

Utilisation des données biométriques des employés

Eva Cellina, le 30 mai 2021

L'autorité italienne de protection des données (GPDP) inflige une amende de EUR 30'000.- pour l'utilisation d'un système de gestion du temps de présence basé sur le traitement des données biométriques des employés.

Garante per la protezione dei dati personali (GPDP), Ordinanza ingiunzione nei confronti di Azienda sanitaria provinciale di Enna, 14 janvier 2021 [9542071]

L'autorité sanitaire de la province d'Enna (« ASP Enna »), en Sicile, avait adopté un système permettant le traitement des données biométriques de ses employés pour la détection des présences. Il devait permettre une plus grande fiabilité technique de vérification de l'identité avec comme objectif connexe de décourager l'absentéisme de certains employés.

Grâce à son système, l'ASP Enna a obtenu les empreintes digitales de plus de 2'000 employés et les y a stockées de manière chiffrée sur le badge de chaque employé. L'ASP Enna procédait au contrôle d'identité de chaque employé en comparant le modèle biométrique de référence et l'empreinte digitale présentée au moment de la détection de la présence. Le numéro de l'employé, la date ainsi que l'heure de l'estampillage étaient alors transmis au système de gestion des présences.

Selon l'ASP Enna, aucun traitement de données personnelles n'était effectué par elle dans la mesure où le traitement de données personnelles ne commençait que lorsque l'employé, de par sa propre volonté, apposait son badge sur le lecteur et son doigt sur le scanner de l'appareil. L'ASP Enna considérait que le logiciel utilisé se limitait à comparer les deux données biométriques (celle stockée dans le badge et celle issue du scan de doigts), sans communiquer ces données à l'extérieur et sans les stocker d'aucune manière (à l'exception de quelques secondes au sein même du système, le temps de la comparaison).

En tout état de cause, l'ASP Enna considérait qu'un tel traitement reposait, conformément à l'art. 6 RGPD, tant sur le consentement des employés (lorsque ces derniers utilisaient effectivement ce système de contrôle) que sur une obligation légale. Sur ce point, l'autorité se référait au règlement d'application de la loi 56/2019 relatif à la prévention de l'absentéisme des employés dans le secteur public.

Suite à son enquête, le GPDP considère qu'il y a effectivement un traitement de données biométriques des employés. Le fait que l'ASP Enna ne conserve pas les données biométriques dans une base de données centralisée, mais sur des dispositifs portables (les cartes à puces détenues directement par les employés) n'est pas relevant. En effet, le GPDP considère que la phase d'enregistrement des données biométriques des employés permet à l'ASP Enna d'enregistrer les descriptions biométriques afin de pouvoir, dans un deuxième temps, les comparer à l'empreinte digitale présentée par l'employé au moment de la détection de présence dans la phase de reconnaissance. Ainsi, le GPDP considère qu'il y a un traitement de données personnelles tant dans la phase d'enregistrement que de reconnaissance.

Le stockage des données biométriques, en mode sécurisé dans des badges avec système de carte à puce confié à chaque employé, répond à un choix du responsable du traitement qui, lors de la détermination des moyens de traitement, adopte cette mesure technique et organisationnelle en application, notamment, du principe de minimisation des données traitées. Le GPDP rappelle cependant que l'adoption de cette mesure n'exclut pas l'application des règles relatives à la protection des données à caractère personnel, notamment la mise en place de dispositifs moins invasifs.

Bien que l'ASP Enna ait assuré que les employés et les syndicats aient reçu les informations prévues à l'[art. 13 RGPD](#), le GPDP considère qu'elle n'a pas suffisamment et correctement informé les employés de l'ampleur du traitement effectué et du caractère licite de ce dernier.

Le GPDP admet qu'il existe effectivement une base légale pour la détection des présences et la vérification du temps de travail. Toutefois, il précise que ladite base légale doit offrir des garanties appropriées concernant les droits et intérêts fondamentaux de la personne concernée. En d'autres termes, le traitement des données biométriques à des fins d'enregistrement du temps ne serait légitime que s'il existe une base légale spécifique, qui offre à la personne concernée des garanties en matière de respect de la vie privée, ce qui n'est pas le cas du [règlement d'application de la loi 56/2019 relatif à la prévention de l'absentéisme des employés dans le secteur public](#).

Le GPDP considère ainsi que l'ASP Enna a violé les [art. 5 par. 1 let. a](#), [6](#) et [9 RGPD](#) en raison du fait qu'il n'y a pas de motif justificatif adéquat pour le traitement des données biométriques des employés, que le consentement des employés ne peut pas être considéré comme valablement donné en raison du déséquilibre de la relation de travail, et que l'ASP Enna n'avait pas fourni d'informations adéquates sur le traitement des données biométriques des employés.

En sus de l'amende infligée, le GPDP a ordonné à l'ASP Enna de cesser d'utiliser le système de traitement biométrique qu'elle avait mis en place.

Et en Suisse ?

Si les empreintes digitales permettent d'identifier une personne déterminée ou déterminable, elles sont des données personnelles sensibles, dans la mesure où elles peuvent révéler notamment l'appartenance raciale de la personne concernée (art. 5 let. c ch. 2 LPD). Dans la nLPD, les données biométriques sont des données personnelles sensibles lorsqu'elles permettent d'identifier la personne concernée de manière univoque (art. 5 let. c ch. 4 nLPD).

L'employeur, responsable du traitement (maître du fichier) ne peut traiter ces données que s'il dispose d'un motif justificatif (consentement, intérêt prépondérant privé ou public ou la loi : art. 13 al. 1 LPD) ou, s'il s'agit d'un organe fédéral, si le traitement est prévu dans une base légale. À défaut, le traitement portera une atteinte illicite à la personnalité des employés.

De plus, l'utilisation par l'employeur du consentement de l'employé comme motif justificatif est très discutable, de par l'existence d'un rapport de subordination entre l'employé et l'employeur, renforcé par la nature sensible des données traitées.

Pour une analyse juridique exhaustive et plus d'informations sur les mesures qui devraient être mises en place par l'employeur dans un tel cas, voir : Stéphanie Fuld / Stéphanie Chuffart-Finsterwald, Nexus droit du travail et protection des données : quelques développements récents, in : Jusletter 12 juin 2017.

Proposition de citation : Eva CELLINA, Utilisation des données biométriques des employés, 30 mai 2021 in www.swissprivacy.law/76