TECHNOLOGIES BIOMÉTRIQUES

Au sein de l'UE, la mise en place de dispositifs sécuritaires reposant sur l'identification par reconnaissance faciale ou sur d'autres formes de technologies d'analyses biométriques a connu un véritable essor au cours de la dernière décennie. © DOMINIQUE DUCHESNES

La reconnaissance faciale a forcé la porte de l'Europe

Sous couvert d'expérimentation, l'usage de technologies biométriques à des fins de surveillance a gagné du terrain dans plusieurs pays européens, dont la Belgique. Le plus souvent hors de tout cadre juridique.

ARTHUR SENTE

Analyser à partir d'une image les caractéristiques physiques d'un visage, les transformer en données, et utiliser celles-ci ou pour identifier une personne. C'est (en version très simplifiée) le principe de la reconnaissance faciale, qui est sans nul doute la technologie biométrique qui suscite le plus d'intérêt à l'heure actuelle. Aujourd'hui, de plus en plus de personnes l'utilisent de leur plein gré, à des fins d'authentification (pour déverrouiller leur téléphone, par exemple), tandis que de l'autre côté du spectre, la manière dont la Chine s'en sert pour mener une surveillance de masse sur sa population est désormais largement documentée.

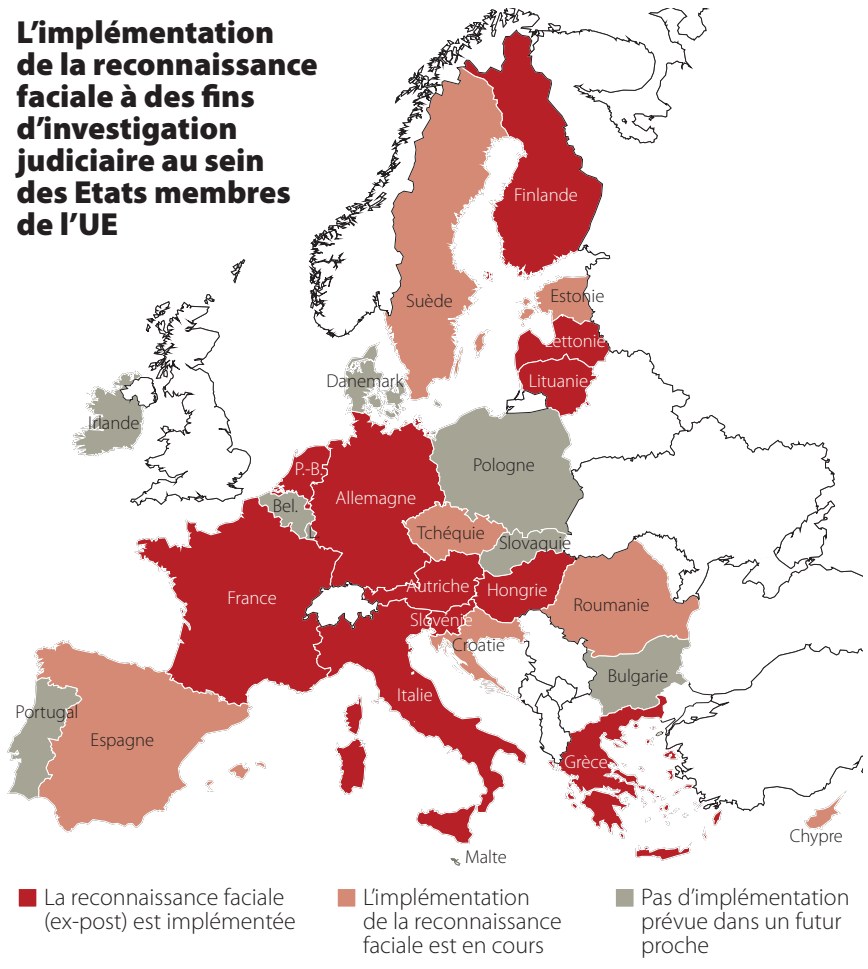
L'Europe n'est pas la Chine. Mais cela n'empêche qu'au sein de l'UE, la mise en place de dispositifs sécuritaires reposant sur l'identification par reconnaissance faciale ou sur d'autres formes de technologies d'analyses biométriques (capteurs de mouvements, de sons, d'émotions, etc.) a connu un véritable essor au cours de la dernière décennie. C'est l'une des conclusions d'un rapport dirigé par le chercheur Francesco Ragazzi, professeur associé en relations internationales à l'Université de Leiden (Pays-Bas), sur demande du groupe des Verts/ALE au Parlement européen. Dans ce document que *Le Soir* a pu consulter, son équipe de recherche s'est attelée à dresser une cartographie de l'existant sur le Vieux Continent. Et le moins que l'on puisse dire, c'est que des projets s'appuyant sur les technologies biométriques ont germé tous azimuts au cours de ces dernières années, bien souvent sous couvert d'expérimentation et dans une zone de flou juridique manifeste – quand ce n'est dans l'illégalité.

