L’authentification biométrique en entreprise

Sommaire

1. Introduction

Contexte et importance de la biométrie en entreprise

L'utilisation de la biométrie en entreprise est de plus en plus courante afin d'accroître la sécurité et d'optimiser l'efficacité des processus d'authentification. Elle se base sur la reconnaissance des personnes grâce à différents traits (empreintes digitales, identification faciale, rétine...). En effet, elle facilite l'identification des employés, rendant les processus plus aisés tout en réduisant l'usage de mots de passe, généralement exposés à des risques. Cependant, sa mise en œuvre pose des questions relatives à la protection des données individuelles et au respect des normes, telles que le RGPD en Europe.

Dans ce dossier, nous étudierons les éléments suivants :

- la définition de la biométrie,
- les technologies qu'elle utilise,
- ses usages dans le monde professionnel,
- les avantages et inconvénients de son utilisation,
- ses limites,
- les aspects légaux de son utilisation.

2. Définition de la biométrie

Explication du concept

La biométrie désigne l'ensemble des caractéristiques permettant d'identifier distinctement des individus (ex : empreintes digitales, visage, voix…).

Elle est utilisée pour contrôler les accès des utilisateurs à des ressources ou des lieux soumis à une authentification, par exemple un bâtiment ou un poste de l'entreprise.

Différenciation entre biométrie physiologique et comportementale.

Il existe différents types de biométrie :

- La biométrie physiologique : Elle utilise des caractéristiques physiques telles que les empreintes digitales, le visage, la voix ou encore les yeux. Elle se base sur des mesures issues de l'ensemble de vos caractéristiques corporelles (taille de la main, yeux, forme du visage…). Généralement ces caractéristiques sont fixes hormis lors de l'enfance.
- La biométrie comportementale : A l'inverse de la biométrie physiologique, les données utilisées par la biométrie comportementale sont dynamiques et vouées à changer régulièrement. Cela inclut la gestuelle, votre manière de vous déplacer, les mouvements de votre signature, ou encore votre démarche.

3. Les différentes technologies biométriques

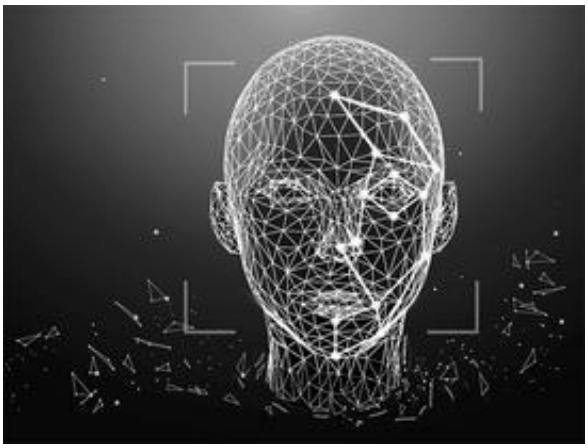
Empreinte digitale...

Il existe différents moyens d'authentification biométrique, notamment les lecteurs d'empreintes digitales, la reconnaissance faciale, les scanners rétiniens, l'identification du réseau veineux et la reconnaissance vocale.

Comparaison des technologies (précision, rapidité, coûts, acceptabilité...).

La reconnaissance d'empreintes digitales : Elle analyse la surface du doigt et vérifie si le paterne correspond à l'enregistrement effectué. Cependant les enregistrements peuvent être répliqués bien que cryptés selon l'emplacement dans lequel il est situé (machine locale, serveur d'entreprise…). De plus, la vérification peut être contournée en utilisant le « spoofing », consistant à tromper le détecteur d'empreintes en utilisant des répliques de l'empreinte. Cela peut causer des problèmes pour les personnes nées avec une mutation génétique empêchant la formation de paternes sur les doigts à leur naissance. Elle engendre peu de coûts et est facile à utiliser.

La reconnaissance faciale : Elle analyse les différentes parties du visage et vérifie si les formes, les emplacements et les tailles correspondent à l'enregistrement stocké. Cependant elle est facilement contournable car utilise des approximations pour fonctionner. Ainsi, si une personne possède des caractéristiques physiques similaires aux vôtres, elle pourra tromper la vérification. L'exemple le plus courant est celui des jumeaux.



L’analyse d’iris : Cette méthode consiste à scanner un iris afin d’en déterminer ses caractéristiques. Les résultats sont alors cryptés puis la vérification s’effectue. Ce moyen d’authentification est très sécurisé. Cependant elle est peu utilisée car la lumière utilisée pour le scan peut causer des dommages pour les personnes ayant des problèmes de vue. De plus, le scan nécessite d’adopter une certaine position. Cette méthode est relativement coûteuse à mettre en place.

Le scan du réseau veineux : Les branches des veines et leurs terminaisons sont capturées sous forme d’images cryptées. Cette technique est plus sécurisée que la reconnaissance d’empreintes digitales car les veines sont situées sous la peau, rendant la falsification difficile voire impossible. Elle est peu connue du grand public et coûte relativement cher à installer.

