AU-053

Présentation de l'autorisation unique et grille d'analyse

Délibération n° 2016-187 du 30 juin 2016

portant autorisation unique de 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, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Présentation de la norme

L'autorisation unique AU053 concerne les dispositifs biométriques reposant sur un stockage des gabarits en base (serveurs distants ou terminal de lecture comparaison par exemple) mis en œuvre pour contrôler l'accès aux locaux, appareils et applications informatiques utilisés sur les lieux de travail.

L'installation de ces dispositifs est soumise à des conditions strictes.

L'organisme doit prouver que le dispositif biométrique est nécessaire aux fins de contrôle d'accès et qu'il ne peut se contenter d'un système moins intrusif (une simple badgeuse par exemple). Il doit justifier de son besoin de centraliser les gabarits biométriques dans ses serveurs. Si le stockage du gabarit biométrique sur un support confié à la personne concernée est possible, l'organisme doit privilégier ce type de dispositif et se référer à une autre autorisation unique, l'AU052. Dans le cas contraire, le responsable du dispositif biométrique devra argumenter par écrit ses choix et appliquer les mesures de sécurité précisées dans l'autorisation unique AU053.

Texte officiel

Délibération n° 2016-187 du 30 juin 2016 portant autorisation unique de 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, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)

Responsables de traitement concernés

- Tout organisme privé (exception : établissement accueillant des mineurs) ;
- Les organismes publics, sauf l'Etat et les établissements accueillant des mineurs.

Objectif(s) poursuivi(s) par le traitement (finalités)

- 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.

Finalités exclues du champ de la norme

Le contrôle des horaires, L'authentification biométrique proposée en dehors de tout contexte professionnel, par une autre personne que l'employeur ou le donneur d'ordre / clients dans le cas d'une relation de soustraitance

Données personnelles concernées

Les données concernent toute personne spécifiquement habilitées par le responsable du traitement à accéder aux locaux, appareils ou applications informatiques protégées par le contrôle d'accès biométrique.

Elles portent sur :

- **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 ;
- **le déplacement des personnes** : porte utilisée, zones et plage horaire d'accès autorisées, date et heure d'entrée et de sortie ;
- **en cas d'accès à un parking** : numéro d'immatriculation du véhicule, numéro de place de stationnement ;

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

Les gabarits peuvent être stockés, soit en base de données où elles peuvent être associées à un numéro d'authentification de la personne, soit dans la mémoire interne du terminal de lecture comparaison qui ne dispose d'aucun port de communication permettant l'extraction de ce gabarit.

Le responsable du traitement s'engage à justifier au moyen d'une documentation appropriée :

- du choix de recourir à un dispositif biométrique plutôt qu'à un traitement non biométrique au regard de la finalité du traitement ;
- du choix du stockage des gabarits en base et des contraintes faisant obstacle au maintien de la maitrise individuelle des personnes sur leur gabarit.

Durée de conservation des données

- Le gabarit biométrique ne peut être conservé que le temps de l'habilitation de la personne concernée et doit être supprimé à son départ.
- Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées cinq ans après le départ de la personne disposant d'une habilitation d'accès de longue durée, et 3 mois après le départ des personnes disposant d'une habilitation d'accès ponctuelle.
- Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de 3 mois.

Destinataires des données

Les personnes habilitées du service du personnel peuvent avoir connaissance des données suivantes : identité (à l'exception du gabarit de la biométrie utilisé et du code d'authentification), vie professionnelle, déplacement des personnes et informations en relation avec la gestion du parking.

Les personnes habilitées du service gérant la sécurité des locaux données peuvent avoir connaissance des données suivantes : identité (à l'exception du gabarit de la biométrie utilisée et du code d'authentification), plages horaires autorisées, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking ou des locaux.

Les personnes habilitées du service ou de l'organisme gérant le restaurant d'entreprise ou administratif peuvent avoir connaissance des données suivantes : identité (à l'exception du gabarit du contour l'organisme gérant le restaurant d'entreprise de la main et du code d'authentification) et informations en relation avec la gestion de la restauration.

Toutes ces personnes ne peuvent avoir accès au gabarit de l'empreinte digitale que de façon temporaire et pour les stricts besoins de l'enrôlement de la personne concernée ou de la suppression du gabarit. Il leur est impossible d'accéder directement, de modifier, ou de copier sur un autre support, les gabarits enregistrés.

