Commission nationale de l'informatique et des libertés

Délibération n° 2019-001 du 10 janvier 2019 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

NOR : *CNIL1908954X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD), notamment son article 9, alinéas 1, 2 et 4 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8 et 11-I-2° *(b)* ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Contexte

La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles a confié à la commission une mission nouvelle, celle d'établir et de publier, en concertation avec les organismes publics et privés représentatifs des acteurs concernés, « *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* ».

A ce titre, la commission peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, devenues sensibles au sens de l'article 9-1° du règlement général sur la protection des données (ci-après RGPD), ainsi que des données génétiques et de santé en application du 4° du même article.

La présente délibération a pour objet l'adoption d'un 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.

Elle intervient à la suite d'une consultation publique menée du 3 au 30 septembre 2018.

En conséquence, la commission adopte le règlement type suivant :

Article 1er

Objet et champ d'application du présent règlement

Conformément aux dispositions des articles 9-4° du RGPD, 11-I-2° *(b)* et 8-II-9° de la loi du 6 janvier 1978 modifiée 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 nécessaires au contrôle par les employeurs publics ou privés 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 (ci-après, « personnes concernées »).

Les données biométriques s'entendent, conformément à l'article 4-14 du RGPD, 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. Ces données sont considérées comme sensibles au sens de l'article 9 du RGPD.

Constitue un « gabarit », au sens du présent règlement type, le résultat du traitement de l'enregistrement brut (photo, enregistrement audio, etc.) de la caractéristique biométrique par un algorithme rendant impossible la reconstitution de celle-ci. Les gabarits constituent des données biométriques dérivées et doivent ainsi être distinguées des données dont sont issues les caractéristiques biométriques.

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.

Les organismes devront s'assurer que les traitements de contrôle d'accès concernés sont fondés au regard de l'article 6 du RGPD.

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 d'accès aux locaux limitativement identifiés par l'organisme comme devant faire l'objet d'une restriction de circulation ;
– le contrôle d'accès aux appareils et applications informatiques professionnels limitativement identifiés de l'organisme.

Article 3

Justification du recours à un traitement de données biométriques

Le responsable de traitement doit démontrer la 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 ;
– détailler les raisons justifiant l'utilisation de la biométrie plutôt qu'une autre technologie ;
– être documentée par le responsable du traitement.

Article 4

Données personnelles collectées et traitées

Dans le cadre du présent règlement type, le dispositif de contrôle d'accès biométrique ne peut comporter que les données à caractère personnel suivantes :

– **Données renseignées par l'employeur ou ses préposés (données d'identification) :**
  – l'identité : nom, prénoms, photographie, enregistrement brut (photo, enregistrement audio, etc.) de la caractéristique biométrique et gabarit(s) d'une ou plusieurs caractéristiques biométriques, numéro d'authentification ou numéro de support individuel, coordonnées professionnelles, clés de chiffrement ;
  – la vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade, identité ou dénomination sociale de la personne (physique ou morale) ayant la qualité d'employeur ;
  – l'accès aux locaux : accès, zones et plages horaires autorisés ;
  – l'accès aux outils de travail : matériels ou applicatifs concernés, plages horaires et modalités d'accès autorisées.
– **Données générées par le dispositif (données de journalisation) :**
  – journalisation des accès aux locaux : accès utilisés, horodatage des tentatives d'accès, numéro d'authentification ou numéro de support individuel ;
  – journalisation des accès aux outils de travail : matériels ou applicatifs concernés, horodatage des tentatives d'accès, numéro d'authentification ou numéro de support individuel.

Article 5

Données biométriques

Est autorisée, en milieu professionnel, l'authentification biométrique basée sur des caractéristiques morphologiques des personnes concernées. L'authentification biométrique nécessitant un prélèvement biologique (salive, sang, etc.) est proscrite dans le champ du présent règlement.

Le choix du ou des types de biométrie (iris, empreinte digitale, réseau veineux de la main, etc.) doit être justifié et documenté par l'employeur, notamment la raison d'utilisation d'une caractéristique biométrique plutôt qu'une autre.

