

SOMMAIRE

PARIS - NANTES
MONTPELLIER - PERPIGNAN

Bureaux intégrés

AIX-EN-PROVENCE - BORDEAUX
CAEN - CLERMONT-FERRAND
LE HAVRE - LYON
MARSEILLE - METZ - ROUEN
SAINT-ETIENNE

Réseau SIMON Avocats

ALGÉRIE - ARGENTINE
ARMÉNIE - AZERBAÏDJAN
BAHAMAS - BAHREÏN
BANGLADESH - BELGIQUE
BIRMANIE - BOLIVIE - BRÉSIL
BULGARIE - CAMBODGE
CAMEROUN - CHILI - CHINE
CHYPRE - COLOMBIE
CORÉE DU SUD - COSTA RICA
CÔTE D'IVOIRE - ÉGYPTÉ
EL SALVADOR
ÉMIRATS ARABES UNIS
ESTONIE - ÉTATS-UNIS
GUATEMALA - HONDURAS
HONGRIE - ÎLE MAURICE
ÎLES VIERGES BRITANNIQUES
INDE - INDONÉSIE - IRAN
ITALIE - KAZAKHSTAN
KOWEÏT - LUXEMBOURG
MADAGASCAR - MALTE
MAROC - MEXIQUE - NICARAGUA
OMAN - PANAMA - PARAGUAY
PÉROU - PORTUGAL - QATAR
RD CONGO - RÉPUBLIQUE
DOMINICAINE - SENEGAL
SINGAPOUR - THAÏLANDE
TUNISIE - URUGUAY
VENEZUELA - VIETNAM
ZIMBABWE

Conventions transnationales

www.simonassociés.com
www.lettredunumerique.com



<p>DATA / DONNÉES PERSONNELLES</p> <p>La reconnaissance faciale : un enjeu de société pour le citoyen européen Commission Européenne, 19 février 2020, Livre blanc consacrée à l'intelligence artificielle</p> <p>Une discrète jeune pousse collecte 3 milliards de photos sur les réseaux sociaux et offre un service de reconnaissance faciale à la police américaine Article du New York Times du 18 janvier 2020</p> <p>La CNIL cible les compteurs communicants Linky et met en demeure les sociétés EDF et ENGIE Délibération n°2019-035 du 31 décembre 2019 mettant en demeure la société ÉLECTRICITÉ DE FRANCE (EDF) ; Délibération n°2019-036 du 31 décembre 2019 mettant en demeure la société ENGIE</p>	<p>p. 2</p> <p>p. 4</p> <p>p. 5</p>
<p>PROPRIÉTÉ INTELLECTUELLE</p> <p>Dépôt d'une marque de mauvaise foi et intention d'usage CJUE, 29 janvier 2020, aff. C.371-18</p> <p>Blocage de sites proposant des produits contrefaisants Trib. Jud. Paris, Ord. réf., 8 janvier 2020, RG n°19/58624</p> <p>Recours administratif à l'encontre d'un brevet d'invention : publication de l'ordonnance n°2020-116 Ordonnance n°2020-116 du 12 février 2020 portant création d'un droit d'opposition aux brevets d'invention</p>	<p>p. 7</p> <p>p. 8</p> <p>p. 9</p>
<p>INTERNATIONAL</p> <p>La loi antitrust en Chine – le projet de modification en vue d'une régulation renforcée des BATX Actualité législative</p>	<p>p. 10</p>
<p>STARTUP & LEGALTECHS / TENDANCES</p> <p>Déploiement national de « Signaux Faibles » : l'IA au service de la prévention des difficultés Actualité</p> <p>Création du comité pilote d'éthique du numérique en France Une avancée significative pour la prise en considération des enjeux liés à l'intelligence artificielle</p>	<p>p. 11</p> <p>p. 12</p>
<p>ACTUALITÉ NUMÉRIQUE</p>	<p>p. 13</p>

DATA / DONNÉES PERSONNELLES

La reconnaissance faciale : un enjeu de société pour le citoyen européen

Commission Européenne, 19 février 2020, Livre blanc consacrée à l'intelligence artificielle

Ce qu'il faut retenir :

La CNIL s'est emparée du sujet considérant le 15 novembre 2019 que la reconnaissance faciale est de plus en plus présente dans le débat public aux niveaux national, européen et mondial. Cette technologie soulève des questions inédites touchant à des choix de société. La Commission Européenne l'a bien compris en publiant son livre blanc consacré à l'intelligence artificielle le 19 février 2020 dans lequel elle considère que cette technologie représente un usage à risque pour nos droits fondamentaux et qu'il est désormais temps de statuer sur une réglementation protectrice de la vie privée du citoyen dans le prolongement du RGPD.

Pour approfondir :

« En 2054, il est difficile de se déplacer incognito car toutes les personnes sont soumises à des scanners rétinien pour la personnalisation des messages publicitaires audios notamment. Pour échapper à toute identification, John Anderton va se faire transplanter de nouveaux yeux chez un chirurgien clandestin ». C'est ainsi que Philip K. Dick, auteur de romans et de nouvelles d'anticipation, a imaginé comment son héros pouvait échapper à cette reconnaissance rétinienne par les autorités qui le recherchent (*Nouvelle « Minority Report » de Philippe K. Dick*).

En écrivant cette nouvelle d'anticipation, Philip K. Dick était loin de s'imaginer que la reconnaissance biométrique ferait l'objet d'un débat relatif aux choix d'organisations sociales dans lesquelles nos sociétés entendent évoluer, notamment en Europe.

Certes, la reconnaissance rétinienne n'est aujourd'hui pas au cœur du débat mais ce dernier concerne plus encore à savoir le visage dans son ensemble. On parle désormais de la reconnaissance faciale.