Information des personnes et respect des droits « informatique et libertés »

Lors de la collecte des données, le responsable du traitement doit informer les personnes :

- de son identité,
- de la finalité du traitement,
- du caractère obligatoire ou facultatif des informations qu'il collecte,
- des destinataires de ces informations,
- de l'existence de droits pour les personnes fichées et du service auprès duquel les faire valoir,
- des transmissions envisagées.
- Préalablement à la mise en place du dispositif de contrôle d'accès, les instances représentatives du personnel sont informées et consultées.

L'information préalable des employés est effectuée par remise d'une notice explicative. Elle précise notamment la manière d'exercer les droits d'accès, de rectification et d'opposition pour motif légitime.

Sécurité et confidentialité

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.

Compte tenu des risques liés au stockage des gabarits en base, le responsable du traitement s'engage à documenter la conformité de son traitement sous forme d'analyse d'impact relative à la protection des données.

L'analyse comprend une description du traitement, de ses finalités, de sa nécessité et de sa proportionnalité ainsi que les mesures prises pour réduire les risques pour les droits et libertés des personnes concernées.

L'AU-053 donne une liste d'exigences de sécurité assortie de mesures concrètes permettant de limiter ces risques.

Les responsable du traitement de données biométriques doivent utiliser le document ci-dessous, afin de documenter les mesures prises en application de l'AU-053.

Grille d'analyse

La présente grille d'analyse a pour but de **démontrer que les risques sont maîtrisés** lors de la mise en œuvre du traitement biométrique, **à l'aide d'une réflexion sur trois axes** :

1. **le choix du dispositif et de ses modalités de mise en œuvre**, pour évaluer sa proportionnalité au regard du contexte d'installation et de la finalité poursuivie par l'organisme ;
2. **le respect des exigences**, pour s'assurer de l'application des principes juridiques de la loi Informatique et Libertés ainsi que des recommandations de la CNIL ;
3. **l'appréciation des risques résiduels**, pour apprécier si les risques sur la vie privée des personnes concernées sont maîtrisés, après application de mesures organisationnelles et techniques.

Ces trois axes ont pour objectif d'accompagner les organismes dans l'appréciation des impacts du traitement biométrique et dans le choix des solutions de contrôle d'accès répondant à leurs besoins.

Note : le **concours du fournisseur, de l'intégrateur et de l'installeur du dispositif peut être utile**, notamment s'ils ont eux-mêmes mené une étude d'impact sur la vie privée (EIVP, plus connue sous son nom en anglais de *Privacy Impact Assessment* – PIA), dans laquelle les descriptions techniques, mesures et conditions de mise en œuvre ont déjà été formalisées.

Le premier axe : étude du dispositif envisagé au regard de ses caractéristiques techniques et de ses modalités de mise en œuvre

Le responsable de traitement doit justifier de la pertinence du recours au dispositif biométrique par rapport à son besoin, notamment :

- de l'usage de la biométrie par rapport à un contrôle d'accès non biométrique (par exemple un contrôle par badge), afin de démontrer que son choix est pertinent et qu'un dispositif moins intrusif n'aurait pas suffi ;
- du choix d'utiliser telle ou telle caractéristique biométrique et tel mode de stockage du gabarit plutôt qu'un autre (par exemple, le choix d'utiliser la reconnaissance faciale avec stockage du gabarit en base plutôt que la reconnaissance d'empreinte digitale avec conservation du gabarit sur un support individuel).

Pour ce faire, le tableau ci-dessous doit être renseigné :

Caractéristiques	Description	Justification[1]
Justification de l'usage du dispositif biométrique (plutôt que sans biométrie)	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Type de technologie employée[2]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Données traitées[3]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Stockage des données biométriques[4]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Nombre de dispositifs concernés et lieu(x) d'implantation	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Nombre de personnes concernées par lieu	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Typologie de la population[5]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Dispositions complémentaires tenant compte des contraintes d'utilisation (si besoin)[6]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.

[1] Justifier les choix décidés en expliquant leur nécessité. Ces justifications peuvent être issues du contexte d'utilisation du dispositif et des risques de sécurité qu'il est censé contribuer à traiter.

[2] Contour de la main, reconnaissance vocale, réseau veineux du doigt ou de la paume, reconnaissance de l'empreinte digitale, reconnaissance de l'iris de l'œil, reconnaissance faciale, ADN notamment.

3 Données biométriques initiales, gabarits biométriques, gabarits révocables par exemple, et historique d'accès.

4 Supports individuels (cartes, clés USB) ou base de données interne au dispositif ou base de données distante. Une base centralisée contient les données biométriques de plusieurs usagers sur un même support, local au dispositif, ou distant à travers un réseau.

5 La typologie de la population permet d'apprécier le choix du dispositif biométrique en fonction des catégories d'usagers en termes de morphologie, de contrainte professionnelle, de prise en compte d'un handicap.

