racine
AVOCATS

Flash Info

10 avril 2019

La CNIL publie le premier règlement type sur le traitement des données biométriques au travail dans le cadre de sa nouvelle mission

L'alignement du droit français sur la législation européenne a été principalement effectué par la loi du 20 juin 2018 modifiant la Loi Informatique et Libertés. Dans une logique d'augmentation du pouvoir réglementaire de la CNIL[1], la loi précitée a confié à la Commission la mission suivante[2] :

« En concertation avec les organismes publics et privés représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. »

Dans ce contexte, à la suite d'une consultation publique menée du 3 au 30 septembre 2018, et dans le but d'accorder une protection particulière aux données biométriques, la CNIL publie le règlement type *« biométrie sur les lieux de travail »,* le premier acte juridique élaboré dans le cadre de sa nouvelle mission.

[1] L'Autorité de contrôle indépendante française chargée de veiller à la protection des données à caractère personnel
[2] 11, I.2, b)

Responsable de publication : Eric Barbry

Qu’est-ce que c’est une donnée biométrique ?

La donnée biométrique est une caractéristique physique ou biologique permettant d’identifier une personne (ADN, forme de la main, empreintes digitales, écartement des yeux, voix, empreintes veineuses etc.).

Conformément à l’article 9 du RGPD, le traitement des données biométriques est par principe interdit, sauf pour certaines exceptions strictement encadrées par la loi. Parmi ces exceptions figure le recours par les employeurs à des dispositifs d’identification biométrique dans le but de contrôler l'accès aux lieux de travail, aux appareils et aux applications informatiques. Considérées comme des données « sensibles » au sens du RGPD et produites à partir du corps humain, leur collecte doit être strictement réglementée. Les risques portant sur la confidentialité de telles données représentent un enjeu majeur mettant en péril la vie privée des salariés.

Champ d’application du règlement

Le règlement s’applique à tout traitement des données biométriques imposé par un employeur de droit public ou privé à ses salariés[3] en vue de contrôler les accès aux locaux, aux applications et aux outils professionnels.

Finalités du traitement

Il est vrai que le traitement des données biométriques est susceptible d’ouvrir la voie à des finalités autres que celles initialement prévues (à titre d’exemple : contrôle des horaires des salariés).
Par conséquent, la CNIL n’autorise, dans le champ dudit règlement type, le traitement de telles données que pour le contrôle d’accès aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.
De plus, dans le cadre du principe d’ « accountability[4] » introduit par le RGPD, elle oblige le responsable de traitement à justifier la nécessité d’un traitement des données biométriques et à documenter cette justification.

Information des salariés

En application de l’article 12 du RGPD, le responsable du traitement, en l’occurrence l’employeur, est tenu de fournir une information, transparente, compréhensible et aisément accessible, en des termes clairs et simples aux personnes concernées. Cette information doit être fournie individuellement à chaque salarié dans une notice écrite préalablement à la mise en œuvre du traitement.
Au-delà de cette information, les instances représentatives du personnel doivent être également informées et consultées.

[3] Salariés au sens large : employés, stagiaires, salariés intérimaires, bénévoles, personnes en service civique, agents des trois fonctions publiques, etc.
[4] Le principe d’« accountability », généralement traduit en français par « responsabilisation », exige que le responsable de traitement soit à tout moment et tout au long du traitement en mesure de documenter, démontrer et justifier sa conformité au RGPD.

Quid du consentement des salariés ?

Afin qu'un traitement soit licite[5], il doit être fondé sur une base légale (consentement, obligation légale, intérêt légitime etc.).
Pour que le consentement soit valablement recueilli, il doit être « libre » en plus d'être spécifique, éclairé et matérialisé par une action positive de la personne. Or, selon les lignes directrices adoptées par le G29 sur le consentement[6], un déséquilibre des rapports de force entre le responsable de traitement et la personne concernée peut avoir lieu dans le cadre des relations de travail. Ce déséquilibre est susceptible d'affecter le caractère « libre » du consentement. À cet égard, le G29 souligne que :
« Au vu de la dépendance résultant de la relation employeur/employé, il est peu probable que la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives suite à ce refus. »

Il ressort de ce qui précède que les employeurs peuvent avoir rarement recours au consentement en tant que fondement juridique, puisqu'il s'avère assez difficile de démontrer que celui-ci est recueilli librement.

Il est alors recommandé aux employeurs de recourir aux autres fondements juridiques : à l'obligation légale ou à l'intérêt légitime.

Sécurité du traitement

Bien que les méthodes d'authentification et d'identification biométrique promettent d'être très performantes, il y a lieu de constater qu'elles engendrent plusieurs risques lorsqu'elles peuvent poursuivre d'autres objectifs au-delà de s'assurer de l'identité des individus, et elles sont, au demeurant, facilement falsifiables.

Pour toutes ces raisons, et afin de répondre à son obligation de sécurité[7], l'employeur est tenu de mettre en œuvre toutes les mesures précisées dans l'article 10 du règlement type de la CNIL.

Analyse d'impact (PIA)

Dans le cadre du principe d'« accountability » susmentionné, le RGPD impose, le cas échéant, l'obligation de mettre en œuvre une analyse d'impact relative à la protection des données (Privacy Impact Assessment – PIA)[8]. Il s'agit d'une analyse portant sur l'évaluation des risques par rapport aux atteintes potentielles à la vie privée. L'objectif est d'aider les responsables du traitement à apporter la preuve de leur conformité et d'organiser la mise en œuvre des mesures de sécurité les plus appropriées pour assurer un niveau de sécurité élevé.

La mise en place d'une PIA n'est obligatoire que si le traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées. Étant étroitement liées au corps humain, les données biométriques requièrent une protection juridique particulière et

[5] Article 6 du RGPD
[6] https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf
[7] Article 32 du RGPD
[8] Article 35 du RGPD

leur traitement nécessite bel et bien la mise en œuvre d'une telle analyse. Celle-ci doit toujours être menée avant l'enrôlement des données biométriques des salariés.

Il est enfin à noter que le règlement constitue un dispositif juridiquement contraignant pour les employeurs. Cela signifie que, contrairement aux recommandations ou aux référentiels élaborés par la Commission, le respect d'un règlement type est obligatoire pour tous les organismes concernés.

***

Pour en savoir plus

https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

Auteurs

Eric Barbry
Avocat associé
ebarbry@racine.eu

Maria Lefe
Avocate au barreau d'Athènes

Responsable de publication : Eric Barbry