Les technologies de reconnaissance faciale vont-elles un jour être utilisées pour identifier les citoyens en temps réel ? Ces méthodes, qui sont déjà une réalité dans certains pays, sont à ce jour interdites en France

comme dans l'ensemble de l'Union européenne dans la mesure où la loi impose de recueillir le consentement explicite de chaque individu soumis à un algorithme de reconnaissance faciale.

• La reconnaissance faciale selon la CNIL

L'une des premières tentatives de reconnaissance de visage est faite par Takeo Kanade en 1973 lors de sa thèse de doctorat à l'Université de Kyoto. Takeo Kanade est aujourd'hui un informaticien japonais spécialiste parmi les plus reconnus en **vision par ordinateur** et détenant une vingtaine de **brevets** dans ce domaine

Plus de 45 ans plus tard, **la CNIL nous alerte en concentrant son analyse sur cette technologie :**

« Cette technologie n'en est désormais plus à ses balbutiements. Les enjeux de protection des données et les risques d'atteintes aux libertés individuelles que de tels dispositifs sont susceptibles d'induire sont considérables, dont notamment la liberté d'aller et venir anonymement. Tout projet d'y recourir devra à tout le moins faire l'objet d'une analyse d'impact relative à la protection des données (AIPD). »

Et l'autorité de contrôle présente la reconnaissance faciale comme une technologie qui permet à partir des traits de visage :

- **D'authentifier une personne :** c'est-à-dire, de vérifier qu'une personne est bien celle qu'elle prétend être (dans le cadre d'un contrôle d'accès) ;

Ou

- **D'identifier une personne :** c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

En pratique, la reconnaissance peut être réalisée à partir d'images fixes (photos) ou animées (enregistrements vidéo) et se déroule en deux phases :

1. A partir de l'image, un modèle ou « gabarit » qui représente, d'un point de vue informatique, les caractéristiques de ce visage est réalisé. Les données extraites pour constituer ce gabarit sont des données biométriques au sens du RGPD (article 4-14) ;

2. La phase de reconnaissance est ensuite réalisée par la comparaison de ces « gabarits » préalablement réalisés avec les modèles calculés en direct sur des visages présents sur l'image candidate (*ibidem*).

La technique permet de comparer deux modèles biométriques, généralement supposés appartenir à la même personne. Ces deux modèles sont comparés aux fins de déterminer si la personne qui figure sur les deux images est bien la même. Cette procédure est, par exemple, utilisée aux portiques de contrôle automatisés des passeports destinés aux vérifications aux frontières dans les aéroports.

La CNIL, dans sa contribution « *Reconnaissance faciale : pour un débat à la hauteur des enjeux* », rendue publique, le 15 novembre dernier, rappelait qu'il était important de « *bâtir un véritable modèle européen face aux usages parfois débridés ou déraisonnables de la reconnaissance faciale à travers le monde* » (*Reconnaissance faciale : pour un débat à la hauteur des enjeux*, CNIL, 15 novembre 2019).

- **La Commission Européenne souhaite ouvrir un vaste débat sur l'intelligence artificielle**

Le 19 février 2020, soit 3 mois après la CNIL en France, la Commission Européenne a inséré la question de la reconnaissance faciale dans un corpus plus vaste : celui de l'intelligence artificielle.

La Commission précise que le recours à la reconnaissance faciale aux fins d'une identification biométrique à distance est généralement interdit et n'est autorisé que dans des cas exceptionnels, dûment justifiés et proportionnés, sous réserve des garanties suffisantes et dans le respect du droit de l'UE ou du droit national.

Les données biométriques sont définies comme étant « *les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données*

dactyloscopiques [empreintes digitales] » (Article 3, paragraphe 13, de la directive en matière de protection des données dans le domaine répressif ; article 4, paragraphe 14, du RGPD ; article 3, paragraphe 18, du règlement (UE) 2018/1725).

Toutefois, comme le souligne la Commission Européenne et ce malgré ce corpus juridique relativement protecteur, la collecte et l'utilisation de données biométriques à des fins d'identification à distance, au moyen, par exemple, du déploiement de la reconnaissance faciale dans des lieux publics, « *comportent des risques particuliers en termes de droits fondamentaux* ». L'utilisation de systèmes d'IA pour l'identification biométrique à distance a des incidences sur les droits fondamentaux qui peuvent considérablement varier selon sa finalité, son contexte et sa portée.

Face à ce constat, la Commission :

« lancera un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que sur les garanties communes à mettre en place » (Commission Européenne, 19 février 2020, Livre blanc consacrée à l'intelligence artificielle).

Tout comme la CNIL 3 mois plus tôt, et consciente que le mouvement est lancé, la Commission Européenne invite les Etats membres de l'UE à s'emparer de ce sujet de société pour établir une législation sur la reconnaissance faciale qui puisse s'inscrire dans la continuité du RGPD.

A suivre attentivement.

A rapprocher : Définition « Reconnaissance faciale », CNIL ; Reconnaissance faciale : pour un débat à la hauteur des enjeux, CNIL, 15 novembre 2019 ; Façonner l'avenir numérique de l'Europe : la Commission présente des stratégies en matière de données d'intelligence artificielle, Commission Européenne, 19 février 2020

Une discrète jeune pousse collecte 3 milliards de photos sur les réseaux sociaux et offre un service de reconnaissance faciale à la police américaine
Article du New York Times du 18 janvier 2020

Ce qu'il faut retenir :

Une jeune pousse américaine revendique 3 milliards de photos d'internautes qu'elle a récupérées de FACEBOOK, YOUTUBE, VENMO et autres sites web, à leur insu, pour créer un service de reconnaissance faciale qu'elle commercialise auprès des autorités de la police locales en Floride au F.B.I. et au Department of Homeland Security.