6 Les contraintes d'utilisation sont liées aux difficultés de captation de la donnée biométrique (déformation de la voix, visage couvert, port de gants ou lunettes, etc.). Des dispositions accompagnant le dispositif biométrique doivent alors être mises en œuvre (sas d'isolement, support visuel pour guider la position du visage, etc.).

Caractéristiques	Description	Justification[1]
Modalités d'enrôlement[7]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Taux de fausses acceptations	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Taux de faux rejets	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Capacité de paramétrage[8]	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.
Autres caractéristiques (si besoin)	Cliquez ici pour taper du texte.	Cliquez ici pour taper du texte.

7 L'enrôlement de l'usager doit être encadré par une personne habilitée à l'administration du dispositif biométrique. Cet enrôlement pourra s'effectuer directement sur le dispositif ou à distance sur un poste spécifique dédié à cette tâche.

8 Le dispositif biométrique possède-t-il des possibilités de réglages de sa fiabilité ? Si oui, quelles sont les personnes habilitées à manipuler ces paramètres ?

Le deuxième axe : étude du respect des exigences de la CNIL

Le responsable de traitement est tenu de décrire, de manière détaillée, les mesures mises en œuvre afin de satisfaire les exigences de la CNIL.

Ces exigences intègrent :

- les obligations juridiques de la loi Informatique et Libertés ;
- les recommandations de la CNIL encadrant l'usage de la biométrie ;
- les mesures permettant de réduire la gravité et la vraisemblance des risques que la mise en œuvre d'un dispositif biométrique fait peser sur la vie privée des personnes concernées.

Afin de s'assurer du respect des exigences, l'organisme doit remplir le tableau suivant[9] :

Exigences permettant d'atteindre les objectifs de la CNIL	Description des mesures prévues OU justification
Exigences portant sur les données	
Collecter et utiliser les seules données biométriques nécessaires [10] ***sous la forme d'un gabarit ne permettant pas de recalculer la donnée biométrique d'origine***	Cliquez ici pour taper du texte.
Chiffrer les données biométriques à l'aide d'un algorithme cryptographique et d'une gestion des clés conformes à l'état de l'art[11]	Cliquez ici pour taper du texte.
Associer un code d'intégrité aux données (par exemple, signature par hachage)	Cliquez ici pour taper du texte.
Interdire tout accès externe à la donnée biométrique (« match-on-card » ou module de sécurité physique/logique type HSM)	Cliquez ici pour taper du texte.
Effectuer le contrôle d'accès par une comparaison entre l'échantillon calculé et le gabarit d'enrôlement enregistré sans copie du gabarit	Cliquez ici pour taper du texte.
Minimiser la durée de conservation des données et veiller à l'effectivité de leur effacement dès la fin de l'habilitation de la personne concernée	Cliquez ici pour taper du texte.
Supprimer la donnée biométrique en cas d'accès non autorisé au terminal de lecture-comparaison ou au serveur distant	Cliquez ici pour taper du texte.

9 Le responsable de traitement doit soit décrire les mesures prévues pour la respecter, soit justifier dûment pourquoi elle ne l'est pas.
10 En particulier, imposer des contraintes à l'enrôlement (distance du capteur, luminosité, angle, arrière-plan, temps de pose, etc.) qui permettront de garantir que seules les données utiles des personnes collaborant activement seront traitées.
11 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.).

Exigences permettant d'atteindre les objectifs de la CNIL	Description des mesures prévues OU justification
Exigences portant sur l'organisation	
Informer les personnes concernées, de manière complète, spécifique et intelligible, via des supports clairs et synthétiques. Consulter les Instances représentatives du personnel si nécessaire	Cliquez ici pour taper du texte.
Responsabiliser les personnes concernées sur les bonnes conditions d'utilisation des matériels	Cliquez ici pour taper du texte.
Mettre à disposition un dispositif alternatif « de secours » ou utilisé à titre exceptionnel[12], sans contrainte, ni surcoût pour les personnes n'utilisant pas la solution biométrique	Cliquez ici pour taper du texte.
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	Cliquez ici pour taper du texte.
Déterminer les actions à entreprendre en cas d'échec de l'authentification[13]	Cliquez ici pour taper du texte.
Gérer de manière stricte l'accès physique et logique au dispositif et bases de données par les personnes habilitées[14]	Cliquez ici pour taper du texte.
Former spécifiquement les administrateurs et personnes habilitées à gérer les données[15]	Cliquez ici pour taper du texte.
Intégrer une mesure technique ou organisationnelle de détection anti-fraude	Cliquez ici pour taper du texte.
Prévenir les personnes concernées en cas d'accès non autorisé à leurs données	Cliquez ici pour taper du texte.
Formaliser, appliquer et faire connaître une procédure de secours en cas d'incident (prévoyant notamment le ré-enrôlement)	Cliquez ici pour taper du texte.
Exigences portant sur les matériels	

[12] Pour les personnes ne répondant pas aux contraintes du dispositif biométrique (enrôlement ou lecture de la donnée biométrique impossible), une « solution de secours » doit être mise en œuvre pour assurer une continuité du service proposé, limitée toutefois à un usage exceptionnel.