Une utilisation judiciaire dans 11 pays

On le sait peu, mais dans plusieurs pays d'Europe, 11 sur 27 pour être précis, la reconnaissance faciale à des fins d'identification de suspects dans le cadre d'investigations judiciaires est effectivement déjà une réalité – et elle le sera bientôt au sein de 7 autres. Sur ce plan, la Belgique (qui ne l'autorise pas) fait ainsi office d'exception au sein de l'UE. *A contrario*, en Allemagne, cela fait déjà plus de dix ans que des croisements entre la base de données policière nationale et des images de caméras peuvent être effectués via analyse biométrique, dans un cadre défini d'enquête. Attention, on ne parle *a priori* pas ici de tentatives d'identification « en temps réel » sur base d'images filmées en direct, mais d'analyses « ex-post », c'est-à-dire sur base d'images enregistrées qui sont consultées dans le cadre d'une enquête, notent les auteurs du rapport.

Si les auteurs estiment que ce type d'usage ne permet pas de parler de « surveillance de masse » à proprement parler, ce n'est pas le cas selon eux du recours à la reconnaissance faciale « en live », qui induit un flicage beaucoup plus généralisé. Or, cette forme de surveillance gagne aussi du terrain. L'épisode belge de l'installation de caméras « intelligentes » dans l'aéroport de Zaventem l'illustre bien. Ainsi, un dispositif « expérimental » de la police fédérale fut mis en place en 2017 mais ne fut amené qu'en 2019 à la connaissance du COC, l'Organe de contrôle de l'information policière belge. Le principe ? Un logiciel analysait en direct les images dans le but de repérer la présence d'éventuels individus « blacklistés ». Le COC a fini par déclarer l'usage illégal et le dispositif fut désactivé, mais restera en place. La mésaventure belge n'a pour autant pas refroidi tout le monde. Après une modification de sa législation en 2019, la Hongrie a notamment ouvert la voie à la reconnaissance faciale « en live » avec son projet « Dragonfly » qui repose sur une centralisation massive de bases de données civiles et policières, couplée à des recherches « en live » à partir d'un réseau de 35.000 caméras disposées à Budapest.

L'implémentation de la reconnaissance faciale à des fins d'investigation judiciaire au sein des Etats membres de l'UE



Le coronavirus, un accélérateur

Il apparaît également de plusieurs exemples cités que la crise sanitaire liée au covid a stimulé le recours à des technologies biométriques à des fins de surveillance. A Paris, un projet expérimental de surveillance du port du masque a par exemple rapidement été recalé par l'autorité française de protection des données numériques, mais il s'est finalement vu légitimé par un décret adopté en mars 2021. La Hongrie, encore elle, a été plus loin encore, en mettant au point une application (HKR) reposant sur la reconnaissance faciale pour vérifier le respect des quarantaines à domicile – les sujets à la quarantaine étant sommés de s'identifier par photo (l'image étant ensuite analysée et recroisée avec une base de données) et de se géolocaliser en même temps, afin de prouver leur présence à leur domicile.

