Reconnaissance faciale : impossibilité juridique ou résistance psychologique ?

Le cadre juridique contraignant de la reconnaissance faciale freine son utilisation dans l'Hexagone. Cependant, rien n'est insurmontable selon Éric Barbry et Raphaël Buchard, avocats au cabinet Racine.

Du côté de la Cnil. Comme le dit la Cnil elle-même, *« cette technologie n'en est désormais plus à ses balbutiements. Les enjeux de protection des données et les risques d'atteinte 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 tout du moins faire l'objet d'une analyse d'impact relative à la protection des données (AIPD). »*
CQFD : même pour la Cnil, la reconnaissance faciale n'est pas interdite mais doit être strictement encadrée.

La ville de Nice a expérimenté la reconnaissance faciale lors du dernier Carnaval.

Pourquoi alors cette technologie, qui fait preuve d'une grande fiabilité aussi bien pour des objectifs d'identification (retrouver une personne dans une foule) que d'authentification (s'assurer que la personne est la bonne), est-elle si peu développée ?
Beaucoup disent que c'est à cause d'un cadre juridique trop contraignant. Il n'en est rien, puisque la mise en œuvre d'un tel mécanisme doit simplement répondre à un double cadre juridique bien connu : le RGPD et la réglementation sur la vidéoprotection.
Il convient ainsi de distinguer différentes situations : d'une part la mise en œuvre par les autorités publiques de solutions de reconnaissance faciale pour des raisons de sécurité et de sûreté, d'autre part l'usage personnel d'outils de reconnaissance faciale (sur votre smartphone par exemple), qui sont toutes deux exclues du champ d'application du RGPD.
Reste la mise en œuvre de solutions de reconnaissance faciale dans le cadre d'une entreprise pour identifier et/ou authentifier ses salariés, ses clients ou d'autres catégories de personnes (élèves, étudiants, membre d'un club…).

Du côté du RGPD. Dans ce cas, la règle est simple côté RGPD. La reconnaissance faciale est clairement une « donnée biométrique » au sens du point 14 de l'article 4 (définitions) du RGPD. Cet article stipule en effet que sont des *« données biométriques, 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 »*. La précision *« telles que les images faciales »* ne fait donc aucun doute sur l'appartenance de la reconnaissance faciale comme « donnée biométrique ».
Ce faisant, la solution de reconnaissance faciale entre dans la catégorie des données dites « particulières » de l'article 9 du RGPD. C'est sur ce seul point qu'il existe une difficulté.
En effet, l'article 9 premier paragraphe précise que *« les traitements des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les traitements des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits »*.

Les exceptions à l'interdiction. Par nature donc, les traitements de données biométriques sont interdits. Mais il existe un certain nombre d'exceptions dont deux majeures : le consentement de la personne et les traitements nécessaires pour des motifs d'intérêt public importants, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionnel à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.
Le droit n'est donc pas l'ennemi ou la justification de l'opposition à la reconnaissance faciale. En réalité l'abandon de projets de reconnaissance faciale a toujours pour origine une fronde de la société civile comme cela fut le cas avec le projet contesté de fluidification de l'accès au métro parisien via ce dispositif ou les difficultés de la ville de Nice pour son « test » grandeur nature lors du Carnaval de Nice.
L'utilisation de cette technologie par la Chine dans le cadre d'un dispositif massif de surveillance de ses citoyens n'en est d'ailleurs certainement par étrangère.
Pourtant, bien qu'il existe effectivement des règles juridiques strictes à respecter, la reconnaissance faciale n'implique rien d'insurmontable pour une entreprise.
Tout au plus, la mise en place de cette technologie peut se résumer en cinq points essentiels : la justification d'une exclusion à l'article 9, l'analyse d'impact, l'information des personnes, la sécurité et le délégué à la protection des données (« DPO »).
La justification à l'exclusion soit du RGPD, soit de l'article 9 est un prérequis. Il conviendra avant tout projet de démontrer qu'en l'espèce, le RGPD n'est pas applicable ou que la personne qui met en œuvre une solution de reconnaissance faciale entre dans une des exceptions de l'article 9.
L'analyse d'impact est une obligation (cf. Cnil) et doit être réalisée préalablement à la mise en œuvre de la solution. Son objectif est de vérifier que le traitement de données personnelles n'engendre pas de risque pour les droits et libertés des utilisateurs du service proposé et, le cas échéant, de proposer et de mettre en œuvre des solutions juridiques et techniques pour y remédier.
Le projet étant ainsi légitimé, il faut encore s'assurer que les personnes susceptibles d'être identifiées ou authentifiées par des moyens de reconnaissance faciale soient informées de manière transparente, claire et précise, sur l'utilisation des données personnelles et les finalités du dispositif. Cette information sera généralement réalisée via la « politique de protection des données ».
Bien évidemment, il est nécessaire de garantir un niveau très élevé de sécurité que ce soit pour la conservation des « gabarits » ou des images elles-mêmes et de définir les durées de conservation et d'accès appropriés.
Enfin, pour garantir le respect du RGPD face à un tel projet, même si cela n'est pas toujours obligatoire, la désignation d'un délégué à la protection des données semble être une bonne pratique. S'il en existe un, il devra impérativement être saisi du projet et conseiller le responsable de traitement.
Le rejet des solutions de reconnaissance faciale est donc essentiellement psychologique. La réalité est d'autant plus triste que nombre de sociétés françaises sont en pointes sur le sujet mais ne peuvent « vendre » leur solution qu'à des pays tiers… Cherchez l'erreur.
Pour cela il existe une solution simple. L'article 9 précité comporte un point 4 qui précise que *« les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé. »* Il suffirait donc que le Gouvernement se saisisse de la question et précise sa pensée sur les conditions d'utilisation de la reconnaissance faciale pour faciliter son usage… ou le condamner définitivement…
Mais il s'agit là d'une tout autre histoire qui ne fait que commencer.

Éric Barbry, avocat associé
Raphaël Buchard, avocat
Département IP IT & Data protection
Racine Avocats