13 Présenter les mesures prises dans le cas du rejet d'une personne par le dispositif biométrique (rejet suite à l'échec de N tentatives, alerte auprès des administrateurs, etc.).

14 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…), 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.

15 Enrôlement, traitements, effacement…

Exigences permettant d'atteindre les objectifs de la CNIL	Description des mesures prévues OU justification
Mettre en œuvre des mesures permettant d'être alerté en cas de tentative d'effraction sur le lecteur ou le dispositif de stockage[16]	Cliquez ici pour taper du texte.
Réserver un matériel spécifique au stockage des données	Cliquez ici pour taper du texte.
Utiliser des matériels certifiés aux conditions d'usage et/ou en termes de sécurité	Cliquez ici pour taper du texte.
Garantir la traçabilité du cycle de vie du matériel	Cliquez ici pour taper du texte.
Obtenir un engagement de responsabilité de la part des administrateurs	Cliquez ici pour taper du texte.
Journaliser les opérations effectuées sur les supports	Cliquez ici pour taper du texte.
Mettre en place des mesures de sauvegarde	Cliquez ici pour taper du texte.
Formaliser et tester une procédure de récupération du système	Cliquez ici pour taper du texte.
Exigences portant sur les logiciels	
Réserver un logiciel spécifique à l'usage des données	Cliquez ici pour taper du texte.
Signer le logiciel et vérifier sa signature	Cliquez ici pour taper du texte.
Tenir les logiciels à jour selon une procédure formalisée	Cliquez ici pour taper du texte.
Vérifier que les modifications apportées par les éditeurs de logiciels ne favorisent pas la fuite de données	Cliquez ici pour taper du texte.
Recourir à des mécanismes de détection et de protection contre les logiciels malveillants et logiciels espions, éprouvés et tenus à jour	Cliquez ici pour taper du texte.
Limiter les actions des usagers sur les logiciels	Cliquez ici pour taper du texte.
Garantir la traçabilité du cycle de vie des logiciels	Cliquez ici pour taper du texte.
Vérifier régulièrement les licences des logiciels utilisés	Cliquez ici pour taper du texte.
Exigences portant sur les canaux informatiques	
Sécuriser les canaux informatiques (canaux réservés et chiffrés)	Cliquez ici pour taper du texte.
Mettre en place des mesures empêchant la transmission des gabarits stockés	Cliquez ici pour taper du texte.

[16] 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.

Dans le cas où les exigences de la CNIL sont appliquées, les objectifs seront considérés comme atteints. Dans les autres cas, il conviendra d'évaluer la pertinence et la suffisance des mesures choisies par le responsable de traitement au regard des objectifs.

Le troisième axe : appréciation des risques résiduels sur la vie privée des personnes concernées

Le responsable de traitement doit apprécier les risques que le dispositif biométrique envisagé va générer sur la vie privée des personnes concernées :

- d'une part, il doit identifier les **impacts potentiels sur la vie privée**[17] des personnes concernées en cas d'atteinte à la disponibilité, à l'intégrité et à la confidentialité de leurs données biométriques, et en estimer la **gravité**[18] en tenant compte des mesures existantes ou prévues ;
- d'autre part, il doit identifier les **principales menaces**[19] qui pourraient permettre que ces impacts surviennent, et en estimer la **vraisemblance**[20] en tenant compte des mesures existantes ou prévues.

Notes :

- cette partie a pour objet de sensibiliser dès à présent les responsables du traitement à une partie importante de l'exercice de l'étude d'impact sur la vie privée (EIVP, plus connue sous son nom en anglais de *Privacy Impact Assessment* – PIA) ;
- le responsable de traitement peut autant recourir à une méthode éprouvée (ex : guides PIA de la CNIL[21]) que mener cette réflexion de manière empirique ;
- les risques sur les données biométriques et données associées des personnes concernées doivent être pris en compte autant durant la collecte, la conservation que pendant la transmission de ces données.