Pour approfondir :

- **Les réseaux sociaux au service de la police malgré eux**

Clearview AI a conçu une application de reconnaissance faciale révolutionnaire. Après avoir pris une photo d'une personne qui est téléchargée, cette photo est comparée à des photos publiques de cette même personne issues des réseaux sociaux, ainsi que des liens vers l'endroit où ces photos sont apparues.

Ainsi le visage d'une personne captée par une caméra de surveillance lors d'une manifestation peut être identifiée grâce aux informations présente dans la base données Clearview AI.

Pour résumer la situation, le New York Times écrit :

« Avec Clearview, on peut utiliser des photos qui ne sont pas parfaites ; la personne peut porter un masque ou des lunettes, et cela fonctionne même avec les images partielles d'un visage ».

Les services de police ont accès à des outils de reconnaissance faciale depuis près de 20 ans, mais ils se sont historiquement limités à rechercher des images fournies par le gouvernement, telles que des photos d'identité et des photos de permis de conduire. Ces dernières années, les algorithmes de reconnaissance faciale ont amélioré leur précision, et des entreprises proposent des produits qui peuvent créer un programme de reconnaissance faciale pour n'importe quelle base de données d'images.

Le New York Times révèle dans son enquête qu'en février 2017, la police de l'État de l'Indiana a commencé à expérimenter Clearview IA. « *Ils ont résolu un cas en 20 minutes* » par l'utilisation de l'application. « *Deux*

hommes s'étaient disputés dans un parc, et cela s'est terminé quand l'un a tiré sur l'autre le blessant gravement à l'abdomen ». Un passant a enregistré le crime sur un téléphone, de sorte que la police avait un visage du tireur qu'elle a pu comparer avec la base de données de Clearview.

Ils ont immédiatement obtenu une « reconnaissance » de son visage. Le suspect est apparu dans une vidéo que quelqu'un avait publiée sur les réseaux sociaux, et son nom était inclus dans une légende sur la vidéo. « *Il n'avait pas de permis de conduire et n'avait pas été arrêté à l'âge adulte, il n'était donc pas dans les bases de données gouvernementales* » a déclaré le capitaine de la police de l'État de l'Indiana à l'époque.

L'homme, qui a été arrêté et inculpé, n'aurait probablement pas été identifié sans la possibilité de rechercher son visage sur les réseaux sociaux.

- **Les Géants du net veulent protéger leur image**

Alors les réseaux sociaux sont-ils complices de Clearview IA sachant que Facebook offre elle-même un service de reconnaissance faciale à destination de ses utilisateurs ?

La réponse est non ! Tout au contraire.

Cette révélation a conduit Facebook et Google à mettre en demeure, 2 jours après les révélations du New York Times, Clearview IA à cesser toute collecte d'images sur leurs sites.

Pour fonder cette injonction, Google, qui détient YouTube, a soulevé ses conditions d'utilisation qui interdisent de :

« recueillir ou utiliser toute information permettant d'identifier une personne (par exemple, collecter les noms d'utilisateurs), sauf si expressément autorisé par la ou les personnes concernées ou par les dispositions de la section 3 ci-dessus » (Conditions d'utilisation de YouTube du 22 juillet 2019).

Ce reproche sur l'absence de consentement de la part des géants du net est paradoxal puisqu'en général ce sont à ces entreprises qu'il est fait reproche de ne pas respecter le consentement des internautes.

Facebook comme Google veulent démontrer qu'elles sont désormais vigilantes sur l'utilisation des données personnelles de leurs utilisateurs qui peuvent être exploitées par des tiers.

Il faut se rappeler que le 24 juillet 2019, la *Federal Trade Commission* (FTC) (l'autorité de la concurrence américaine) a condamné Facebook à verser 5 milliards de dollars d'amende aux Etats-Unis pour avoir mal protégé les données de ses utilisateurs.

Cette condamnation a été prononcée dans le prolongement des révélations et des controverses liées au scandale *Cambridge Analytica*. Cette entreprise britannique, prestataire de la campagne présidentielle de Donald Trump, avait récolté les informations de 87 millions d'utilisateurs de Facebook (dont des Américains) sans leur consentement, qui lui ont ensuite servi à faire du marketing électoral.

Quelques semaines plus tard, en septembre 2019, et toujours dans cet esprit de transparence affiché, les utilisateurs de Facebook pouvaient choisir d'activer la reconnaissance faciale s'ils veulent s'en servir pour être identifiés sur les photos postées sur le réseau social. Dans le cas contraire, la fonctionnalité restera désactivée par défaut.

Ce changement est intervenu alors que le groupe subit une pression des institutions pour mieux protéger la vie privée de ses usagers.

- **Une atteinte aux libertés individuelles**

Cette collecte de photos acquises sans le consentement des intéressés et dénoncée par les réseaux sociaux eux-mêmes a de quoi inquiéter nos sociétés.

L'entreprise Clearview IA affirme que son système trouve une correspondance dans 75 % des cas, mais ne donne pas le taux de « faux positifs » c'est-à-dire le nombre de personnes identifiées par erreur. Or, plus la base de données est importante, plus les chances d'y trouver plusieurs personnes dotées d'une forte ressemblance augmentent, *a fortiori* lorsque l'image utilisée pour la recherche est de mauvaise qualité. Plusieurs études ont également montré que les logiciels de reconnaissance faciale, s'ils sont en progrès constant, sont loin d'être précis à 100 %.

Toujours d'après l'enquête du New York Times, les policiers et les investisseurs de Clearview IA prévoient que son application sera finalement disponible au public.