Comme le notent les auteurs de l'étude, « il est intéressant dans ce cas de constater que l'application HKR a été "offerte" au gouvernement par Asura Technologies », l'entreprise à l'origine de son développement. Une marque de générosité de la part du privé qui ne fait pas figure d'exception : les auteurs identifient effectivement une série d'autres exemples où des dispositifs technologiques ont été « offerts » à des municipalités – ainsi, la firme chinoise Huawei a gracieusement livré plus de 200 caméras « intelligentes » à la Ville de Valenciennes en 2017.

Alors que le flou législatif actuel au niveau européen a facilité la mise en place d'un certain nombre de ces projets, le Parlement de l'UE devra très prochainement étudier la proposition de règlement sur l'intelligence artificielle émise par la Commission. Laquelle s'inscrit dans une perspective générale d'interdiction de la reconnaissance faciale « en live », moyennant néanmoins un certain nombre d'exceptions pour des cas « strictement nécessaires ». En attendant, le Contrôleur européen de la protection des données (CEPD), organe sous mandat des instances de l'UE, se pose lui-même en partisan d'un moratoire sur l'utilisation de cette technologie à des fins sécuritaires.

Tandis que certains acteurs de la société civile, à l'instar du réseau d'ONG EDRi (European Digital Rights), se posent en faveur d'une interdiction pure et simple.

Saskia Bricmont « On est à un moment clé »

© DR

ENTRETIEN

A.SE.

Commanditaire avec son groupe politique du rapport susmentionné et membre de la commission des Libertés civiles, de la Justice et des Affaires intérieures (LIBE) au Parlement européen, l'eurodéputée écologiste Saskia Bricmont (Les Verts/ALE) suit de près les travaux relatifs à l'encadrement des technologies de reconnaissance biométrique. Elle se pose par ailleurs en faveur d'une interdiction de la reconnaissance faciale à des fins sécuritaires.

Est-on à un moment charnière concernant le déploiement de la surveillance par reconnaissance faciale en Europe ?

Je pense effectivement qu'on est à un moment clé. On voit bien au travers de l'étude qu'en Europe se met en marche une série de développements d'expériences, souvent en dehors de tout cadre légal, ce qui en général mène à leur suspension ou annulation par les autorités de protection des données de plusieurs pays. Pendant ce temps, les dispositifs restent souvent en place, quand bien même hors d'usage. Donc, tout est prêt pour que ça ait lieu. Les technologies sont là, les bases de données toujours plus croisées aussi, avec des croisements de données criminelles et non criminelles. Tout permettrait d'y arriver si on ne légifère pas.

Finalement, le sujet ne semble pas faire l'objet d'un débat brûlant…

Je pense que c'est parce qu'il est largement méconnu et mal documenté. En tout cas il n'est pas sur la place publique. On a déjà normalisé le fait que nos smartphones utilisent nos empreintes digitales ou même des dispositifs de reconnaissance biométrique de manière large pour accéder à certains services. Petit à petit, on a déjà habitué les gens à se passer de leur vie privée et à ne plus protéger leurs données personnelles. Tout ça concourt au fait que l'industrie technologique profite de cette absence de contestation, qui pour l'instant reste essentiellement le fait d'organisations de la société civile.

Où en est-on sur le plan législatif, au niveau européen ?

Il y a 15 jours, en séance plénière du parlement européen, on a adopté un rapport sur l'utilisation de l'intelligence artificielle en droit pénal, où très explicitement le Parlement a pris position pour l'interdiction de la reconnaissance biométrique à des fins policières et de surveillance. C'est important d'avoir ce positionnement-là car les travaux vont justement démarrer au niveau parlementaire. Cette position est intéressante en soi, elle pose le principe d'une interdiction, ce qui est une bonne chose, mais elle introduit des exceptions pour le recours à des techniques de reconnaissance faciale pour des situations spécifiques, comme la présomption d'une menace spécifique, la détection ou l'identification de personnes, etc. Pour nous, ces exceptions au principe d'interdiction amènent finalement à l'autorisation. Car une fois que la technologie est instaurée, il va être difficile de s'assurer qu'elle n'est utilisée que pour ces cas exceptionnels spécifiquement prévus.