Article 6

Personnes habilitées à traiter les données

Des profils d'habilitation doivent être prévus afin de gérer les accès aux données en tant que de besoin.

Les personnes habilitées ne peuvent accéder aux données que dans les limites de leurs attributions. Une revue annuelle des habilitations doit être opérée afin d'assurer que les droits accordés restent bien cohérents avec les personnes habilitées et leurs fonctions.

– **Concernant les données biométriques :**

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. Elles ne doivent accéder à ces gabarits dans le cadre de leur habilitation que de façon temporaire et pour les stricts besoins des actions précitées.

– **Concernant les autres données renseignées par l'employeur ou ses préposés :**

Peuvent avoir accès aux autres données à caractère personnel renseignées dans le dispositif biométrique (identité, vie professionnelle, accès aux locaux, matériels et applicatifs) les personnes qui sont limitativement habilitées en raison de leurs fonctions à gérer l'enrôlement de la personne concernée, la suppression ou la modification de son profil d'accès, ou à assurer la maintenance du dispositif.

– **Concernant les données générées par le dispositif :**

Seules peuvent avoir accès aux données générées par le dispositif biométrique les personnes qui sont limitativement habilitées en raison de leurs fonctions à assurer la sécurité des locaux, matériels et applicatifs concernés, ou de la sécurité du dispositif biométrique lui-même.

Article 7

Choix des modalités de détention du gabarit

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

– type 1 : les gabarits sous maîtrise 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 maîtrisé par l'employeur ou ses préposés, mais qui sont conservés sous une forme les rendant inexploitables sans l'utilisation d'un secret détenu par 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 ne nécessitant ni badge contenant le gabarit ni utilisation d'un secret maîtrisé par la personne concernée.

En l'absence de circonstances particulières mentionnées aux alinéas suivants, les traitements de données biométriques mis en place par des employeurs publics ou privés ne peuvent utiliser que des gabarits sous maîtrise des personnes concernées (type 1).

Il ne peut être fait recours aux gabarits sous maîtrise partagée (type 2) que s'il est avéré que la détention d'un support dédié au seul stockage du gabarit (type 1) n'est pas adaptée à l'architecture et au contexte d'exploitation du dispositif.

De la même manière, il ne peut être fait recours aux gabarits non maîtrisés par les personnes (type 3) que s'il est avéré que la mise en place des gabarits sous maîtrise partagée (type 2) ou des gabarits sous maîtrise des personnes concernées (type 1) n'est pas adapté au vu de l'architecture et du contexte d'exploitation du dispositif et seulement si les éléments de sécurité prévus à l'article 10 sont complétés par l'analyse des risques sur les droits et libertés des personnes prévue à l'article 11.

La décision de recourir aux gabarits de type 2 ou 3 doit être documentée de manière détaillée en justifiant le choix effectué.

Article 8

Modalités et durées de conservation

Les enregistrements bruts (photo, enregistrement audio, etc.) de la caractéristique biométrique ne peuvent être traités que le temps nécessaire au calcul du ou des gabarits : elles ne peuvent donc pas être conservées.

Les données biométriques dérivées ne peuvent être conservées que sous forme de gabarits chiffrés ne permettant pas de recalculer la caractéristique biométrique d'origine.

Elles ne peuvent être conservées que pendant la durée d'habilitation de la personne concernée, et doivent être supprimées en cas de retrait des habilitations ou en cas de cessation des fonctions de la personne concernée dans l'organisme employeur.

Les données de journalisation des accès produites par le dispositif biométrique ne peuvent être conservées en base active pendant plus de six mois glissants à compter de leur date d'enregistrement. Cela ne fait toutefois pas obstacle à leur conservation sous forme d'archives intermédiaires distinctes de la base active, avec accès restreint, dans la mesure où il existerait des dispositions législatives ou réglementaires spécifiques, ou encore si ces données présenteraient un intérêt en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables.

Les données d'identification, autres que les gabarits biométriques, doivent être supprimées au plus tard dans les six mois qui suivent la date du retrait des habilitations ou celle de la cessation des fonctions de la personne concernée au sein ou pour le compte de la personne physique ou morale ayant la qualité de l'employeur.