Le fondateur de l'entreprise a déclaré qu'il était réticent à cette éventualité craignant une mauvaise utilisation.

Même si Clearview IA ne met pas son application à la disposition du public, maintenant que le tabou est brisé, une entreprise tierce pourrait le faire. Rechercher quelqu'un de face pourrait devenir aussi simple que de rechercher un nom sur Google. Une personne marchant dans la rue serait immédiatement identifiable et son adresse personnelle ne serait qu'à quelques clics. Cela annoncerait la fin de l'anonymat public.

Face à cette évolution inéluctable, il est temps que les gouvernements travaillent sur ce sujet, ultrasensible de la reconnaissance faciale au regard de l'ampleur de ses enjeux en matière de libertés publiques.

A rapprocher : *The Secretive Company That Might End Privacy as We Know It* (The New York Times, Jan. 18, 2020) ; Conditions d'utilisation Youtube ; La reconnaissance faciale, des promesses et des risques (Le Monde, 20 fév. 2020)

La CNIL cible les compteurs communicants Linky et met en demeure les sociétés EDF et ENGIE
Délibération n°2019-035 du 31 décembre 2019 mettant en demeure la société ÉLECTRICITÉ DE FRANCE (EDF) ; Délibération n°2019-036 du 31 décembre 2019 mettant en demeure la société ENGIE

Ce qu'il faut retenir :

Les mises en demeure de la CNIL concernant les compteurs communicants Linky constituent un opportun rappel aux règles entourant le consentement comme base légale d'un traitement de données à caractère personnel mais également un rappel à la nécessité de déterminer des durées de conservation des données proportionnées aux finalités poursuivies.

Pour approfondir :

Par deux délibérations en date du 31 décembre 2019 et rendues publiques le 11 février 2020, la Commission Nationale de l'Informatique et des Libertés (CNIL) met en demeure les sociétés ENGIE et ELECTRICITE DE FRANCE (EDF) pour deux manquements constatés au règlement (UE) 2016/679 du Parlement et du Conseil du 27 avril 2016 (RGPD) et relatifs aux compteurs communicants LINKY.

Ces compteurs électriques permettent le relevé à distance d'informations de consommation d'électricité plus précises que les compteurs électriques traditionnels, telles que les données de consommation quotidiennes et à l'heure ou à la demi-heure.

Ayant vocation à permettre aux consommateurs d'acquérir une meilleure maîtrise de leur consommation d'électricité, ces compteurs sont déployés depuis 2015 et la société ENEDIS prévoit d'ici 2021 de procéder à l'installation de 35 millions de compteurs communicants.

Alors qu'une action collective visant à réclamer le droit de refuser leur installation a été déposée le 24 février 2020 et qu'une pétition en ce sens regroupe plus de 13.000 signataires, la CNIL met en exergue et rend publiques les défaillances des sociétés ENGIE et EDF.

Aux termes de ces délibérations, l'autorité de contrôle relève en effet des manquements à l'obligation de disposer d'une base légale pour les traitements mis en œuvre et à l'obligation de définir une durée de conservation proportionnée à la finalité des traitements.

La CNIL pointe en effet les nombreuses défaillances entourant le recueil du consentement des consommateurs des compteurs. Il est en effet relevé que l'utilisateur, pour consentir au suivi de sa consommation détaillée d'électricité, se voit proposer une seule case à cocher pour deux (ENGIE) à trois (EDF) opérations de traitement distinctes.

Or, l'autorité de contrôle souligne que « *selon la granularité de la donnée (données journalières ou données de consommation fines à l'heure ou à la demi-heure) et le rôle du responsable de traitement dans la chaîne énergétique (gestionnaire de réseau de distribution ou fournisseur), la collecte des données de consommation peut nécessiter de recueillir le consentement du client* ».

Il est opportun de souligner que parmi les six bases légales citées par l'article 6 du RGPD, le consentement, première énumérée, apparaît comme un fondement naturel mais délicat en ce qu'il s'associe à la fois à de nombreuses conditions de validité mais également à un droit de retrait de la personne concernée.

En premier lieu, rappelons que le consentement, lorsque celui-ci fonde légalement un traitement de données à caractère personnel, doit être libre, spécifique, éclairé et univoque. La CNIL reproche ici aux deux sociétés de recueillir un consentement non spécifique et non suffisamment éclairé s'agissant des données de consommation à l'heure ou à la demi-heure notamment.

D'une part, un consentement spécifique est caractérisé lorsque la personne concernée est en mesure de donner son consentement de façon indépendante pour chaque finalité poursuivie.

D'autre part, un consentement éclairé est caractérisé lorsque la personne concernée est informée de la portée du traitement et notamment des finalités poursuivies ou encore des catégories de données collectées et utilisées. En effet, le recueil du consentement des personnes concernées doit aller de pair avec leur information sur l'étendue du traitement opéré, car ladite information conditionne le caractère libre et éclairé du consentement.

En l'absence de tels éléments, la personne concernée risque inmanquablement d'être trompée sur la portée de son engagement.

Enfin, rappelons que le responsable de traitement doit mettre en œuvre des mesures permettant le retrait du consentement par la personne concernée dans les mêmes conditions que son octroi.

La Commission pointe également les défaillances des sociétés dans la détermination de durées de conservations proportionnées aux finalités poursuivies. En l'espèce, les deux sociétés se voient reprocher la fixation de durées de conservation excessives et non nécessaires aux finalités poursuivies.

En effet, conformément à l'article 5 du RGPD, les données à caractère personnel doivent être conservées « *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

Les durées de conservation des données sont sujettes à de nombreuses interrogations des responsables de traitement à qui revient l'obligation de les déterminer lorsqu'elles ne sont pas fixées dans un texte légal.