4. Les usages de la biométrie en entreprise

Authentification physique : contrôle d’accès aux bâtiments, sécurisation des locaux sensibles.

L’intégration de systèmes biométriques aux portes d'entrée des locaux ou encore aux terminaux d'accès aux ordinateurs permet ainsi aux entreprises de stratégiquement restreindre l'accès aux personnes autorisées, réduisant ainsi les risques de cambriolage, de vol, d'intrusion ou d’utilisation frauduleuse de données.

Les données biométriques sont particulièrement difficiles à falsifier, ce qui renforce considérablement la fiabilité du système de contrôle d'accès. La biométrie offre de plus un suivi précis des mouvements du personnel, permettant aux entreprises de savoir qui a accédé à quel endroit et à quel moment, un atout de taille pour les entreprises qui gèrent des zones sensibles ou qui doivent respecter des réglementations strictes en matière de sécurité.

Authentification logique : connexion aux systèmes d'information, gestion des accès.

Le contrôle d'accès logique est un système de contrôle d'accès à un système d'information. Il est souvent couplé avec le contrôle d’accès physique et permet de restreindre le nombre d’utilisateurs du système d’information.

Au sein de leurs structures, les entreprises gèrent des informations sensibles. Ces informations sont conservées soit dans des bases de données numériques, soit de manière physique dans des locaux. Cela implique que l'accès à ces informations ne soit pas disponible pour tous. Dans ce but, les entreprises instaurent des contrôles d'accès logiques. Dans les entreprises, l'établissement de comptes utilisateurs à l'aide de mots de passe, via la distribution de badges électroniques ou encore par le biais d'une vérification biométrique est couramment pratiqué.

L'accès complet ou partiel au système d'information de l'entreprise peut être déterminé en fonction du rôle d'un employé au sein de l'organisation. Par exemple, dans un système intégré de gestion, certaines fonctions sont attribuées aux comptables tandis que d'autres, comme l'accès aux contrats de travail, restent inaccessibles.

Cas d'usage spécifiques : signature biométrique, paiement sécurisé, surveillance.

Les fonctionnalités biométriques intégrées dans les smartphones et autres appareils mobiles, telles que la reconnaissance faciale, les empreintes digitales et la reconnaissance vocale, permettent aux utilisateurs de déverrouiller leurs appareils de

manière sécurisée et d'authentifier les transactions sans avoir à saisir de mots de passe ou de codes PIN.

5. Avantages de la biométrie

Les principaux avantages et inconvénients de l’authentification biométrique sont :

- Sécurité renforcée : Les caractéristiques biométriques sont uniques à chaque individu, ce qui assure une protection de haut niveau contre les intrusions non autorisées

- Unicité des identifiants biométriques : Contrairement aux mots de passe ou aux cartes d'identité, les caractéristiques biométriques ne peuvent pas être facilement falsifiées ou partagées

- Amélioration de l'expérience utilisateur : L'authentification biométrique offre une méthode rapide et conviviale pour vérifier l'identité des utilisateurs, éliminant ainsi le besoin de se souvenir de mots de passe complexes ou de transporter des cartes d’identité

- Réduction de la fraude : Les techniques biométriques réduisent les risques de fraude liés à l'usurpation d'identité ou à l'utilisation de mots de passe volés

- Traçabilité accrue : Les données biométriques permettent de tracer plus facilement les interactions des utilisateurs avec les systèmes, ce qui peut s’avérer très utile dans les enquêtes judiciaires ou pour lutter contre la fraude de manière générale

6. Risques et limites de la biométrie

Bien que présentant de nombreux atouts, la biométrie n’est pas infaillible et présente des inconvénients :

- Protection de la vie privée : La collecte et le stockage des données biométriques peuvent soulever des préoccupations quant à la confidentialité et à la protection des informations personnelles

- Risques de fausses acceptations et rejets : Il existe un risque que le système biométrique accepte une personne non autorisée ou rejette un utilisateur légitime, ce qui peut compromettre la sécurité (même si le risque reste faible)

- Sécurité de l’accès au système : En cas de fausse acceptation ou de rejet, la sécurité du système peut être compromise, notamment dans les secteurs d’activités sensibles type industrie pharmaceutique ou défense

- Coût initial élevé : La mise en place d'un système biométrique peut nécessiter des investissements importants en termes d'infrastructures et de technologies

- Dépendance à la technologie : Les systèmes biométriques restent sensibles aux pannes techniques, ce qui peut entraîner des problèmes d'authentification en cas de dysfonctionnement

7. Fiabilité et failles des systèmes biométriques

Les systèmes biométriques, utilisés pour authentifier les individus via des caractéristiques physiques ou comportementales, présentent des avantages en termes de sécurité et de commodité. Cependant, leur fiabilité est sujette à caution en raison de diverses vulnérabilités. Par exemple, des chercheurs ont démontré que les systèmes de reconnaissance faciale peuvent être trompés par des photographies ou des vidéos, compromettant ainsi leur intégrité.

