DS NEWSLETTER savoir, faire

NEWSLETTER – INFORMATIONS JURIDIQUES

PROPOSÉES PAR LE CABINET DS AVOCATS

Faut-il avoir peur de la reconnaissance faciale ?

ASIE

CONTEXTE

La reconnaissance faciale est une technologie combinant les techniques biométriques, l'intelligence artificielle, la cartographie 3D et le Deep Learning pour comparer et analyser les traits du visage d'une personne afin de l'identifier. Elle utilise des caméras pour collecter des images ou des flux vidéo, puis détecte automatiquement les données faciales qui s'y trouvent pour parvenir à la reconnaissance des personnes.

Depuis les trois dernières années, la reconnaissance faciale est utilisée largement en Chine dans des domaines aussi variés que la finance, la justice, l'armée, la sécurité publique, les contrôles aux frontières, l'aérospatiale, l'énergie, l'industrie, l'éducation, le médical et aussi bien par le gouvernement, que par des entreprises et institutions privées et publiques. Ainsi, par exemple, elle est communément utilisée pour accéder aux applications sur les téléphones mobiles. Elle permet d'effectuer des paiements en ligne et de se connecter à certains comptes bancaires simplement en « souriant » à la caméra de nos téléphones mobiles. Avec la popularité croissante de cette technologie, les données faciales deviennent progressivement la clé d'accès et le nouveau mot de passe des comptes bancaires.

Les autorités chinoises ont publié ces dernières années plusieurs circulaires ou avis préconisant l'application de la technologie de reconnaissance faciale. De ce fait, la reconnaissance faciale tient un rôle de plus en plus présent dans notre vie quotidienne:

- La Banque populaire de Chine encourage, depuis novembre 2016, les banques chinoises à utiliser des moyens technologiques sûrs et efficaces pour vérifier les données d'identité personnelles des titulaires de comptes bancaires individuels. Conformément à ce principe, plusieurs banques utilisent la reconnaissance faciale pour vérifier l'identité du titulaire d'un compte.

- Dans la province du Fujian et la ville de Guangzhou, les retraités peuvent déposer leur demande de départ à la retraite et d'obtention de pension par reconnaissance faciale, ce qui facilite les formalités administratives.

- Le bureau local des taxes de Pékin commence à délivrer des certificats / justificatifs pour les expatriés en utilisant la reconnaissance faciale

- Le Conseil des affaires d'État a recommandé dans une circulaire publiée le 26 février 2019 l'application de la reconnaissance faciale pour d'améliorer « l'enregistrement immobilier sur Internet ».

Outre les applications susmentionnées, de nombreux immeubles de bureaux, barrières de sécurité routière et applications mobiles utilisent la reconnaissance faciale.

LE CADRE JURIDIQUE GÉNÉRAL

La reconnaissance faciale est un sujet sensible car elle implique la collecte et la reconnaissance de données strictement personnelles, à savoir la biométrie faciale. Une utilisation incorrecte de celle-ci peut causer un réel impact sur notre vie privée. C'est pourquoi, compte tenu des menaces potentielles sur la vie privée liées à un abus de technologie, certains pays, tels les États-Unis, la Chine et la Suède, ont commencé à restreindre, voire à interdire, l'utilisation de la technologie de reconnaissance faciale dans certains domaines.

Vous avez certainement entendu parler de la condamnation de Facebook à une amende de 5 milliards de dollars pour abus de technologie de reconnaissance faciale en juillet 2019 prononcée par la Federal Trade Commission des États-Unis. Suite à cette amende, Facebook a mis à jour la fonction de reconnaissance faciale qui n'est plus activée par défaut dans son système, les utilisateurs pouvant dorénavant choisir leurs propres paramètres.

De même en Chine, le 1er novembre dernier, le tribunal populaire du district de Fuyang dans la ville de Hangzhou a été saisi de la première plainte civile pour un abus de technologie de reconnaissance faciale. Le demandeur, titulaire d'une carte annuelle d'un zoo, a poursuivi le zoo parce que ce dernier avait changé le système d'entrée, passant de la numérisation des empreintes digitales à l'utilisation de la reconnaissance faciale sans aucune information et sans le consentement des titulaires de la carte annuelle. Le zoo a ensuite été accusé de violation (i) des dispositions de l'accord de services entre le zoo et les titulaires de carte annuelle et (ii) de la loi de la République populaire de Chine sur la protection des droits et intérêts des consommateurs.