C'est dans ce contexte que les délibérations de la CNIL constituent un juste et utile indice à la détermination de ces durées de conservation.

Aux termes de la mise en demeure de la société EDF, la CNIL précise que la conservation des données de consommations quotidiennes et à la demi-heure en base active pendant la durée de vie du contrat puis pendant cinq ans sans archivage intermédiaire était excessive.

De la même façon, la conservation par ENGIE des données des coordonnées du client et des données nécessaires à l'exécution du contrat pendant trois ans en base active puis pendant huit ans en archivage intermédiaire présente un sort similaire.

Les sociétés EDF et ENGIE disposent d'un délai de trois mois pour mettre en œuvre des mesures rectificatives aux manquements constatés et en justifier auprès de la CNIL.

A rapprocher : Décision n°MED 2019-035 du 31 décembre 2019 mettant en demeure la société ÉLECTRICITÉ DE FRANCE (EDF) ; Décision n°MED 2019-036 du 31 décembre 2019 mettant en demeure la société ENGIE ; EDF et ENGIE : mises en demeure pour non-respect de certaines conditions de recueil du consentement concernant les données des compteurs communicants, CNIL, 11 février 2020

PROPRIÉTÉ INTELLECTUELLE

Dépôt d'une marque de mauvaise foi et intention d'usage

CJUE, 29 janvier 2020, aff. C.371-18

Ce qu'il faut retenir :

La CJUE précise que le dépôt d'une marque sans intention de l'utiliser peut être considéré comme ayant été effectué de mauvaise foi, que si la preuve en est rapportée ; aucune présomption ne découle du fait que le demandeur au dépôt n'a pas d'activité dans le secteur d'activité concerné par le libellé.

Pour approfondir :

Dans le cadre d'un contentieux de contrefaçon entre deux sociétés anglaises devant la High Court of Justice de Londres, la société poursuivie contestait la validité de la marque qui lui était opposée. Elle soulevait à cette fin différents motifs de nullité dont la mauvaise foi, estimant que le dépôt de la marque avait été effectué de mauvaise foi car la société titulaire de celle-ci n'avait manifestement pas l'intention de l'utiliser.

La juridiction anglaise a saisi la CJUE de la question préjudicielle suivante : « *Le simple fait de demander l'enregistrement d'une marque sans aucune intention de l'utiliser concernant les produits et les services spécifiés constitue-t-il un acte de mauvaise foi ?* ».

La Cour rappelle en premier lieu que le dépôt d'une marque effectué de « mauvaise foi » compte parmi les causes de nullité de la marque. Si la jurisprudence européenne a pu donner des exemples de cas de mauvaise foi justifiant l'annulation du dépôt, elle était pour la première fois saisie de la question de savoir si, celui qui dépose une marque en n'ayant pas l'intention de l'utiliser, peut se voir sanctionné et perdre ses droits.

La Cour procède ensuite au rappel utile que le système européen n'exige pas une exploitation immédiate de la marque lorsqu'elle est déposée. On sait en effet que la déchéance pour défaut d'exploitation est encourue au terme d'un délai de cinq ans suivant le dépôt, il peut en effet arriver que, lorsqu'il accomplit cette formalité, le déposant ne connaisse pas l'usage qu'il fera de la marque qu'il dépose.

Aussi, aux termes de cet arrêt, la CJUE répond à la question préjudicielle ainsi : « *La mauvaise foi ne peut cependant être caractérisée que s'il existe des indices objectifs pertinents et concordants tendant à démontrer que, à la date du dépôt de la demande d'enregistrement de la marque considérée, le demandeur de celle-ci avait l'intention soit de porter atteinte aux intérêts de tiers d'une manière non conforme aux usages honnêtes, soit d'obtenir, sans même viser un tiers en particulier, un droit exclusif à des fins autres que celles relevant des fonctions d'une marque (...). La mauvaise foi du demandeur d'une marque ne saurait donc être présumée sur la base du simple constat que, au moment du dépôt de sa demande d'enregistrement, ce demandeur n'avait pas d'activité économique correspondant aux produits et aux services visés par ladite demande.* ».

Aussi, retenons que la mauvaise foi doit toujours être prouvée, par conséquent un dépôt de marque sans l'intention de l'utiliser pourrait être considéré comme ayant été effectué de mauvaise foi, pour autant et seulement si la preuve d'une intention de porter atteinte aux intérêts de tiers ou d'obtenir un droit exclusif en détournant le droit des marques de sa fonction soit rapportée. Difficile preuve à rapporter si la mauvaise foi réside, prétendument, dans le fait de déposer une marque sans avoir l'intention de l'utiliser car cela peut résulter, par exemple, d'un changement de stratégie commerciale.

La Cour rassure ainsi en affirmant que la mauvaise foi ne saurait être présumée du seul fait que le déposant n'exerce pas d'activité économique dans le secteur correspondant aux produits et services objets du libellé de la marque.

A rapprocher : CJUE, 29 janvier 2020, aff.C.371-18

Blocage de sites proposant des produits contrefaisants

Trib. Jud. Paris, Ord. réf., 8 janvier 2020,
RG n°19/58624

Ce qu'il faut retenir :

En cas d'atteinte à une marque, le titulaire de celle-ci peut solliciter des mesures de blocage d'accès à des sites internet auprès des FAI sur le fondement de l'article 6-I-8 de la LCEN.

