Réalité augmentée
Vers un encadrement juridique 3.0 ?

Avec la réalité augmentée, le monde virtuel se superpose désormais au monde réel, créant ainsi une forme de réalité mixte enrichie de nombreuses informations. Ce nouveau moyen de visualiser des contenus en 2D ou en 3D, promis à un bel avenir, pourrait bien bousculer les comportements des utilisateurs et la vie des affaires.

La réalité augmentée, de l'anglais « *AR* » ou « *Augmented Reality* », est une technologie permettant la superposition d'informations sur le monde réel. Lorsqu'un individu filme ce qui l'entoure, généralement avec la caméra de son smartphone ou de sa tablette – mais bientôt via ses lunettes ou ses lentilles connectées – du texte, des images ou des vidéos s'affichent alors en temps réel sur ce qu'il voit au travers de son écran, en fonction de ses mouvements, grâce à des marqueurs préalablement enregistrés qui déclenchent l'affichage des éléments visuels. Selon l'étude du cabinet américain Markets and Markets, le marché mondial de la réalité augmentée pourrait dépasser 5 milliards de dollars d'ici 2016[1]. De nouvelles formes d'atteintes à la vie privée, aux données personnelles et à la vie des affaires sont susceptibles de voir le jour, appelant ainsi une adaptation du cadre juridique actuellement applicable à cette nouvelle technologie.

LA REALITE AUGMENTEE DANS LA VIE DES UTILISATEURS

A l'instar des objets connectés, les applications embarquant des technologies de réalité augmentée auront, sous peu, un impact non négligeable sur la vie des utilisateurs. Technologies portées, géolocalisation, publicités ciblées, la plupart de ces dispositifs soulèvent des problématiques juridiques inédites à une échelle internationale, en raison notamment du traitement globalisé des données personnelles, plus connu sous le nom de Big Data.

WEARABLES ET VIE PRIVÉE

Parmi les technologies dites « *wearable* », *que l'on peut porter sur soi et qui évitent de tenir un appareil, les lunettes connectées* « *Google Glass* » dévoilées l'an dernier par le géant de l'internet Google devraient permettre d'afficher en temps réel des informations relatives à l'environnement de l'utilisateur, à son itinéraire, aux appels et messages reçus sur son téléphone, etc. Si à première vue, ces verres intelligents peuvent assister leur propriétaire dans sa vie quotidienne, ils peuvent aussi générer un risque important de violation de nos droits.

Les Google Glass peuvent ainsi se transformer en caméras de vidéosurveillance pour celui qui souhaiterait en faire une utilisation plus déplaisante puisqu'elles sont en effet capables de filmer et photographier discrètement et en haute définition les personnes croisées par leur porteur, et de partager ces images et vidéos sur internet. Les individus pourront ainsi être « *taggués* » sur des réseaux sociaux à leur insu, encore plus facilement qu'avec un simple smartphone. Le droit au respect de la vie privée de l'article 9 du code civil pourrait dans ce cas être sérieusement mis à mal.

Les risques d'atteinte à l'image ou à la réputation sont d'autant plus élevés que des applications de reconnaissance faciale ou vocale ont déjà été créées. En France, des étudiants ont développé dès 2011 un concept d'application de rencontres amoureuses basé sur la réalité augmentée[2]: via un dispositif de reconnaissance faciale, les passants croisés dans la rue sont identifiés et leurs affinités amoureuses affichées, grâce aux informations partagées sur internet. Début 2014, une start-up a également développé l'application NameTag, permettant de trouver l'ensemble des profils d'une personne croisée dans la rue sur les réseaux sociaux. Si Google a indiqué refuser d'approuver de telles applications pour ses lunettes, la police de Dubaï a d'ores et déjà équipé ses officiers de Google Glass, lesquelles, synchronisées avec un fichier de délinquants, pourraient en faciliter l'arrestation, au détriment du droit au respect de la vie privée des individus. Aux États-Unis, NameTag permet même de reconnaître les personnes condamnées pour agression sexuelle, le fichier américain des délinquants sexuels étant librement accessible sur internet[3].

