Délibération n°2018-xxx du xxx 2018 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail

La Commission nationale de l'informatique et des libertés,

Vu … ;

Vu la … ;

Vu … ;

Article premier

Objet et champ d'application du présent règlement

Conformément aux dispositions du 9° du II de l'article 8 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le présent règlement type a pour objet de fixer des exigences spécifiques applicables aux traitements de données biométriques qui sont nécessaires au contrôle par les employeurs et les administrations de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires.

Le règlement type n'a pas vocation à se substituer aux obligations générales découlant du RGPD et de la Loi « Informatique et Libertés » modifiée, mais à les compléter ou à préciser certaines d'entre elles. Les organismes mettant en œuvre de tels traitements devront ainsi respecter l'ensemble des autres exigences légales et réglementaires, relatives aux principes du traitement de données, aux droits des personnes ou aux transferts internationaux des données. En particulier, ils devront s'assurer que les traitements de données biométriques concernés sont fondés sur une base légale telle que l'exécution d'une obligation légale ou la poursuite d'un intérêt légitime, à l'exclusion notamment du consentement de la personne concernée.

Pour les besoins du présent règlement type, les données biométriques s'entendent comme les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Article 2

Finalités du traitement

Le recours aux dispositifs biométriques n'est autorisé, dans le champ du présent règlement-type, que pour les finalités suivantes :

- Le contrôle des accès à l'entrée et dans les locaux limitativement identifiés par l'organisme comme devant faire l'objet d'une restriction de circulation, à l'exclusion de tout contrôle des horaires des employés ;

- Le contrôle des accès à des appareils et applications informatiques professionnels limitativement identifiés de l'organisme, à l'exclusion de tout contrôle du temps de travail de l'utilisateur.

Article 3

Justification du recours à un traitement de données biométriques

Le responsable de traitement doit démontrer la stricte nécessité de recourir à un traitement de données biométriques en indiquant les raisons pour lesquelles le recours à d'autres dispositifs d'identification (badges, mots de passe, *etc.*) ou mesures organisationnelles et techniques de protection ne permet pas d'atteindre le niveau de sécurité exigé.

Cette justification doit :

- détailler le contexte spécifique rendant nécessaire un niveau de protection élevé.

  Par exemple, manipulation des machines ou produits dangereux, accès aux fonds ou aux objets de valeur, matériel ou produits faisant l'objet d'une réglementation spécifique – précurseurs des substances psychotropes, produits chimiques pouvant être utilisés pour la fabrication d'armes ;

- être documentée par le responsable du traitement.

Article 4

Données personnelles collectées et traitées

Les traitements faisant objet du présent règlement peuvent porter sur les données à caractère personnel suivantes :

- l'identité : nom, prénom, photographie et gabarit de la caractéristique biométrique, clé biométrique résultat du traitement des mesures par un algorithme (et non une image ou une photographie de cette caractéristique), numéro d'authentification ou numéro de support individuel, coordonnées ;
- la vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade, nom de l'employeur ;

- l'accès aux locaux : porte utilisée, zones et plage horaire d'accès autorisées, date et heure d'entrée et de sortie ;
- l'accès aux outils de travail : matériel ou applicatifs concernés, modalités d'accès autorisées, date et heure de début et de fin d'utilisation.

Constituent un « gabarit », au sens du présent règlement, les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques (empreinte digitale, forme de la main, iris, *etc.*), biologiques (ADN, urine, sang, *etc.*) ou comportementales (démarche, dynamique de tracé de signature, *etc.*) de la personne concernée, que ce soit sous forme brute (image photographique) ou dérivée.

Article 5

Destinataires des données traitées

Seules peuvent avoir accès aux données visées à l'article 5 les personnes qui y sont limitativement habilitées en raison de leurs fonctions.

Dans les limites de leurs attributions respectives ces personnes ne peuvent accéder aux gabarits que de façon temporaire et pour les stricts besoins de l'enrôlement de la personne concernée, de la suppression du gabarit ou de la maintenance du dispositif.

L'architecture du dispositif biométrique ne doit pas permettre aux destinataires d'accéder directement aux gabarits enregistrés, de les modifier ou de les copier vers un autre support.