Pour approfondir :

L'article 716-6 du Code de la propriété intellectuelle contient les dispositions spéciales organisant la procédure de référé en cas d'atteinte au droit sur une marque. Aux termes de l'ordonnance en référé rendue le 8 janvier 2020, le président du tribunal judiciaire de Paris admet qu'en cas de contrefaçon, le titulaire d'une marque puisse se fonder sur les dispositions de l'article 6-I-8 de la LCEN (Loi pour la confiance dans l'économie numérique) pour solliciter des mesures de blocage d'accès à des sites internet.

La LCEN organise en effet un régime de responsabilité en cascade des éditeurs de site, hébergeurs et des fournisseurs d'accès à internet. L'article 6-I-8 de cette loi prévoit ainsi : « *L'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 ou, à défaut, à toute personne mentionnée au 1, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* » ; les FAI (fournisseurs d'accès internet) peuvent donc se voir contraints de prendre des mesures pour bloquer l'accès à des sites lorsque les démarches auprès des éditeurs et hébergeurs n'ont pas permis de faire cesser les troubles constatés. En l'espèce, des titulaires de marques de luxe dans le domaine de la joaillerie avait constaté la vente de produits manifestement contrefaisants sur plusieurs sites internet. Ceux-ci ne comportaient pas les mentions légales obligatoires et, faute d'avoir pu contacter les éditeurs desdits sites, avaient pris contact avec les hébergeurs pour solliciter qu'ils suppriment l'accès aux sites litigieux. Or, leurs démarches étaient restées vaines. Pour cette raison, le recours au référé prévu par l'article 6-I-8 précité semblait le seul possible pour obtenir des mesures de nature à empêcher l'accès aux sites proposant à la vente des produits contrefaisants.

La décision de référé autorise ce recours alors que l'un des FAI tentait de faire juger qu'en raison de l'existence d'une procédure spéciale de référé-contrefaçon prévue par l'article L.716-6 du Code de la propriété intellectuelle, il n'était pas possible de se fonder sur l'article 6-I-8 de la LCEN. Or, l'ordonnance de référé énonce clairement : « *Les demandes de blocage de l'accès à certains noms de domaine faites par les sociétés demanderesses peuvent de ce fait reposer sur le fondement des articles 809 du Code de procédure civile et 6-I-8° de la Loi pour la confiance dans l'économie numérique* ».

On se félicitera de cette décision qui va dans le sens d'une meilleure protection contre la contrefaçon en autorisant le recours à des mesures efficaces et radicales.

A rapprocher : Article 6-I-8 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique

Recours administratif à l'encontre d'un brevet d'invention : publication de l'ordonnance n°2020-116
Ordonnance n°2020-116 du 12 février 2020 portant création d'un droit d'opposition aux brevets d'invention

Ce qu'il faut retenir :

Le 13 février 2020, a été publiée au Journal Officiel l'ordonnance n°2020-116, adoptée la veille et portant création d'un droit d'opposition aux brevets d'invention délivrés par l'Institut National de la Propriété Intellectuelle (INPI). Tel que prévu par l'article 121 de la loi PACTE du 22 mai 2019, cette ordonnance donne aux tiers la possibilité d'introduire un recours administratif auprès de l'INPI à l'encontre d'un brevet d'invention en vue d'en demander la modification ou la révocation. L'ordonnance entrera en vigueur au 1^{er} avril 2020, ses dispositions n'étant applicables qu'aux brevets d'invention publiés au Bulletin Officiel de la Propriété Intellectuelle (BOPI).

Pour approfondir :

Jusqu'à présent, seule une action en nullité auprès du tribunal de grande instance permet de s'opposer à un brevet délivré par l'INPI. Cette action est particulièrement contraignante tant elle suggère des coûts importants, l'intervention de plusieurs acteurs et des délais longs et non maîtrisables. Elle s'est ainsi révélée de nombreuses fois comme un obstacle pour les acteurs économiques les plus faibles, comme les chercheurs indépendants, les TPE, PME et les start-ups.

L'article 121 de la loi PACTE a instauré un nouveau droit d'opposition aux brevets d'invention délivrés par l'INPI pour permettre aux tiers de demander par voie administrative la révocation ou la modification d'un brevet. Ce nouveau droit vise à mettre en place une procédure simplifiée dont les coûts (moindres) et les modalités devaient être précisés par voie d'ordonnance.

C'est dans ce contexte que l'ordonnance du 12 février 2020 met fin à cette situation défavorable pour les inventeurs. En créant un droit d'opposition à l'encontre des brevets d'invention, elle marque le début d'une ère nouvelle permettant aux tiers de faire valoir leurs droits de propriété industrielle dans le cadre d'une procédure administrative simple et peu coûteuse. Si le champ

d'application de ce nouveau droit est limité aux seuls brevets d'invention, à l'exclusion des autres titres de propriété industrielle protégeant les inventions, comme le certificat d'utilité et le certificat complémentaire de protection, la sécurité juridique conférée aux tiers n'en est pas moins accentuée.

L'ordonnance compte trois chapitres et huit articles, le premier modifiant les livres IV et V du Code de la propriété intellectuelle, le second s'intéressant aux mesures d'application et d'adaptation pour l'outre-mer et le dernier détaillant les dispositions transitoires et finales.

Dès l'entrée en vigueur de cette ordonnance, le 1^{er} avril 2020, les missions de l'INPI se verront renforcées et une nouvelle obligation pèsera sur les épaules de son directeur général. Ce dernier aura la responsabilité de statuer sur les demandes d'opposition que les tiers pourraient former à l'encontre des brevets d'invention.

Ce droit pourra être exercé par toute personne, à l'exception du titulaire du brevet, sans que sa mise en œuvre ne soit soumise à un intérêt à agir (article L.613-23 modifié du Code de la propriété intellectuelle). L'idée est de permettre aux tiers de s'opposer, sur tout ou partie du brevet, au monopole d'exploitation du titulaire sur son invention.