Face à ce risque exponentiel d'intrusion généralisée, les autorités de protection des données personnelles se sont mobilisées. Dès mars 2012, le G29 a émis un avis sur la reconnaissance faciale, rappelant qu'une image numérique contenant le visage clairement visible d'une personne qui peut ainsi être identifiée, peut constituer des données à caractère personnel[4]. Il est ainsi recommandé

aux responsables de traitements de veiller à ce que les images traitées ne représentent que des utilisateurs enregistrés. En juin 2013, plusieurs Cnil européennes ont sollicité du dirigeant de Google des explications sur le fonctionnement des Google Glass et sur leur conformité avec les lois de protection des données personnelles. En réponse à ces inquiétudes, Google a édité un code de bonne conduite – relativement sommaire – pour l'utilisation de ses lunettes[5]. Une interrogation subsiste néanmoins sur les moyens dont disposera une personne de faire cesser l'affichage d'informations la concernant sur l'écran connecté d'un passant qu'elle croise et qui aura scanné son visage, sans qu'elle n'en ait nulle connaissance...

GÉOLOCALISATION ET PUBLICITÉ CIBLÉE

La plupart des smartphones comportent aujourd'hui des systèmes de géolocalisation permettant de connaître la position exacte d'un individu au moyen de puces GPS. Lorsque celui-ci explore son environnement à l'aide de la caméra de son téléphone et d'une application embarquant un dispositif de réalité augmentée, telle l'application Yelp, il est alors possible de connaître l'endroit où se situe l'utilisateur. Il est ainsi tout à fait envisageable de lui proposer différentes offres et réductions dans les magasins ou restaurants environnants, voire d'indiquer sur les réseaux sociaux dans quelle enseigne la personne concernée s'est rendue. Outre les difficultés rencontrées en matière de protection de la vie privée, cette nouvelle forme de publicité ciblée, couplée à la réalité augmentée et à la géolocalisation, soulève sans surprise une problématique liée à l'utilisation des données personnelles de l'utilisateur et au recueil de son consentement. Les données de localisation sont en effet définies par la directive 2002/58/CE du 12 juillet 2002 comme des « *données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

Pourtant, si l'utilisateur souhaite obtenir des informations sur une boutique en particulier via un dispositif de réalité augmentée, il n'aura pas nécessairement donné son accord pour recevoir les offres des magasins concurrents sur l'écran de son portable, par SMS ou par e-mail, ou pour que son activité de la journée soit partagée sur un réseau social. Les traitements de données à caractère personnel étant régis en France par les dispositions de la loi Informatique et libertés du 6 janvier 1978 et par celles de la directive 95/46/CE du 24 octobre 1995, les concepteurs d'applications utilisant des dispositifs de réalité augmentée devront ainsi impérativement respecter les obligations portées par ces textes, et prendre en compte le futur règlement européen sur la protection des données personnelles, lequel prévoit notamment un durcissement de la responsabilité des responsables de traitement[6].

Face au développement fulgurant de cette technologie, il apparaît enfin nécessaire de sensibiliser les utilisateurs sur les implications de la réalité augmentée en matière de données personnelles. Le 15 octobre 2010, la Cnil avait déjà alerté les utilisateurs de Facebook sur les dangers de la fonctionnalité « *Facebook Places* » permettant aux internautes d'indiquer librement leur emplacement et celui de leurs amis. La Cnil avait à ce titre rappelé que la mise en place de publicités ciblées issues de données de géolocalisation ne pouvait être adressée aux internautes qu'après les avoir dûment informés et avoir recueilli leur consentement express, en application de la loi Informatique et libertés et de l'article L34-1 V du code des postes et des communications électroniques. Le G29, dans un avis du 16 mai 2011, a également recommandé que le service de géolocalisation d'un smartphone ne soit pas mis en service par défaut et que le consentement de l'utilisateur soit renouvelé chaque année[7]. Il ne fait cependant nul doute que les responsables de traitements contourneront une telle contrainte par l'obtention de l'accord du client potentiel lors de son adhésion à un programme de fidélisation quelconque lui permettant d'obtenir régulièrement des offres promotionnelles et exclusives.

LA REALITE AUGMENTEE DANS LA VIE DES AFFAIRES

Les usages professionnels de la réalité augmentée sont promis à un fort développement ces prochaines années et pourraient soulever certaines difficultés, notamment en matière de secret des affaires, de concurrence déloyale, et d'atteintes aux marques.

Un secret des affaires malmené ?