De plus, des biais algorithmiques ont été identifiés, rendant ces systèmes moins précis pour certaines populations, notamment les femmes et les personnes à la peau foncée. En 2018, une étude a révélé que les principaux systèmes de reconnaissance faciale affichaient des taux d'erreur plus élevés pour ces groupes démographiques.

Par ailleurs, des hackers comme Jan Krissler, alias Starbug, ont démontré la possibilité de reproduire des empreintes digitales à partir de photographies haute résolution, mettant en évidence les failles des systèmes d'identification biométrique.

Ces exemples illustrent que, malgré leur potentiel, les technologies biométriques nécessitent des améliorations continues pour assurer une sécurité et une fiabilité optimales.

8. Cadre légal et réglementaire

Les dispositifs biométriques mettent en danger la vie privée et la protection des données. En enregistrant ces informations dans un système informatique, on crée des failles de sécurité multiples et bien réelles. Si les données biométriques (les empreintes, les voix ou encore les traits du visage de personnes) d'une société ou d'une collectivité sont dérobées et/ou dupliquées, les conséquences seraient bien plus graves que lors d'un hacking « classique ».

Le grand danger de l'authentification biométrique est le risque d'usurpation d'identité à long terme.

En France, la collecte de données sensibles doit respecter le règlement général sur la protection des données (RGPD), mais aussi la loi Informatique et Libertés. Concrètement, le traitement ne doit être réservé qu'à des cas particuliers, et doit être réalisé avec le consentement des personnes.

En France, la Défenseure des droits réclame un meilleur encadrement des systèmes biométriques. Elle demande un contrôle régulier de la protection des données. Par ailleurs, la loi RGPD, entrée en application le 25 mai 2018, a profondément affecté le cadre juridique existant.

L'utilisation de procédés biométriques ne dépend pas uniquement de la simple volonté des entreprises puisque la CNIL limite leur installation. Avant la mise en place, les organismes, publics ou privés, doivent au préalable, soit obtenir son autorisation soit fournir une déclaration de conformité, dans des situations spécifiquement prévues par la CNIL. Les entreprises devront justifier leur choix en démontrant la finalité du dispositif mis en place. Il ne pourra s'agir uniquement que de contrôler l'accès à des locaux, aux ordinateurs ou aux applications informatiques. Elles devront également expliquer les raisons pour lesquelles elles ont préféré avoir recours aux données biométriques plutôt qu'à d'autres dispositifs d'identification (badges, mot de passe, …). Une analyse d'impact relative à la protection des données devra aussi être fournie afin d'identifier les risques pour les droits et libertés des salariés notamment en matière d'atteinte à la vie privée. De plus, la CNIL précise que les salariés devront être informés par écrit de la mise en place d'un système biométrique avant le recueil des données. L'entreprise doit certes les informer, mais elle n'a pas l'obligation d'obtenir leur consentement puisque le traitement des données biométriques peut être justifié par l'intérêt légitime de l'employeur. Cependant, les salariés ont le droit de s'y opposer selon l'article 21 du RGPD.

Les données biométriques sont des données « sensibles » selon le RGPD, elles doivent donc être protégées. Les risques de piratage, de vol ou d'usurpation auraient de graves conséquences. C'est pourquoi les entreprises doivent garantir un niveau de protection élevé en limitant par exemple l'usage de ces données ou en mettant à jour régulièrement les appareils électroniques. Ces données doivent être

enregistrées dans des fichiers sécurisés et permettre une identification rapide. La CNIL limite le nombre de personnes ayant accès à ces données. En effet, « seules peuvent avoir accès aux données biométriques les personnes qui sont limitativement habilitées en raison de leurs fonctions à gérer l'enrôlement de la personne concernée, à supprimer les gabarits ou à assurer la maintenance du dispositif ». Cependant, aucun système n’est infaillible et le risque est présent. Il est donc conseillé aux entreprises de coupler les données biométriques avec un mot de passe ou une solution d’authentification bifactorielle ou multifactorielle pour plus de sécurité.

Sources

https://www.cnil.fr/fr/les-dispositifs-de-biometrie-sur-le-lieu-de-travail

https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2021/la-biometrie-un-outil-en-constante-evolution-dans-les-entreprises

https://www.thalesgroup.com/fr/markets/digital-identity-and-security/government/inspired/what-are-physiological-biometrics

https://www.thalesgroup.com/fr/markets/digital-identity-and-security/government/inspired/what-are-behavioral-biometrics

https://recogtech-com.translate.goog/en/insights-en/5-common-biometric-techniques-compared/

https://www.signicat.com/fr/blog/utilisation-de-lauthentification-biometrique-pour-garantir-lidentification

https://fr.wikipedia.org/wiki/Contrôle_d%27accès_logique

https://rendre-notre-monde-plus-sur.goron.fr/donnees-biometriques-menace-ou-securite