Instaurer la confiance vis-à-vis du contrôle d'accès biométrique

 # CONTRÔLE D'ACCÈS

POSTÉ LE 12.03.21

Alors que les entreprises se tournent de plus en plus vers la biométrie pour sécuriser et fluidifier le contrôle d'accès, elles se heurtent régulièrement à un même écueil : apaiser les inquiétudes de ceux qui pourraient se méfier de cette technologie « futuriste ». Même si la plupart des gens ne sont pas toujours au courant des spécificités concernant la confidentialité des données biométriques et des aspects réglementaires qui s'y rapportent, des processus très rigoureux sont en place pour protéger les données personnelles des employés, des clients et des visiteurs de passage.

Combattre les idées reçues sur les données biométriques

Tout d'abord, il est important de comprendre que les appareils et systèmes biométriques n'utilisent que des *gabarits* biométriques (ce qu'on appelle des « *templates* » en anglais). **Ils ne stockent pas des images entières d'empreintes digitales ou de visages**, comme beaucoup pourraient le penser. Chaque gabarit consiste en une sélection de points aléatoires d'une empreinte digitale ou d'un visage. Ces points sont chiffrés et stockés de manière anonyme.

Cela signifie que si une personne non autorisée parvenait à pénétrer dans le système d'une entreprise, les données volées seraient inexploitables. **Il est impossible de reconstituer l'empreinte digitale ou le visage complet d'un employé** avec les points en question. De même, les entreprises ne peuvent pas recouper les gabarits biométriques des employés avec les registres nationaux ou toute autre base de données externe. En bref, le gabarit sécurisé ne sert qu'à une seule chose : identifier l'employé sur site et lui accorder l'accès. Cela s'arrête là.

Protéger la confidentialité des données biométriques et orienter les pratiques des entreprises

Que les employés se rassurent, leurs données sont également protégées par **plusieurs réglementations nationales et internationales**. L'une des plus récentes, et peut-être celle qui a la plus grande portée, est le Règlement Général sur la Protection des Données (RGPD). Les entreprises doivent se conformer à ces directives légales, mises en place pour donner aux citoyens européens le contrôle de leurs données personnelles. L'une des règles clés du RGPD est que **les employés doivent donner leur consentement explicite** pour l'utilisation de leurs données biométriques et peuvent retirer celui-ci à tout moment.

Le RGPD exige que les entreprises **prouvent la nécessité d'un contrôle d'accès biométrique** dans leurs locaux, par le biais d'une analyse d'impact sur la protection des données (DPIA). En conduisant cet audit, elles devront notamment expliquer pourquoi elles ont besoin de la biométrie pour la gestion de l'identité, quels appareils elles utiliseront et comment ces appareils seront déployés, mais aussi comment elles collecteront et protégeront les données. Elles devront également fournir une liste détaillée des personnes qui pourront accéder aux données.

L’ensemble de ces mesures contribue non seulement à rassurer les employés, mais aussi à garantir que les entreprises utilisent et stockent les données correctement et conformément aux normes locales et internationales les plus strictes.