchronisé sur la couche MAC pour permettre une transmission sécurisée, participant ainsi à la résolution du problème technique posé par l'invention.

Par conséquent, l'extraction de la caractéristique isolée selon laquelle le chiffrement a lieu dans la couche MAC du terminal et du réseau local sans fil, hors revendication de l'utilisation de l'algorithme WEP, alors que, pour la personne du métier, ces caractéristiques sont étroitement liées et que la seule caractéristique revendiquée ne s'applique pas directement et sans ambiguïté au contexte plus général de l'invention qui décrit le recours au protocole WEP, est donc une généralisation intermédiaire interdite constitutive d'une demande de protection s'étendant au-delà du contenu de la demande.

Le jugement sera donc confirmé en ce qu'il a annulé les revendications opposées 1, 11 et 14 limitées du brevet EP'002 et rejeté les demandes formées par la société Intellectual Ventures I au titre de la contrefaçon.

Sur la demande reconventionnelle en dénigrement :

La société SFR fait valoir qu'est fautive la dénonciation faite à la clientèle d'une action de justice qui n'a pas donné lieu à une décision ; que la société Intellectual Ventures I a publié un encart sur son propre site Internet, annonçant qu'elle avait intenté une action en contrefaçon contre la société SFR devant le tribunal de grande instance de Paris, lequel a été publié le jour même de la signification de l'assignation, soit le 15 novembre 2016 ; qu'aucune décision n'ayant été rendue à cette date, cette annonce prématurée constitue un acte de dénigrement portant atteinte à l'image et la réputation de la société SFR.

La société Intellectual Ventures I réplique que la publication d'un communiqué de trois lignes sur son site Internet en langue anglaise informant brièvement et sobrement ses investisseurs de l'engagement d'une action en contrefaçon contre la société SFR sans préjuger de l'issue du litige n'est pas fautive ; que

ce communiqué, purement informatif, ne visait pas la clientèle de la société SFR ni le public français, et ne présente aucun caractère dénigrant ni excessif ou désobligeant ; que le dénigrement invoqué n'est pas caractérisé.

Réponse de la cour :

En vertu de l'article 1240 du code civil, tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer.

Même en l'absence d'une situation de concurrence directe et effective entre les personnes concernées, la divulgation, par l'une, d'une information de nature à jeter le discrédit sur un produit commercialisé par l'autre constitue un acte de dénigrement, à moins que l'information en cause ne se rapporte à un sujet d'intérêt général et repose sur une base factuelle suffisante, et sous réserve qu'elle soit exprimée avec une certaine mesure.

Au cas d'espèce, il résulte d'un procès-verbal de constat d'huissier de justice du 3 février 2017 (pièce SFR n°4.4) que la société Intellectual Ventures I a mis en ligne une publication accessible à l'adresse http://www.intellectualventures.com/news/legal-updates/intellectual-venturesfiles-patent-infringement-complaint-against-sfr/ :

Cette publication, accessible par le public français, y compris la clientèle de la société SFR, qui divulgue une action en contrefaçon, est dépourvue de base factuelle suffisante en ce qu'elle ne repose que sur le seul acte de poursuite engagé par la société Intellectual Ventures I et ne se rapporte pas à un sujet d'intérêt général.

Par conséquent, la publication incriminée constitue un acte de dénigrement fautif portant atteinte à l'image de la société SFR.

Le jugement sera donc confirmé en ce qu'il a condamné la société Intellectual Ventures I à payer à la société SFR la somme de 50 000 euros à titre de dommages-intérêts en réparation du préjudice subi.

Sur les demandes accessoires :

Le jugement sera confirmé du chef des dépens et de l'article 700 du code de procédure civile.

Partie succombante, la société Intellectual Ventures I sera condamnée aux dépens d'appel et au paiement d'une indemnité de procédure au titre des frais irrépétibles exposés par la société SFR.

PAR CES MOTIFS

La Cour,

CONFIRME en toutes ses dispositions le jugement dont appel,

Y AJOUTANT,

CONDAMNE la société Intellectual Ventures I aux dépens d'appel,

EN APPLICATION de l'article 700 du code de procédure civile, CONDAMNE la société Intellectual Ventures I à payer à la société SFR la somme de 50 000 euros et REJETTE la demande formée par la société Intellectual Ventures I.

La Greffière La Présidente

Copyright 2025 - Dalloz - Tous droits réservés.