Alors que le secret des affaires s'inscrit indéniablement dans les actifs immatériels d'une société, l'utilisation de la réalité augmentée pourrait mettre à mal la confidentialité qui entoure les informations concernées. Les wearables utilisant la technologie de réalité augmentée possédant des capacités de photographie et de vidéo, des salariés malintentionnés pourraient discrètement enregistrer, photographier ou filmer des informations confidentielles ou sensibles et les partager sur internet ou les transmettre à des concurrents en quelques secondes. L'entreprise éprouvera alors des difficultés à connaître l'origine de la fuite et à tracer les moyens utilisés. Cette menace est certes déjà présente depuis le développement des smartphones, mais elle pourrait bien prendre une toute autre dimension avec la réalité augmentée.
Dans ces conditions, les employeurs devront donc se montrer vigilants et adopter des mesures de sécurité adaptées au sein de leurs sociétés. En premier lieu, l'ensemble des documents sensibles devront comporter un filigrane portant la mention « *confidentiel* ». Les employeurs pourront en second lieu choisir de limiter voire d'interdire l'utilisation d'une telle technologie dans certaines zones de l'entreprise, en affichant ces règles à destination des salariés ou des visiteurs ou en utilisant des systèmes de brouillage. Enfin, une adaptation de la charte informatique de l'entreprise sera également nécessaire, ainsi que la signature d'accords de confidentialité par les salariés.
A l'heure actuelle, le secret des affaires connaît une protection juridique au travers d'infractions particulières telles que l'atteinte au secret professionnel, au secret des correspondances, le vol, l'intrusion dans un système informatisé de données, la révélation d'un secret de fabrique, etc. Afin de faciliter la sanction des atteintes au secret des affaires, des députés ont présenté le 16 juillet 2014 une proposition de loi relative à la protection du secret des affaires[8]. Le Livre premier du code de commerce serait complété par un titre V, comportant un nouvel article L. 151-1 qui définit notamment le secret des affaires comme « *toute information qui ne présente pas un caractère public* » « *qui revêt une valeur économique* » et « *qui fait l'objet de mesures de protection raisonnables* ». Un principe général d'interdiction de violer le secret des affaires serait édicté et les sanctions pénales fixées à 3 ans d'emprisonnement et 375.000 euros d'amende. S'il est voué à prévenir les atteintes au secret des affaires, ce futur cadre juridique devrait aussi dissuader les utilisateurs de réalité augmentée de commettre de telles infractions lorsqu'ils portent ces dispositifs.

De nouvelles formes de concurrence déloyale

La généralisation des smartphones et tablettes a poussé les entreprises

à investir dans des applications de réalité augmentée pour proposer leurs produits aux utilisateurs. Les utilisateurs peuvent ainsi tester un canapé virtuel dans leur salon avant de l'acheter, essayer des vêtements devant leur ordinateur et des agents immobiliers leur indiquer en temps réel les appartements à vendre près de l'endroit où ils se trouvent.

Toutefois, à partir du moment où l'utilisateur doit capturer des clichés ou une vidéo de la réalité qui l'entoure pour que des informations relatives à une enseigne précise apparaissent, on peut imaginer que des concurrents tentent de bénéficier des investissements de celle-ci. Ce sera notamment le cas si une entreprise développe une application permettant de reconnaître la marque ou le logo d'un concurrent et d'y apposer, à la place, son propre élément distinctif ou ses propres offres commerciales. Ces informations nouvelles se superposeront ainsi à la réalité et cacheront la publicité ou la marque du concurrent. Au-delà des atteintes potentielles aux marques, cette forme d'« *ARsquatting* » *pourra être qualifiée de parasitisme économique, défini par les juges comme « l'ensemble des comportements par lesquels un agent économique s'immisce dans le sillage d'un autre afin de tirer profit, sans rien dépenser, de ses efforts et de son savoir-faire* »[9].

Par ailleurs, la réalité augmentée pourrait permettre à certains de jeter le discrédit sur un concurrent ou sur les produits qu'il fabrique afin d'en tirer un profit. Ce dénigrement, qui est une forme de concurrence déloyale, pourrait ainsi se matérialiser par l'ajout de fausses informations ou de commentaires particulièrement négatifs sur l'enseigne, le siège social ou le magasin d'un concurrent lorsque son logo ou sa marque sont captés par l'appareil de l'utilisateur. Les entreprises dénigrées engageront vraisemblablement des actions tendant à voir réparer leur préjudice, à condition de démontrer l'existence de celui-ci, notamment en cas de perte de clientèle.