L'opposition doit nécessairement reposer sur l'un des motifs énoncés à l'article modifié L.613-23-1 du Code de la propriété intellectuelle, à savoir le défaut de brevetabilité de l'invention, la faiblesse de la description qui ne permet pas à un homme du métier de pouvoir l'exécuter, l'extension de l'objet au-delà du contenu de la demande initiale telle qu'elle a été déposée.

Au cours de la procédure d'opposition, l'ordonnance reconnaît au titulaire du brevet la possibilité de modifier son titre afin de se mettre en conformité avec les revendications, sous réserve de respecter les conditions posées par le texte et qui seront codifiées au nouvel article L.613-23-3 du Code de la propriété intellectuelle.

La procédure d'opposition, aux termes du nouvel article L.613-23-2 du Code de la propriété intellectuelle, comprend une phase d'instruction et est contradictoire.

La décision du directeur général de l'INPI aura les effets d'un jugement, à préciser que le silence de ce dernier et de l'INPI vaudra rejet de la demande d'opposition. Le directeur général aura le choix de la décision et pourra soit rejeter la demande – ce qui implique que le titre soit conservé tel que délivré –, soit y faire droit. S'il décide de recevoir la demande, le directeur général pourra révoquer le brevet dans son intégralité ou simplement partiellement, auquel cas le titulaire du brevet sera renvoyé devant l'INPI afin qu'il demande la modification de son titre pour se conformer à la décision.

Cette demande ne sera recevable que si la décision statuant sur la décision est insusceptible de recours ; le directeur général aura la possibilité de la rejeter pour défaut de conformité à la décision de révocation partielle.

Le nouvel article L.613-23-6 du Code de la propriété intellectuelle qui prévoit ces hypothèses précise que la décision de révocation a un effet absolu et rétroactif à la date de dépôt de la demande de brevet.

Concernant les frais de procédure, l'article L.613-23-5 du Code de la propriété intellectuelle indique que chaque partie supporte les frais qu'elle a exposés, bien que le directeur général de l'INPI puisse décider d'une répartition différente.

Enfin, l'ordonnance modifie les articles L.613-24 et L.613-25 du Code de la propriété intellectuelle qui, respectivement, articulent les procédures d'opposition et de limitation des brevets et ajoutent aux motifs de nullité d'un brevet l'hypothèse de l'extension de la protection conférée par le titre à la suite d'une décision statuant sur une opposition.

La création de ce droit d'opposition aux brevets d'invention s'inscrit dans le cadre des actions de modernisation du système français de propriété industrielle prévues par la loi PACTE du 22 mai 2019, dont l'objectif est de conforter la qualité des brevets français, et ainsi de renforcer l'attractivité de la France pour le dépôt de titre de propriété intellectuelle. L'ordonnance permet d'accorder le droit français avec les pratiques des autres offices de propriété industrielle en Europe et dans le monde, et avant tout sur celles de l'Office Européen des Brevets qui prévoyaient déjà des recours administratifs à l'encontre de brevets d'invention.

L'ordonnance entrera en vigueur le 1^{er} avril 2020 et s'appliquera à tous les brevets d'invention dont la mention de délivrance a été publiée au BOPI à compter de cette date. La procédure d'opposition, les conditions d'exercice du droit et les délais seront précisés par un décret, très attendu, du Conseil d'Etat.

A rapprocher : Article 121 de la loi n°2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite loi PACTE ; Ordonnance n°2020-116 du 12 février 2020 portant création d'un droit d'opposition aux brevets d'invention

INTERNATIONAL

La loi antitrust en Chine – le projet de modification en vue d'une régulation renforcée des BATX Actualité législative

Ce qu'il faut retenir :

La Chine a annoncé la première modification depuis 2008 de sa législation antitrust afin de renforcer la régulation des BATX, l'équivalents chinois des GAFAs américains. La législation, qui ne visait auparavant pas les géants de l'internet chinois, devrait désormais s'appliquer à toutes les entreprises du secteur numérique du pays, cette fois-ci sans exception.

Pour mémoire :

Dans les pays occidentaux, on entend parler de GAFAs, pour Google, Apple, Facebook, Amazon afin de désigner les géants du web et de la tech. En Chine, il existe également les BATX, pour Baidu, Alibaba, Tencent et Xiaomi.

Le monopole de ses BATX commence à poser problème à la Chine, tout comme aux États-Unis et en Europe avec les GAFAs, car le pouvoir économique des BATX en Chine (sur l'e-commerce, le paiement par mobile, les jeux-vidéo, l'IA etc.) ne permet plus à de petites start-ups d'émerger et d'innover dans différents domaines technologiques et ainsi permettre à la croissance économique de la Chine.

Comme beaucoup d'Etats, dans un premier temps, la Chine a été tolérante envers certaines pratiques anti-concurrentielles pour ne pas freiner l'innovation et le développement des entreprises dans le secteur numérique. La Chine estime qu'il est désormais temps d'instaurer un climat de concurrence pour libérer de l'espace aux start-ups.

Pour la première fois depuis 2008, la Chine modifierait la législation antitrust afin de les réguler ce monopole de BATX, une manière de libérer de l'espace aux start-ups, souvent étouffées par les positions monopolistiques des géants.

Pour approfondir :

Le projet de la modification de la loi antitrust (《反垄断法》修订草案 (公开征求意见稿)) (le « **Projet** ») a été publié par State Administration for Market Regulation (市场监管总局) en date du 02/01/2020 pour une ouverture de consultation publique.

Le Projet consiste en la multiplication des sanctions pécuniaires visant les BAXT qui ne respecteraient pas la tendance gouvernementale.

