

Résumé

Les citoyens et la biométrie.

Techniques biométriques pour contrôler l'accès : qu'en pense le citoyen ?

Les premières applications biométriques remontent déjà à la préhistoire. L'empreinte digitale était alors utilisée pour sceller les accords commerciaux. La révolution agricole et les révolutions industrielles opérées du 17^e au 21^e siècle ont conduit à l'automatisation des techniques biométriques. La mise en œuvre de ces techniques a connu son apogée à la suite des attentats du 11 septembre 2001. Depuis, on croit fermement que la technologie accroît la sécurité et peut mettre fin à la criminalité.

La biométrie est un ensemble de techniques permettant de mesurer ou de déterminer les caractéristiques corporelles d'une personne ou d'un individu. Il existe différentes techniques biométriques ; il convient de faire une distinction entre les techniques physiologiques liées aux mécanismes naturels des êtres vivants et les techniques comportementales qui se rapportent plutôt à une activité ou au comportement d'un individu. Les empreintes digitales, la géométrie de la main, la reconnaissance du réseau, la reconnaissance faciale et le scan de l'iris sont des exemples de techniques physiologiques. La reconnaissance vocale, le scan du clavier et l'analyse des signatures sont des exemples de techniques comportementales. Beaucoup de ces techniques ont une longue histoire. L'automatisation de la technique biométrique, telle que l'empreinte digitale ou le scan de l'iris, naît souvent d'une réaction ou d'un dysfonctionnement d'une autre technique d'identification.

Les techniques biométriques sont de plus en plus employées dans divers secteurs. L'un des principaux utilisateurs est le secteur financier ; la biométrie est également fréquemment utilisée dans le domaine de la migration. Les autres secteurs qui ont recours à cette technologie sont les services publics, sanitaires, la défense, les sciences légales et le secteur commercial.

L'utilisation des techniques biométriques doit tenir compte du cadre législatif. Les dispositions législatives relatives aux données biométriques sont réglementées aux niveaux international et national. Au niveau international, le règlement général sur la protection des données s'applique, ainsi que la législation du Conseil de l'Europe et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Au niveau national, la loi belge sur la protection des données et certains articles de la Constitution sont en vigueur.

L'utilisation croissante des techniques biométriques et du cadre législatif a donné lieu à toutes sortes de discussions. Les partisans insistent sur l'amélioration de l'efficacité et de la sécurité, tandis que les opposants soulignent l'importance de la protection de la vie privée. Des principes tels que la souhaitabilité, la proportionnalité... sont soulevés par les critiques et le « stockage » des données dans une base de données est une source de discussion. En outre, il existe des réserves quant à la mise en œuvre des techniques biométriques et l'on évoque

fréquemment des « dérives » comme en Chine, par exemple, où les contrevenants routiers sont identifiés par reconnaissance faciale et leur portrait est rendu public. La culture de la honte est ainsi promue.

Néanmoins, la mise en œuvre de nouvelles technologies est de plus en plus jugée comme nécessaire pour se protéger contre les risques grandissants. L'utilisation de nouvelles technologies est légitimée en ce sens parce que notre société doit être protégée contre tout risque concevable (Vermeersch & De Pauw, 2017). Cette soif de contrôle a également fait l'objet de critiques. D'une part, plusieurs scientifiques signalent que la société occidentale est de plus en plus confrontée à une surprotection, à une culture de la peur et à l'idée que « les nouvelles technologies permettent de nouvelles formes de surveillance et qu'elles doivent donc être implémentées ». D'autre part, on parle de « l'érosion silencieuse de la vie privée » en raison de l'utilisation croissante de nouvelles technologies par les organismes privés/publics et les gouvernements dans une zone grise.

Néanmoins, nous observons un usage croissant de ces technologies car leur utilisation n'est pas toujours connotée négativement. De plus en plus de voix s'élèvent pour souligner l'importance de ces nouvelles formes de surveillance, selon Vermeersch & De Pauw (2017). C'est pourquoi de plus en plus de recherches sont menées sur l'adhésion sociale et l'acceptabilité de ces technologies.

L'institut Vias n'élabore pas seulement quelques enquêtes de perception - dans lesquelles les citoyens sont interrogés sur l'adhésion sociale et l'acceptabilité de la technologie - mais interroge également 1000 citoyens sur l'utilisation des techniques biométriques. Les citoyens connaissent-ils la biométrie ? Que pense le citoyen de la biométrie ? Dans quelle mesure la biométrie est-elle acceptée et à quel point cette acceptation l'est-elle ? Que pensent les gens de la reconnaissance d'empreintes digitales comme forme de contrôle d'accès ? Où la reconnaissance d'empreintes digitales peut-elle être appliquée ? Quels acteurs sont autorisés à utiliser quelles formes de biométrie ? Quid du respect de la vie privée ? Y a-t-il une volonté d'échanger sa vie privée contre plus de sécurité ?