Pour ce faire, le tableau ci-dessous doit être renseigné :

17 Les dommages sur les personnes concernées peuvent être corporels, matériels ou moraux.

18 L'échelle suivante peut être utilisée pour estimer la gravité des risques :

1. Négligeable : les personnes concernées ne seraient pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteraient sans difficulté.
2. Limitée : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés.
3. Importante : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés.
4. Maximale : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.

19 Voir notamment l'annexe « Menaces génériques » du guide de la CNIL

20 L'échelle suivante peut être utilisée pour estimer la vraisemblance des risques :

1. Négligeable : le risque ne devrait pas se (re)produire.
2. Limitée : le risque pourrait se (re)produire.
3. Importante : le risque devrait se (re)produire un jour ou l'autre.
4. Maximale : le risque devrait certainement se (re)produire prochainement.

21 Guides « étude d'impact sur la vie privée » (http://www.cnil.fr/linstitution/actualite/article/article/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil/).

Risques	Impacts potentiels résiduels	Gravité résiduelle	Principales menaces résiduelles	Vraisemblance résiduelle
Accès non autorisé aux données biométriques	Cliquez ici pour taper du texte.	Choisissez un élément.	Cliquez ici pour taper du texte.	Choisissez un élément.
Modification non désirée des données biométriques	Cliquez ici pour taper du texte.	Choisissez un élément.	Cliquez ici pour taper du texte.	Choisissez un élément.
Disparition des données biométriques	Cliquez ici pour taper du texte.	Choisissez un élément.	Cliquez ici pour taper du texte.	Choisissez un élément.

Il convient de vérifier que les réponses apportées, et notamment que les impacts envisagés sont bien des impacts sur la vie privée des personnes concernées, et non des impacts sur l'organisme, et que la gravité et la vraisemblance ne sont pas sous-estimées.

L'exemple fictif suivant illustre l'utilisation du tableau précédent :

Dans le contexte d'élévation du niveau de sécurité pour un accès à une zone sensible au sein d'un organisme bancaire, la mise en place d'un dispositif biométrique de contrôle d'accès physique est présentée comme une réponse adéquate. Cet accès est limité à un nombre connu d'employés habilités. Le dispositif proposé doit répondre à plusieurs contraintes notamment un haut degré de fiabilité écartant le risque de fausse acceptation et une grande rapidité d'exécution n'entravant pas la fluidité des passages.

De nombreux agents habilités se déplacent entre différents sites. Dans le cas de l'usage d'un support individuel, les problèmes de perte ou de vol restent similaires à ceux rencontrés avec le dispositif classique par badge concernant la disponibilité de l'accès. Pour cette raison et afin d'assurer l'accès aux locaux aux personnes habilitées en nombre restreint, même en l'absence de leur badge, dans des situations d'urgence, une solution de conservation des données biométriques en base centrale est préférée.

Risques	Impacts potentiels résiduels	Gravité résiduelle	Principales menaces résiduelles	Vraisemblance résiduelle
Accès non autorisé aux données biométriques	Utilisation des données pour incriminer une personne (attaque ciblée contre elle ou pour détourner les soupçons des forces de l'ordre). Ré-identification d'une personne pour un délit ou un crime (par des services de renseignement, la police, etc.). Perte de la confiance de l'authentification / identification du fait que des données biométriques ont été compromises.	3. Importante	Observation de données interprétables sur un écran, vol d'un terminal (ex : ordinateur portable) permettant d'accéder aux données, utilisation de fonctionnalités d'administration avancées, contagion par un code malveillant lors d'une configuration par les développeurs ou les mainteneurs, interception de flux sur le réseau interne ou externe permettant d'observer des données interprétables.	2. Limitée
Modification non désirée des données biométriques	Usurpation d'identité sans qu'elle puisse facilement le démontrer et ses conséquences (ex : licenciement pour faute grave, poursuites pour avoir compromis des secrets de l'entreprise, vol, etc.). Dans le cas d'une base centralisée, mauvaise identification de la personne pouvant entrainer des conséquences diverses liées à la nature de la base (limitée pour un lieu de travail où une pièce d'identité pourra facilement démontrer l'erreur).	2. Limitée	Modifications inopportunes dans une base de données, utilisation de fonctionnalités d'administration avancées.	2. Limitée
Disparition des données biométriques	Service ou lieu inaccessible. Obligation de la personne à procéder à un nouvel enrôlement. La gravité est limitée car la disparition sera détectée rapidement.	2. Limitée	Surexploitation des capacités de traitement, panne de courant, dysfonctionnement d'un dispositif de stockage entraînant un effacement, erreur de manipulation menant à la suppression de données, effacement d'un exécutable en production ou de code sources, arrêt des mises à jour de maintenance de sécurité par l'éditeur.	2. Limitée