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