Des amendes allant jusqu'à 100 fois la somme initialement prévue pour les cas de manquement pourront désormais être appliquées. Il est à noter que l'ancienne législation préconisait déjà des sanctions allant de 1 à 10% du chiffre d'affaire total des entreprises contrevenantes.

Désormais, les sociétés pourront être pénalisées jusqu'à 7 millions de dollars. Néanmoins cet élan peut être relativisé dans la mesure où les sanctions prononcées à l'égard des GAFAs par la Commission européenne pour abus de position dominante demeurent bien supérieures : Google a, en deux ans, été condamné à verser 8,2 milliards d'euros par Bruxelles.

Dans le passé, la Chine utilisait les revenus ou les parts de marché pour déterminer si une entreprise détenait un monopole. Mais ces principes ne sont plus adaptés à l'ère d'internet qui a fait émerger des sociétés qui parfois contrôlent de précieuses informations sans forcément produire beaucoup d'argent car elles n'ont pas monétisé ces données.

La législation permet en outre le renforcement des pouvoirs de régulation des autorités chinoises sur les BATX, à l'heure où la question de la protection et de l'utilisation des données personnelles commence en outre à prendre part au débat public.

A rapprocher : Le texte du Projet en chinois sur le site de State Administration for Market Regulation

STARTUP & LEGALTECHS / TENDANCES

Déploiement national de « Signaux Faibles » : l'IA au service de la prévention des difficultés
Actualité

Ce qu'il faut retenir :

Après des premiers résultats encourageants, le nouvel outil « Signaux Faibles » a été déployé sur l'ensemble du territoire national permettant ainsi de détecter précocement les difficultés rencontrées par les entreprises.

Pour approfondir :

Développé par la startup d'Etat « Etalab », l'outil « Signaux Faibles » permet de croiser les données financières, économiques et sociales relatives aux entreprises détenues par les différents services de l'Etat, ces données confidentielles étant, par la suite, traitées par des algorithmes basés sur des mécanismes d'apprentissages permettant de déterminer une probabilité de défaillance à 12, 18 voire 24 mois.

Les résultats sont ensuite partagés sur une plateforme numérique collaborative ouverte exclusivement à la Direction générale des entreprises, la Banque de France, la Délégation générale à l'Emploi et à la Formation professionnelle et l'Agence centrale des organismes de sécurité sociale, permettant ainsi à ces organismes de proposer des solutions d'accompagnement adaptées aux besoins des entreprises en difficulté via l'intervention des CRP, chargés de mission de la Direccte, services de l'Urssaf ou encore les correspondants entreprises de la Banque de France en lien avec les partenaires régionaux.

D'abord testé en 2017 dans la région Bourgogne-Franche-Comté à l'initiative de la Direccte et de l'Urssaf Bourgogne, les premiers résultats se sont avérés très encourageants, la plateforme ayant vraisemblablement permis de détecter les difficultés rencontrées par 63 entreprises de la région aboutissant à 48 visites permettant une analyse de la situation.

Fort de ces premiers résultats, l'outil a été étendu à l'ensemble des régions, une convention de déploiement national ayant été conclue le 3 avril 2019 entre les organismes précités et le ministère de l'Économie.

Ce déploiement s'inscrit dans la droite ligne de la directive européenne n°2019/1023 du 20 juin 2019, relative aux restructurations préventives, cette dernière sollicitant des états membres qu'ils mettent au point des systèmes statistiques garantissant un suivi régulier des procédures et la création d'outils d'alerte précoce permettant de détecter les circonstances susceptibles de conduire à l'insolvabilité (articles 3 et 29).

Si aucun bilan n'a, pour l'heure, été établi au terme de cette année 2019 et à la suite du déploiement national de « Signaux Faibles », on peut espérer que ce nouveau dispositif permettra, en sus de ceux déjà existants, de détecter au plus tôt les difficultés des entreprises.

A rapprocher : Convention de déploiement national de l'outil « Signaux Faibles » du 3 avril 2019

Création du comité pilote d'éthique du numérique en France

Une avancée significative pour la prise en considération des enjeux liés à l'intelligence artificielle

Ce qu'il faut retenir :

En décembre dernier, le Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé (CCNE) a été chargé par le Premier Ministre, Edouard Philippe, de créer un comité pilote d'éthique du numérique.

Pour approfondir :

La création de ce comité constitue une avancée majeure pour la prise en considération et l'encadrement des enjeux éthiques relatifs à

l'intelligence artificielle. Cette démarche s'inscrit notamment dans la continuité du récent rapport publié par Cédric Villani « Donner un sens à l'intelligence artificielle » et de l'avis 129 du CCNE.

Le comité ainsi créé regroupe des professionnels d'horizons variés (et notamment des spécialistes du numérique, philosophes, médecins, juristes et membres de la société civile).

Les premiers avis du comité pilote d'éthique du numérique porteront sur les agents conversationnels (ou chats bots) ; le véhicule autonome et le diagnostic médical à l'ère de l'intelligence artificielle.

Un premier bilan des activités du comité pilote d'éthique du numérique devra être remis, au début de l'année 2021, au Président du CCNE, qui émettra ensuite des recommandations sur ce fondement.

ACTUALITÉ NUMÉRIQUE SIMON ASSOCIÉS

ÉVÉNEMENT REPORTÉ

En raison du contexte actuel lié à l'épidémie Covid-19, l'événement suivant, initialement prévu le 31 mars prochain, est reporté à une date ultérieure :

Le contrat informatique à l'heure du numérique

Petit-déjeuner conférence organisé par SIMON ASSOCIÉS et
l'AGENCE POUR LA PROTECTION DES PROGRAMMES (APP)