Si la concurrence déloyale est sanctionnée sur le fondement de l'article 1382 du code civil, la difficulté principale face à de tels comportements anticoncurrentiels portera vraisemblablement sur la preuve de ces agissements. En effet, sur le plan technique, la réalité augmentée repose sur des symboles appelés « *marqueurs* », préalablement enregistrés sur les images qui seront filmées par l'utilisateur. Or ces marqueurs ne sont pas visibles par celui-ci, seul le contenu qui apparaît pouvant être visionné en temps réel. Ce dispositif rappelle d'ailleurs l'utilisation de mots-clés ou de meta tags invisibles aux yeux des visiteurs dans le code source des sites internet. Nul doute que les procès-verbaux de constats d'huissier réalisés sur des smartphones alimenteront un nouveau contentieux judiciaire. Il appartiendra dès lors aux magistrats d'adapter les règles applicables en la matière afin de clarifier les types de preuves pouvant être produites devant les juridictions.

Des contrefaçons numériques inédites

En ajoutant des données ou des médias au monde réel, la réalité augmentée permet de transformer le monde physique aux yeux des utilisateurs. En matière de propriété intellectuelle, cette technologie pourrait donc permettre d'utiliser des marques protégées de manière illicite.

L'article L713-3 du code de la propriété intellectuelle interdit la reproduction, l'usage, ou l'apposition d'une marque sans l'autorisation de son propriétaire s'il peut en résulter un risque de confusion dans l'esprit du public. L'article L713-2 du même code interdit pour sa part la suppression ou la modification d'une marque régulièrement apposée. Dans ces conditions, un individu qui remplacerait ou modifierait une marque via une application de réalité augmentée, sans l'autorisation de son titulaire, pourrait s'exposer à une action en contrefaçon sur le fondement des articles précités.

Les juridictions auront donc à se prononcer rapidement sur les véritables impacts de la réalité augmentée. En effet, les juges pourraient estimer que l'utilisation de certaines applications de réalité augmentée entraîne la transformation effective de la marque originale et que sa nouvelle forme se matérialise sur le smartphone ou la tablette de l'utilisateur. À l'inverse, il serait également possible de considérer que les contenus proposés en réalité augmentée ne modifient pas véritablement le monde physique mais constituent seulement une plateforme visuelle enrichie d'informations et accessible de manière éphémère. Dans ce dernier cas, le délit de contrefaçon pourrait alors être écarté.

Une démonstration frappante des possibles atteintes aux marques concerne une application iPhone intitulée « *The Leak in your Home Town* », littéralement « *une fuite dans votre ville natale* ». Utilisant la réalité augmentée, elle proposait en 2010 aux utilisateurs de filmer et de remplacer le logo de la compagnie pétrolière BP par l'image d'un puits déversant du pétrole, en réaction à l'explosion de sa plateforme Deepwater Horizon et à la marée noire intervenue dans le Golfe du Mexique l'année précédente. Bien que BP n'engagea aucune poursuite contre les développeurs, sûrement par peur de l'effet « *Streisand* », phénomène qui augmente la visibilité d'un contenu que l'on cherche à retirer, ce projet fut considéré comme la première atteinte à une marque grâce à la réalité augmentée.

CONCLUSION

Certains la voient comme une falsification du réel, d'autre comme une nette amélioration du monde qui nous entoure. Dans tous les cas, grâce à la réalité augmentée, de nombreux services pourront être proposés aux utilisateurs en temps réel et notre société de l'information se verra plus riche de centaines de milliers de nouveaux contenus, accessibles dans tout notre environnement et non plus sur nos équipements traditionnels. Il nous appartiendra toutefois de nous montrer vigilants : qu'elles concernent la vie privée, la concurrence ou la propriété intellectuelle, les nouvelles formes d'atteintes aux droits pourraient fortement augmenter, et ce de manière bien réelle…

Caroline LAVERDET
Avocat à la cour

Notes

(1) Virtual Reality & Augmented Reality Market Forecast by Product (2011 - 2016), http://www.marketsandmarkets.com/Market-Reports/reality-applications-market-458.html

(2) Concept Go For It Dating 3.0

(3) National Sex Offender Public Website, www.nsopw.gov

(4) Groupe de travail « Article 29 » sur la protection des données, avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles, 22 mars 2012

(5) https://sites.google.com/site/glasscomms/glass-explorers

(6) Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données en date du 25 janvier 2012

(7) Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents, 16 mai 2011

(8) Proposition de loi relative à la protection du secret des affaires, n° 2139, 16 juillet 2014

(9) Com. 26 janv. 1999, n° 96-22.457; Com., 4 févr. 2014, n° 13-11.044