Article 6

Choix des modalités de détention du gabarit

Le présent règlement distingue entre trois types de détention de gabarits biométriques, selon le degré de maîtrise exercé sur le support de conservation par les personnes concernées :

- Type 1 : les gabarits sous maitrise des personnes concernées sont ceux dont le seul support de stockage durable est détenu par la personne elle-même, par exemple sous forme de badge ou de carte à puce ;
- Type 2 : les gabarits sous maîtrise partagée sont ceux dont le support de stockage durable est maitrisé par l'employeur ou ses préposés, mais qui sont conservés sous une forme les rendant inexploitables en absence d'intervention de la personne concernée ;
- Type 3 : les gabarits non-maîtrisés par les personnes concernées sont ceux dont le support de stockage durable est maîtrisé par l'employeur ou ses préposés sous une forme exploitable même en absence d'intervention de la personne concernée.

Les traitements de données biométriques mis en place par des employeurs publics ou privés ne peuvent en principe utiliser que des gabarits sous maîtrise des personnes concernées (type 1).

Il ne peut être fait recours aux gabarits sous maîtrise partagée (type 2) qu'en cas d'impossibilité de mettre en place des gabarits sous maîtrise de la personne (type 1).

Il ne peut être fait recours aux gabarits non-maitrisés par les personnes (type 3) qu'en cas d'impossibilité de mettre en place des gabarits sous maitrise partagée (type 2).

La décision de recourir aux gabarits sous maîtrise partagée ou non-maîtrisés par la personne concernée, doit être documentée de manière détaillée en justifiant le choix effectué.

Article 7

Modalités et durées de conservation

Les caractéristiques biométriques ne peuvent être conservées que sous la forme d'un gabarit chiffré ne permettant pas de recalculer la donnée biométrique d'origine.

Le gabarit de la donnée biométrique associé ne peut être conservé que le temps de l'habilitation de la personne concernée et doit être supprimé à son départ ou au moment de retrait de son habilitation.

Les catégories de données relatives à l'identité, à la vie professionnelle et aux accès aux locaux, aux appareils et applications informatiques peuvent être conservées au maximum trois mois après le départ de la personne concernée ou le retrait de son habilitation.

Les éléments relatifs aux accès aux locaux, aux appareils et applications informatiques professionnels ne doivent pas être conservés plus de trois mois après leur enregistrement.

Article 8

Information des personnes

L'information obligatoire prévue par les articles 12 et suivants du RGPD doit figurer dans une notice écrite remise par le responsable de traitement à chaque collaborateur préalablement à l'enrôlement des données biométriques de ce dernier.

Article 9

Sécurité des données

Mesures existantes ou prévues

Le responsable du traitement prend toutes 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.

A cette fin, le responsable de traitement adopte les mesures suivantes ou des mesures dont il démontre l'équivalence :

Mesures relatives aux données :

- cloisonner les données lors de leur transmission et leur conservation ;
- chiffrer les données biométriques, dont les gabarits, à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art ; en particulier, une politique de chiffrement et de gestion des clés doit être clairement définie (changement des clés par défaut, algorithmes et tailles des clés conformes à l'état de l'art, renouvellement prévu, *etc.*) ;
- associer un code d'intégrité aux données (par exemple, signature ou hachage) ;
- interdire tout accès externe à la donnée biométrique (comparaison sur carte (« *match-on-card* ») ou module de sécurité physique/logique de type HSM – *Hardware Security Module*) ;
- effectuer le contrôle d'accès par une comparaison entre l'échantillon calculé et le gabarit d'enrôlement enregistré (en base interne/distante ou sur support individuel) sans copie du gabarit ;
- veiller à l'effectivité de l'effacement des données à l'issue de la durée de conservation ;
- supprimer la donnée biométrique en cas d'accès non autorisé au terminal de lecture-comparaison ou au serveur distant ;
- supprimer toute donnée non utile au traitement ultérieur lors de la fin de vie du dispositif biométrique.