Pour rappel, cette suppression n'impacte pas les autres traitements mis en place par l'employeur pour des finalités différentes et portant sur des données similaires.

Article 9

Information des personnes

Sans préjudice de ses obligations relatives à l'information et à la consultation des instances représentatives du personnel, l'employeur fournit aux personnes concernées l'information individuelle obligatoire prévue par les articles 12 et suivants du RGPD.

Cette information doit figurer dans une notice écrite remise par le responsable de traitement à chaque personne concernée préalablement à l'enrôlement des données biométriques de ce dernier.

Article 10

Sécurité des données

Le responsable du traitement prend toutes précautions utiles, au regard de la nature des données et des risques que le traitement fait peser sur les personnes concernées et leurs droits, pour préserver la disponibilité, l'intégrité et la confidentialité des données traitées.

A cette fin, le responsable de traitement adopte au minimum 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 taille des clés conformes à l'état de l'art, renouvellement prévu, etc.) ;
- associer un code d'intégrité aux données (par exemple, signature ou hachage) ;
- intégrer une mesure technique ou organisationnelle de détection de fraude (par exemple : mesure de détection de faux doigts) ;
- interdire tout accès externe à la donnée biométrique, par exemple en mettant en œuvre des mesures de types 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 ;
- interdire la transmission de tout gabarit stocké par l'employeur en dehors du système ;
- veiller à l'effectivité de l'effacement des données à l'issue de la durée de conservation (destruction physique des cartes restituées en présence de la personne concernée ou information sur les moyens de destruction de la puce en l'absence de restitution, effacement automatisé et sécurisé des données en base, etc.) ;
- supprimer la donnée biométrique en cas d'accès non autorisé au terminal de lecture-comparaison ou au serveur distant (non applicable au stockage de type 1) ;
- 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, situation de handicap rendant difficile son utilisation, etc.) 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. L'utilisation de données biométriques de volontaires, qui ne sauraient être liées à leur profil réel mais à des profils créés pour les tests pour la validation du bon fonctionnement, doit être limitée au strict nécessaire. L'ensemble des données doit être supprimé au plus tard à la fin des tests ;
- déterminer les actions à entreprendre en cas d'échec de l'authentification (impossibilité de vérifier une identité, défaut d'habilitation à pénétrer dans une zone sécurisée, etc.) ;
- gérer de manière stricte l'accès physique et logique aux dispositifs 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.) ;
– 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 réenrôlement).

Mesures relatives aux matériels :

– mettre en œuvre des mesures soit permettant d'être alerté, soit supprimant les données biométriques 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'arrachage 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 biométriques, voire aux données du traitement ;
– 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'environnement d'exécution de l'application de biométrie.

Mesures relatives aux canaux informatiques :

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

Le responsable de traitement doit régulièrement, et au moins tous les ans, contrôler la bonne mise en œuvre de ces mesures. Il doit de plus effectuer une veille lui permettant d'agir dans un délai raisonnable en cas de modification par la CNIL de cette liste de mesures.

Article 11

Analyse d'impact relative à la protection des données

Conformément à la délibération n° 2018-327 du 11 octobre 2018 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, les traitements régis par le présent règlement type sont considérés comme susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées.

Par conséquent, une analyse d'impact relative à la protection des données doit être effectuée par le responsable du traitement préalablement à leur mise en œuvre, et ce quel que soit le type (1, 2 ou 3) de détention du gabarit biométrique choisi, conformément à l'article 35 du RGPD.

Le responsable de traitement devra donc à la fois respecter les dispositions du présent règlement type, documenter et tenir à disposition de la CNIL les justifications qui y sont demandées et procéder à une évaluation des risques sur les droits et libertés des personnes aux fins de les identifier et, le cas échéant, de les traiter.

Le choix de recourir aux modalités de détention du gabarit biométrique garantissant une moindre maîtrise de la personne, en particulier du type 3, doit faire l'objet d'une documentation particulièrement circonstanciée.

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

Il doit mettre à jour régulièrement, au moins tous les trois ans, cette évaluation des risques ainsi que les mesures de sécurité supplémentaires qui en découleraient.

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. Falque-Pierrotin