LES PRINCIPES GÉNÉRAUX DE LA PROTECTION DES INFORMATIONS BIOMÉTRIQUES EN CHINE

La reconnaissance faciale est basée sur les informations biométriques des personnes physiques, qui sont clairement définies comme des données personnelles[1] à l'article 76 alinéa 5 de la loi sur la cyber sécurité de la République populaire de Chine (« la CSL ») et qui à ce titre sont protégées par les lois chinoises.

La CSL stipule en outre que les opérateurs de réseau doivent respecter les principes de légalité, de proportionnalité et de nécessité lors de la collecte et de l'utilisation des données personnelles, et donc des informations biométriques. De plus, préalablement à toute collecte, ils doivent systématiquement obtenir le consentement des personnes concernées en leur indiquant le but, la méthode et l'étendue de la collecte et de l'usage des données.

Les principales exigences de la CSL concernant la collecte et l'utilisation des données faciales sont les suivantes:

Exigences	Contenus
Notification claire	Les opérateurs de réseau ne doivent pas utiliser d'expressions vagues pour obtenir le consentement des personnes physiques.
Consentement exprès	Les opérateurs de réseau doivent obtenir le consentement exprès des personnes physiques et non pas un consentement implicite.
Pertinence	Les opérateurs de réseau ne sont pas autorisés à collecter des données personnelles qui ne sont pas pertinentes pour leurs activités.
Confidentialité	Les opérateurs de réseau ne doivent pas divulguer, altérer les données personnelles ou les fournir à un tiers sans le consentement préalable des personnes physiques concernées, sauf dans le cas où les données personnelles ont fait l'objet d'un traitement rendant impossible leur récupération et la correspondance avec une personne spécifique, c'est-à-dire lorsque la confidentialité des données personnelles est maintenue.
Droit de suppression/correction	Les personnes physiques ont le droit de demander la correction et / ou la suppression de leurs données personnelles aux opérateurs de réseau. Ces derniers doivent prendre des mesures pour supprimer ou corriger ces données.

[1] *«Toute information enregistrée électroniquement ou par tout autre moyen, qui indépendamment ou conjointement peut être utilisée pour identifier les informations personnelles d'une personne physique, y compris de manière non-exhaustive les noms, date de naissance, n° de carte d'identité, information biométriques, adresses, n° de téléphone, etc. ».*

Sanctions administratives en cas de violation de l'une des 5 exigences ci-dessus: • Avertissement et/ou ; • Confiscation des revenus illégaux et/ou ; • Amende d'un montant compris entre une fois et dix fois les revenus illégaux, ou en cas d'absence de revenu illégal, d'un montant maximum de 1 million de RMB (environ 128 000 €) ; • De plus, une amende comprise entre 10 000 RMB (environ 1 278 €) et 100 000 RMB (environ 12 776 €) peut être infligée aux responsables directs de l'infraction ; • Enfin dans les cas graves, les opérateurs de réseau peuvent être condamnés à : - suspendre les activités concernées, - arrêter les activités concernées et procéder à une rectification, - fermer le site Web, - la révocation de leurs licences et autorisations professionnelles.	
L'utilisation illégale des données personnelles est interdite	Il est interdit d'acquérir des données personnelles en volant ou par d'autres moyens illégaux, ni de vendre ou de fournir illégalement des données personnelles à des tiers.
Sanctions administratives pour violation de l'obligation susmentionnée: • Confiscation des revenus illégaux et/ou ; • Amende d'un montant compris entre une fois et dix fois les revenus illégaux, ou en cas d'absence de revenu illégal, d'un montant maximum de 1 million de RMB (environ 128 000 €).	

ADDVICES OF DS:

Avant toute collecte ou utilisation de données faciales, les entreprises doivent non seulement veiller au respect du principe de «consentement préalable», mais également procéder à une évaluation minutieuse afin de s'assurer que l'utilisation de ces données satisfait bien aux principes de légalité, proportionnalité et nécessité. Elles peuvent par exemple se poser les questions suivantes : est-il vraiment nécessaire de collecter des données de reconnaissance faciale pour vérifier uniquement la fréquentation d'un site, ou pour compter le nombre de personnes physiques présentes sur site à un instant T ? N'y aurait-il pas un autre moyen permettant d'aboutir au même objectif, en collectant des données moins sensibles ?

