CONTRÔLE D'ACCÈS

Reconnaissance du réseau veineux, une biométrie allégée

La Cnil a assoupli les formalités pour la mise en œuvre de dispositifs sécuritaires biométriques, telle la reconnaissance du réseau veineux.

EMMANUEL WALLE, AVOCAT, ALAIN BENSOUSSAN-AVOCATS

L'ENJEU

> Distinguer les autorisations délivrées par la Cnil selon qu'il s'agisse d'un dispositif à empreinte digitale ou d'une identification effectuée par le réseau veineux.

LA MISE EN ŒUVRE

> Adresser à la Cnil un engagement de conformité.

CRÉDIT

Vidéosurveillance, géolocalisation et biométrie font désormais partie de la panoplie sécuritaire des espaces privés ou publics. Aujourd'hui, l'accès à une salle d'examen ou à un bloc opératoire peut ainsi être soumis à l'obligation de scanner le réseau veineux palmaire du candidat ou du personnel médical (délib. 2009-360 du 18/6/09 et 2009-174 du 26/3/09). En application de la loi Informatique et libertés (6/1/78, modifiée en 2004), les dispositifs de reconnaissance biométrique sont, pour la plupart, soumis à une autorisation préalable de la Cnil. Or, cette dernière vient d'alléger les formalités d'autorisation pour la mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main, privilégiant ainsi les dispositifs d'identification sans contact (délib. 2009-316 du 7/5/09 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail). Encore faut-il que cette technique ne soit affectée qu'au contrôle de l'accès des locaux sur le lieu de travail. La société, qui souhaite s'équiper d'un tel dispositif dans le respect des dispositions de la décision unique n° AU-019, doit adresser à la Cnil un engagement de conformité.

La biométrie regroupe les techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Ces données sont ainsi considérées comme des données à caractère personnel, permettant d'identifier une personne de manière irrévocable. Or, selon la loi Informatique et libertés, tous les traitements comportant des données biométriques doivent faire l'objet d'une autorisation préalable de la Cnil.

Parmi les données biométriques utilisées aujourd'hui, la Cnil considère l'empreinte digitale comme une donnée à risque dont la diffusion, non maîtrisée ou accidentelle, peut avoir des conséquences irrémédiables pour les personnes. Contrairement à tout autre identifiant (code, mot de passe), l'empreinte digitale ne peut être modifiée une fois collectée, ce qui impose d'en limiter l'usage pour éviter une usurpation d'identité presque « parfaite ». Cette « biométrie à trace » est donc particulièrement encadrée par la Cnil qui, l'an dernier, a refusé d'autoriser plusieurs dispositifs ne pouvant justifier d'un fort impératif de sécurité. Pour la Cnil, confier ses données biométriques à un tiers doit répondre à une nécessité a priori exceptionnelle et être entourée de garanties sérieuses.

Cette technologie doit tout d'abord présenter certaines caractéristiques techniques (chiffrage de l'enregistrement du gabarit veineux ou possibilité d'associer d'autres données d'identification – nom, prénom, photographie – au gabarit du réseau veineux du doigt). La Cnil précise que le gabarit veineux doit être enregistré dans la mémoire du lecteur biométrique ou sur un support individuel sécurisé. La durée de conservation des données doit être fixée (de trois mois à cinq ans selon les cas). Le responsable du traitement doit également prendre « toutes les précautions utiles pour préserver la sécurité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance » (Art. 34 loi du 6/1/78 modifiée). Enfin, l'information des employés et des instances représentatives du personnel doit être effectuée avant la mise en œuvre effective du dispositif biométrique, au risque d'une peine pouvant atteindre 300 000 euros d'amende et cinq ans de prison.

Jurisprudence

ACCIDENT DU TRAVAIL

L'employeur ne peut pas demander une expertise pour trancher la contestation avec la CPAM sur le caractère professionnel d'un accident.
(Cass. Civ 2, 4.2.2010, N° 213, Kereol c/ CPAM du Morbihan)

VIOLENCE AU TRAVAIL

Les salariés victimes de violences de leur patron ou d'un collègue peuvent demander une indemnisation au Fonds de garantie des victimes d'infractions.
(Cass. Civ 2, 4.2.2010, N° 207, Guebouli c/ Fonds de garantie des victimes d'infractions)

TRANSFERT DU CONTRAT

En cas de cession d'entreprise, le salarié bénéficie aussitôt de la convention collective du cessionnaire, mais garde les dispositions plus favorables de l'ancien accord.
(Cass. Soc, 10.2.2010, N° 323, Mecasem c/ Legros)

CHSCT

Le CHSCT ne peut pas recourir à une expertise lorsqu'un projet de réorganisation n'est pas de nature à modifier les conditions de santé, de sécurité ou de travail des salariés.
(Cass. Soc, 10.2.2010, N° 325, CHSCT Nextiraone c/ Nextiraone France)

MAÎTRE D'ŒUVRE

Le maître d'œuvre qui installe un matériel est tenu d'une obligation de résultat à l'égard du maître d'ouvrage.
(Cass. Com, 16.2.2010, N° 205, Somival c/ CMCIC et a.)