Un premier constat important est que les connaissances varient en fonction de la technique. La technique biométrique la plus connue est celle des empreintes digitales, puisque pas moins de 85% des personnes interrogées déclarent connaître cette technique et savoir ce qu'elle renferme. Ce résultat de recherche est confirmé par d'autres études (ex. : Krupp, Rathgeb & Busch, 2013 ; Ada Lovelace Institute, 2019). La reconnaissance faciale occupe la deuxième place, la reconnaissance vocale la troisième place et la technique la moins connue semble être la reconnaissance de l'empreinte palmaire. Lorsque nous examinons les variables de base, nous constatons que les répondants âgés de 18 à 34 ans ont souvent une meilleure connaissance de ces techniques biométriques et savent ce qu'elles signifient par rapport aux autres catégories d'âge.

La connaissance d'une certaine technique est également fondamentale en termes d'acceptabilité. Plus on est familiarisé avec une technique particulière, plus elle est acceptée (Koops & Vedder, 2001 ; Dinev, Masssimo, Hart, Christian, Vincenzo, 2005). Notre enquête montre que l'acceptabilité est la plus élevée pour la reconnaissance des empreintes digitales, qui est aussi la technique la plus connue. Le scan de l'iris arrive en deuxième position, la reconnaissance de l'empreinte palmaire occupe la troisième position et la technique de reconnaissance faciale arrive en quatrième place. Les scores de non-acceptabilité les plus

élevés se situent au niveau de la reconnaissance vocale. Il est frappant de constater que la reconnaissance des empreintes digitales et de l'iris est principalement acceptée par les personnes de plus de 55 ans comme forme de contrôle d'accès.

C'est pour le déverrouillage du smartphone que la propension à utiliser l'empreinte digitale comme forme de contrôle d'accès est la plus importante (81,4 %). Ensuite, l'entreprise dans laquelle l'on travaille est citée et en troisième position vient l'aéroport. La raison pour laquelle le déverrouillage du smartphone obtient un score élevé est probablement due à son utilisation fréquente. Après tout, c'est une pratique très courante.

Si cette propension est liée à la variable de base « âge », on constate que les 18-34 ans sont moins enclins que les +34 ans à utiliser leurs empreintes digitales pour accéder à « l'entreprise où travaillent les autres », à un « club sportif », à « un stade de football ou autre », à « un festival de musique » et à « des établissements scolaires ». La réticence à utiliser leurs empreintes digitales pour avoir accès aux « transports en commun tels que le train, le tram, le métro et le bus », au « centre commercial » et au « parking public » est encore plus marquée chez les 18-34 ans.

Selon les personnes interrogées, la police devrait pouvoir utiliser le plus souvent la technologie et les techniques biométriques. 81,4% affirment que la police peut utiliser des caméras, 80,1% trouvent qu'elle peut utiliser les empreintes digitales, 59,2% estiment que c'est le cas pour la reconnaissance faciale et 52,6% signalent qu'elle peut utiliser le scan de l'iris. Cela s'explique par la confiance dans la police. Il existe un lien entre l'acceptation et la confiance, et les études démontrent que la confiance dans la police est très élevée (Verwee, 2012). Les répondants qui font confiance aux autorités publiques sont plus susceptibles d'accepter l'utilisation de la technologie par ces autorités (Vermeersch & De Pauw, 2017 ; Van den Broek, Ooms, Friedewald, van Lieshout & Rung, 2017 ; Mitrou, Drogkaris & Leventakis, 2017 ; Snijders, Biesiot, Munnichs & van Est, 2019 ; Institut Ada Lovelace, 2019). L'intérêt public - comme le renforcement de la sécurité ou de la protection - est plus fondamental pour le citoyen dans le processus d'acceptation de la reconnaissance faciale que l'intérêt commercial. Les citoyens sont moins enthousiastes lorsque les entreprises privées utilisent de telles techniques. Ils se posent plus de questions sur l'applicabilité, l'éthique, la vie privée, la collecte de données...

L'attitude la plus sceptique à l'égard de l'utilisation de la technologie se retrouve au niveau des médias sociaux. 61 % affirment que les médias sociaux ne devraient utiliser aucune de ces techniques.

La majorité des répondants, soit 57,5 %, est disposée à échanger sa vie privée contre plus de sécurité. Les réponses extrêmes obtiennent de moins bons résultats : les gens sont « plutôt disposés » ou « plutôt pas disposés » à échanger leur vie privée contre plus de sécurité. Si nous croisons ces résultats avec la question de l'acceptabilité, nous remarquons que les répondants qui acceptent les techniques biométriques sont plus enclins à échanger leur vie privée contre la sécurité. Cela signifie que ceux qui n'acceptent pas la technologie sont généralement moins disposés (ou pas disposés) à échanger leur vie privée au profit de la sécurité. Enfin, en ce qui concerne la vie privée et la sécurité, il est important que la recherche européenne (Pavone, Santiago & Degli-Esposti, 2015) indique que les citoyens veulent la sécurité et le respect de leur vie privée et non la sécurité aux dépens de leur vie privée.