En outre, les entreprises doivent prendre des mesures raisonnables pour restreindre l'accès aux données collectées, et respecter les exigences minimales raisonnables et nécessaires pendant la durée de rétention.

En cas d'utilisation de données faciales collectées par des entreprises à des fins commerciales, il est dûment nécessaire d'informer les personnes concernées et d'obtenir leur consentement à l'avance. De plus, les entreprises devront prendre des mesures raisonnables pour empêcher tout accès aux données, qu'il soit autorisé ou pas, et d'éviter de collecter des types et/ou des volumes de données injustifiés. En ce qui concerne la durée de rétention (combien de temps les données personnelles peuvent être gardées et/ou contrôler depuis qu'elles ont été collecté), il n'y a pas actuellement de durée de rétention maximum mandataire ou unifiée pour les données personnelles, normalement la durée de rétention ne doit pas excéder la période de temps nécessaire requise par les besoins commerciaux et/ou les lois et régulations applicables. Cependant, il faut noter que dans certains domaines spéciaux il y a une durée de rétention mandataire minimum associée aux données personnelles. Par exemple, CSL exige que les opérateurs de

réseau gardent les fichiers web pertinents au statut du fonctionnement de leurs réseaux et aux incidents de sécurité informatique durant une période d'au moins six mois. Dans ce cas, si ces fichiers web contiennent des données personnelles, les opérateurs de réseau devront les garder durant au moins six mois.

En cas d'utilisation d'un logiciel de reconnaissance faciale ou d'équipements et installations fournis par un tiers, il est fortement recommandé de conclure un accord avec ce tiers afin de définir le champ autorisé d'utilisation des données personnelles collectées, en spécifiant notamment, les droits et obligations de ce tiers, les obligations de confidentialité, la durée de rétention des données personnelles collectées et le droit des personnes physiques concernées à faire supprimer leurs données à la fin de la coopération commerciale. Par exemple, si l'entreprise A collecte des données personnelles (qui peuvent inclure des données faciales) en utilisant un logiciel fourni par l'entreprise B, et les deux entreprises ont conclu un accord du type mentionné plus haut, l'entreprise A se devra de contacter l'entreprise B et de lui demander d'effacer certaines données sauvegardées/ partagées avec l'entreprise B par l'entreprise A, au moment où ces entreprises terminent leur coopération ou à la demande de la personne concernée.

Enfin, en l'état actuel des lois et réglementations en vigueur, les données faciales ne sont pas clairement définies comme entrant dans la catégorie des données personnelles sensibles. Selon le Guide d'information sur la sécurité de l'information sur la protection des informations personnelles du système d'information des services publics et commerciaux, **les données personnelles sensibles** se réfèrent aux **informations personnelles** qui peuvent avoir des effets négatifs si elles sont divulguées ou modifiées. Elles incluent par exemple **les numéros de carte d'identité, l'origine, l'appartenance politique, la religion ou croyance, les informations génétiques ou les empreintes digitales, etc.,**

Cependant, elles pourraient prochainement être définies comme des données personnelles sensibles. Selon le projet de norme nationale « technologie de sécurité des données - spécifications de sécurité des données personnelles, les données faciales sont considérées comme des données biométriques individuelles rentrant dans la catégorie des données personnelles sensibles. Auquel cas, les entreprises devront, alors, assumer des obligations de protection plus strictes. Par conséquent, en anticipation de ces futures obligations, nous conseillons aux entreprises d'améliorer leur système de protection en matière de sécurité des données biométriques, de chiffrer ses dernières, de les stocker de manière sécurisée, de prendre des mesures de désensibilisation (désensibilisation signifie traiter les données personnelles de façon à ce qu'elles ne puissent pas être utilisées pour identifier une personne précise) et d'autres mesures techniques, et de procéder à leur suppression complète à l'expiration de la période de traitement ou lorsque la personne concernée demande leur suppression.

Pour toute information complémentaire, merci de contacter :

Zhang Beibei : Associate
zhangbeibei@dsavocats.com

Sylvie Savoie : Counsel
savoie@dsavocats.com