Mesures relatives à l'organisation :

- responsabiliser les personnes concernées sur les bonnes conditions d'utilisation des matériels ;
- mettre à disposition un dispositif alternatif « de secours » ou utilisé à titre exceptionnel, sans contrainte ni surcoût pour les personnes n'utilisant pas la solution biométrique ; en particulier, pour les personnes ne répondant pas aux contraintes du dispositif biométrique (enrôlement ou lecture de la donnée biométrique impossible) et en prévision d'une indisponibilité du dispositif biométrique (tel qu'un dysfonctionnement du dispositif), une « solution de secours » doit être mise en œuvre pour assurer une continuité du service proposé, limitée toutefois à un usage exceptionnel ;
- tester le système selon une procédure formalisée, avant sa mise en place et après toute modification, dans un environnement dédié et sans recourir à des données réelles ;
- déterminer les actions à entreprendre en cas d'échec de l'authentification (impossible de vérifier une identité, défaut d'habilitation à pénétrer dans une zone sécurisée, *etc.*) ;
- gérer de manière stricte l'accès physique et logique aux dispositif et bases de données par les personnes habilitées ; en particulier, une politique de gestion des droits et des accès doit être clairement définie ; il s'agit de formaliser les différentes catégories de personnes habilitées (utilisateurs, administrateurs et gestionnaires de bases de données, personnes en charge de la gestion des données, personnes techniques de maintenance, *etc.*), leurs droits sur les données, la manière dont les habilitations sont gérées, la manière dont leur accès est contrôlé, la manière dont les secrets sont gérés, les traces journalisées, la manière dont les traces sont gérées, *etc.* ;
- former spécifiquement les administrateurs et personnes habilités à gérer les données (enrôlement, traitements, effacement, *etc.*) ;
- intégrer une mesure technique ou organisationnelle de détection anti-fraude ;
- prévenir les personnes concernées en cas d'accès non autorisé à leurs données ;

- formaliser, appliquer et faire connaître une procédure de secours en cas d'incident (prévoyant notamment le ré-enrôlement).

Mesures relatives aux matériels :

- mettre en œuvre des mesures permettant d'être alerté en cas de tentative d'effraction sur le lecteur ou le dispositif de stockage ; en particulier, en cas de stockage de la donnée sur une base locale intégrée au dispositif biométrique, toute tentative d'ouverture ou d'arrachement du terminal de lecture-comparaison doit être détectée, suivie d'un signalement à l'administrateur du dispositif ;
- réserver un matériel spécifique au stockage des données ;
- utiliser des matériels certifiés aux conditions d'usage et en termes de sécurité ;
- garantir la traçabilité du cycle de vie du matériel.

Mesures relatives aux logiciels :

- réserver un logiciel spécifique à l'usage des données ;
- signer le logiciel et vérifier sa signature ;
- tenir les logiciels à jour selon une procédure formalisée ;
- vérifier que les modifications apportées par les éditeurs de logiciels ne favorisent pas la fuite de données ;
- recourir à des mécanismes de détection et de protection contre les logiciels malveillants et logiciels espions, éprouvés et tenus à jour ;
- limiter les actions des usagers sur les logiciels ;
- garantir la traçabilité du cycle de vie des logiciels ;
- vérifier régulièrement les licences des logiciels utilisés ;
- interdire l'installation de logiciels permettant une observation interne (dans le cas d'un badge) ;
- s'assurer du cloisonnement de l'application de biométrie.

Mesures relatives aux canaux informatiques :

- sécuriser les canaux informatiques (canaux réservés et chiffrés).

Appréciation des risques

Le responsable de traitement analyse les risques d'accès non autorisé, de modification non désirée et de disparition de données à caractère personnel, compte tenu des mesures retenues.

Le responsable de traitement illustre les risques résiduels et les estime en termes de gravité et de vraisemblance.

Article 10

Obligation de documenter

Les justifications exigées dans le présent règlement, ainsi que l'estimation des risques devront faire l'objet d'une documentation détaillée. A ce titre, elles peuvent figurer au registre qui doit être tenu par le responsable de traitement conformément à l'article 30 du RGPD.

Article 11

Analyse d'impact sur la vie privée

Les traitements effectués dans le respect des dispositions du présent règlement type sont exonérés de la nécessité d'effectuer une analyse d'impact relative à la protection des données, prévue par l'article 35 du RGPD.